

IJNS

**International Journal
of Network Security**



ISSN 1816-353X (Print)
ISSN 1816-3548 (Online)

Vol. 19, No. 4 (July 2017)

INTERNATIONAL JOURNAL OF NETWORK SECURITY

Editor-in-Chief

Prof. Min-Shiang Hwang

Department of Computer Science & Information Engineering, Asia University, Taiwan

Co-Editor-in-Chief:

Prof. Chin-Chen Chang (IEEE Fellow)

Department of Information Engineering and Computer Science, Feng Chia University, Taiwan

Publishing Editors

Shu-Fen Chiou, Chia-Chun Wu, Cheng-Yi Yang

Board of Editors

Ajith Abraham

School of Computer Science and Engineering, Chung-Ang University (Korea)

Wael Adi

Institute for Computer and Communication Network Engineering, Technical University of Braunschweig (Germany)

Sheikh Iqbal Ahamed

Department of Math., Stat. and Computer Sc. Marquette University, Milwaukee (USA)

Vijay Atluri

MSIS Department Research Director, CIMIC Rutgers University (USA)

Mauro Barni

Dipartimento di Ingegneria dell'Informazione, Università di Siena (Italy)

Andrew Blyth

Information Security Research Group, School of Computing, University of Glamorgan (UK)

Soon Ae Chun

College of Staten Island, City University of New York, Staten Island, NY (USA)

Stefanos Gritzalis

University of the Aegean (Greece)

Lakhmi Jain

School of Electrical and Information Engineering, University of South Australia (Australia)

James B D Joshi

Dept. of Information Science and Telecommunications, University of Pittsburgh (USA)

Çetin Kaya Koç

School of EECS, Oregon State University (USA)

Shahram Latifi

Department of Electrical and Computer Engineering, University of Nevada, Las Vegas (USA)

Cheng-Chi Lee

Department of Library and Information Science, Fu Jen Catholic University (Taiwan)

Chun-Ta Li

Department of Information Management, Tainan University of Technology (Taiwan)

Iuon-Chang Lin

Department of Management of Information Systems, National Chung Hsing University (Taiwan)

John C.S. Lui

Department of Computer Science & Engineering, Chinese University of Hong Kong (Hong Kong)

Kia Makki

Telecommunications and Information Technology Institute, College of Engineering, Florida International University (USA)

Gregorio Martinez

University of Murcia (UMU) (Spain)

Sabah M.A. Mohammed

Department of Computer Science, Lakehead University (Canada)

Lakshmi Narasimhan

School of Electrical Engineering and Computer Science, University of Newcastle (Australia)

Khaled E. A. Negm

Etisalat University College (United Arab Emirates)

Joon S. Park

School of Information Studies, Syracuse University (USA)

Antonio Pescapè

University of Napoli "Federico II" (Italy)

Zuhua Shao

Department of Computer and Electronic Engineering, Zhejiang University of Science and Technology (China)

Mukesh Singhal

Department of Computer Science, University of Kentucky (USA)

Nicolas Sklavos

Informatics & MM Department, Technological Educational Institute of Patras, Hellas (Greece)

Tony Thomas

School of Computer Engineering, Nanyang Technological University (Singapore)

Mohsen Toorani

Department of Informatics, University of Bergen (Norway)

Shuozhong Wang

School of Communication and Information Engineering, Shanghai University (China)

Zhi-Hui Wang

School of Software, Dalian University of Technology (China)

Chuan-Kun Wu

Chinese Academy of Sciences (P.R. China) and Department of Computer Science, National Australian University (Australia)

Chou-Chen Yang

Department of Management of Information Systems, National Chung Hsing University (Taiwan)

Sherali Zeadally

Department of Computer Science and Information Technology, University of the District of Columbia, USA

Jianping Zeng

School of Computer Science, Fudan University (China)

Justin Zhan

School of Information Technology & Engineering, University of Ottawa (Canada)

Mingwu Zhang

College of Information, South China Agric University (China)

Yan Zhang

Wireless Communications Laboratory, NICT (Singapore)

PUBLISHING OFFICE

Min-Shiang Hwang

Department of Computer Science & Information Engineering, Asia University, Taichung 41354, Taiwan, R.O.C.

Email: mshwang@asia.edu.tw

International Journal of Network Security is published both in traditional paper form (ISSN 1816-353X) and in Internet (ISSN 1816-3548) at <http://ijns.jalaxy.com.tw>

PUBLISHER: Candy C. H. Lin

© Jalaxy Technology Co., Ltd., Taiwan 2005

23-75, P.O. Box, Taichung, Taiwan 40199, R.O.C.

1. An Improved Two-party Password-Authenticated Key Agreement Protocol with Privacy Protection Based on Chaotic Maps
Hongfeng Zhu, Yifeng Zhang 487-497
2. Pre-image Resistant Cancelable Biometrics Scheme Using Bidirectional Memory Model
Mayada Tarek, Osama Ouda, Taher Hamza 498-506
3. Propagation Model with Varying Population Size of Removable Memory Device Virus
Cong Jin, Xiaoyan Wang 507-516
4. Provably Authenticated Group Key Agreement Based on Braid Groups - The Dynamic Case
Pipat Hiranvanichakorn 517-527
5. An Evolutionary Multi-objective Approach for Modelling Network Security
Seyed Mahmood Hashemi, Jingsha He 528-536
6. A New Trusted Routing Protocol for Vehicular Ad Hoc Networks Using Trusted Metrics
Thangakumar Jeyaprakash, Rajeswari Mukesh 537-545
7. New Constructions of Binary Interleaved Sequences with Low Autocorrelation
Ruifang Meng, Tongjiang Yan 546-550
8. A New Level 3 Trust Hierarchal Certificateless Public Key Cryptography Scheme in the Random Oracle Model
Mohammed Hassouna, Bazara Barry, and Eihab Bashier 551-558
9. A Secured Access Control Technique for Cloud Computing Environment Using Attribute Based Hierarchical Structure and Token Granting System
Balamurugan Balusamy, P. Venkata Krishna, G. S. Tamizh Arasi, and Victor Chang 559-572
10. A Certificateless Strong Designated Verifier Signature Scheme with Non-delegatability
Yang Chen, Yang Zhao, Hu Xiong, and Feng Yue 573-582
11. COL-MOD: A New Module to Quantify the Weight of Damage Incurred by Collision Attacks
Mina Malekzadeh, Moghis Ashrotaghi 583-592
12. Chaotic Map Based Random Image Steganography Using LSB Technique
Sujarani Rajendran, Manivannan Doraipandian 593-598
13. A Secure Strong Designated Verifier Signature Scheme
Asif Uddin Khan, Bikram Kesari Ratha 599-604
14. On the Security of an Mutual Verifiable Provable Data Auditing in Public Cloud Storage
Jianhong Zhang, Pengyan Li, and Min Xu 605-612
15. Linear Complexity of Quaternary Sequences Over Z_4 Derived From Generalized Cyclotomic Classes Modulo $2p$
Zhixiong Chen, Vladimir Edemskiy 613-622
16. A Key-insulated Proxy Re-encryption Scheme for Data Sharing in a Cloud Environment
Yilei Wang, Dongjie Yan, Fagen Li, Xiong Hu 623-630

17. NFC Communications-based Mutual Authentication Scheme for the Internet of Things
Yanna Ma 631-638
18. An Improved Key-Management Scheme for Hierarchical Access Control
Wan-Yu Chao, Cheng-Yi Tsai, Min-Shiang Hwang 639-643
19. Security on a Knapsack-Type Encryption Scheme Based Upon Hybrid-Model Assumption
Zhengping Jin, Hong Zhang, Zhongxian Li 644-647
20. Comments on a Secure Authentication Scheme for IoT and Cloud Servers
Wei-Liang Tai, Ya-Fen Chang 648-651

An Improved Two-party Password-Authenticated Key Agreement Protocol with Privacy Protection Based on Chaotic Maps

Hongfeng Zhu, Yifeng Zhang

(Corresponding author: Hongfeng Zhu)

Software College, Shenyang Normal University

No. 253, HuangHe Bei Street, HuangGu District, Shenyang 110034, P.R. China

(zhuhongfeng1978@163.com; 1548452125@qq.com)

(Received Jan. 31, 2016; revised and accepted Apr. 23 & May 7, 2016)

Abstract

Since the 1990s, chaotic systems have widely used to cryptography which can be used to design kinds of secure protocols, digital signatures, hash functions and so on. Recently, Guo and Zhang proposed an chaotic public-key cryptosystem based key agreement protocol. In 2015, Lee has proved that Guo et al.'s scheme cannot resist off-line password guess attack. Then, Liu and Xue further point out that Guo et al.'s scheme has redundancy in protocol design and still has some security flaws. In this paper, we further prove that Liu's scheme has four flaws at least and a potential loophole. Moreover, these papers provided no privacy protection which is a very important property in the modern social network. So an improved Two-party Password-Authenticated Key Agreement Protocol with Privacy Protection is proposed for amending these flaws and loophole. Compared with the related literatures recently, our proposed scheme can not only own high efficiency and unique functionality, but is also robust to various attacks and achieves perfect forward secrecy. Finally, we give the security proof and the efficiency analysis of our proposed scheme.

Keywords: Chaotic maps, key agreement, off-line password-guessing attack, privacy protection

1 Introduction

Authenticated key exchange (AKE) allows two or more parties to compute shared keys and also ensures their identities are authentic in insecure networks. The mutual authentication and the key agreement are impartible and the reasons are:

- 1) A protocol only has the attribute of key agreement will lead the man-in-the-middle attacks at least, just like the first key agreement scheme Diffie-Hellman (D-H) key agreement [1].

- 2) A protocol only has the attribute of mutual authentication will bring about some function loss. For example, you can use mutual authentication scheme for acquiring E-mail service, but you cannot only use mutual authentication scheme for getting Instant Messaging service, because there is no session key to protect transmissive information. Unlike digital signature needing the third party for arbitration and many other properties, MAKA protocols are only related with the involving participants, so naturally the efficient chaotic cryptosystem is the first candidate.

Compared with other cryptosystem systems, chaotic system has numerous advantages, such as extremely sensitive to initial parameters, unpredictability, deterministic random-like process and so on. In the past few years, cryptography systems based on chaos theory have been studied widely [2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16], such as two-party AKE protocols [3, 4, 5, 16], three-party AKE protocols [6], N-party AKE protocols [7], random number generating [8], symmetric encryption [9], asymmetric encryption [10], hash functions [11], digital signature [12], anonymity scheme [13], Multi-server Environment (Centralized Model) [14], Multiple Servers to Server Architecture (Distributed Model) [15].

In 2007, Xiao et al. [16] proposed a chaos-based key agreement protocol. However, Guo and Zhang [3] pointed out that Xiao et al.'s [16] scheme could not resist server spoofing attacks and denial-of-service (DoS) attacks. Furthermore, in Guo and Zhang [3] proposed an improved scheme, which claimed that their protocol could resist the security flaws of Xiao et al.'s protocol. Moreover, in [4], the author has proved that Guo et al.'s scheme cannot resist off-line password guess attack. However, the improved scheme in [4] introduces a traditional asymmetric encryption algorithm to address the issue. Very recently, Liu and Xue [5] pointed out Guo et al.'s protocol [3] has unnecessary redundancy in protocol design which will in-

crease the implementation time of key agreement to bring about more unnecessary delay and also has the threat of replay attacks and DoS attacks.

In this paper, we demonstrate that Liu et al.'s protocol [5] has still security problems: password Guessing Attacks for privileged-insider, off-line Password Guessing Attacks for any adversary, stolen-verifier attacks and the complications from Off-line Password Guessing Attacks and Potential Loophole of XOR Operation. Based on [5], we provide an improved secure password and chaos-based two-party key agreement protocol. The main contributions are shown as below.

- 1) By analyzing of Liu et al.'s scheme, we found four flaws (password Guessing Attacks for privileged-insider, off-line Password Guessing Attacks for any adversary, stolen-verifier attacks and the complications from Off-line Password Guessing Attacks) and one loophole (Potential Loophole of XOR Operation).
- 2) The improved protocol provides privacy protection. Moreover, for eliminating Potential Loophole of XOR Operation and at the same time for improving efficiency, the proposed scheme uses multiplication in finite field method instead of XOR operation for two different length messages.

The rest of the paper is organized as follows: Review and cryptanalysis of Liu et al.'s protocol is given in Section 2. Next, an improved privacy-protection two-party password-authentication key agreement protocol is described in Section 3. Then, the security analysis and efficiency analysis are given in Section 4 and Section 5. This paper is finally concluded in Section 6.

2 Review of Liu et al.'s Protocol

In this section, we first describe the Chebyshev chaotic map, which has semigroup property and can be used to design chaos-based public-key cryptosystems. After that, we introduce Liu et al.'s two-party key agreement protocol and give its security analysis.

2.1 Chebyshev Chaotic Maps

Let n be an integer and let x be a variable with the interval $[-1, 1]$. The Chebyshev polynomial [17]. $T_n(x) : [-1, 1] \rightarrow [-1, 1]$ is defined as $T_n(x) = \cos(n \arccos(x))$. Chebyshev polynomial map $T_n : R \rightarrow R$ of degree n is defined using the following recurrent relation:

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x). \quad (1)$$

where, $n \geq 2$, $T_0(x) = 1$, and $T_1(x) = x$. The first few Chebyshev polynomials are:

$$\begin{aligned} T_2(x) &= 2x^2 - 1, \\ T_3(x) &= 4x^3 - 3x, \\ T_4(x) &= 8x^4 - 8x^2 + 1, \\ &\vdots \end{aligned}$$

One of the most important properties is that Chebyshev polynomials are the so-called semi-group property which establishes that

$$T_r(T_s(x)) = T_{r \cdot s}(x). \quad (2)$$

An immediate consequence of this property is that Chebyshev polynomials commute under composition:

$$T_r(T_s(x)) = T_s(T_r(x)). \quad (3)$$

In order to enhance the security, Zhang [18] proved that semi-group property holds for Chebyshev polynomials defined on interval $(-\infty, +\infty)$. In our proposed protocol, we utilize the enhanced Chebyshev polynomials:

$$T_n(x) = (2xT_{n-1}(x) - T_{n-2}(x)) \pmod{N}, \quad (4)$$

where, $n \geq 2$, $x \in (-\infty, +\infty)$, and N is a large prime number. Obviously,

$$T_{r \cdot s}(x) = T_r(T_s(x)) = T_s(T_r(x)). \quad (5)$$

Definition 1. *Semi-group property of Chebyshev polynomials:*

$$\begin{aligned} T_r(T_s(x)) &= \cos(r \cos^{-1}(\cos(s \cos^{-1}(x)))) \\ &= \cos(r \cos^{-1}(x)) \\ &= T_{sr}(x) \\ &= T_s(T_r(x)). \end{aligned}$$

Definition 2. *Given x and y , it is intractable to find the integer s , such that $T_s(x) = y$. It is called the Chaotic Maps-Based Discrete Logarithm problem (CMBDLP).*

Definition 3. *Given x , $T_r(x)$, and $T_s(x)$, it is intractable to find $T_{rs}(x)$. It is called the Chaotic Maps-Based Diffie-Hellman problem (CMBDHP).*

2.2 Review of Liu et al.'s Protocol [5]

Assume that the user A and the server S share the hash value $h_{pw} = H(ID_A || PW_A)$ of A's password PW_A and A's identification ID_A . The hash value of the user's password is required to be stored in the server. Figure 1 shows the main process of Liu et al.'s protocol.

- 1) User A \rightarrow Server S: $\{ID_A, N_1, r_a, T_1, T_2\}$.

User A generates a random number $r_a \in [-1, 1]$, a random integer r and a timestamp value N_1 , then computes $T_r(r_a)$. Next, A computes the functions T_1 and T_2 as follows: $T_1 = H(h_{pw} || r_a || N_1) \oplus H(T_r(r_a))$, $T_2 = H(H(T_r(r_a)))$.

- 2) Server S \rightarrow User A: $\{r_b, T_3, H(T_s(r_a))\}$.
After receiving the message, the server first verifies the timeliness of it: timestamp whether the N_1 in the received message is in a permitted time window. If not, the server S stops here. Otherwise, S goes on to take out his own copy of h_{pw} by using the index " ID_A ," and computes the function K_{B_1} as follows: $K_{B_1} = H(h_{pw} || r_a || N_1)$. Then S computes the function $K_{B_1} \oplus T_1$ to get $X_1 (= H(T_r(r_a)))$ and further verifies whether $H(X_1) = T_2$. If not, B stops here; otherwise, B generates a random number $r_b \in [-1, 1]$ and a random integer s . Next S computes the function $T_s(r_a)$. Then S computes the functions T_3 and T_4 as follows: $T_3 = H(h_{pw} || r_a || r_b) \oplus T_s(r_a)$, $T_4 = H(T_s(r_a))$.
- 3) User A \rightarrow Server S: $\{T_5\}$.
After receiving the message, User A computes the function $K_A = H(h_{pw} || r_a || r_b)$. Then A computes the function $K_A \oplus T_3$ to get the value of $X_2 (= (r_a))$ and verifies whether $H(X_2)$ is equal to the received T_4 . If not, A stops here; otherwise, the server S is authenticated. After that, A computes the function $T_5 = H(h_{pw} \oplus r_b) \oplus T_r(r_a)$. Finally, A sends T_5 to S.
- 4) After receiving the message, the server S computes $K_{B_2} = H(h_{pw} \oplus r_b)$. Then S computes the function $K_{B_2} \oplus T_5$ to get the value of T_2 which is received in (1). If not, B stops here; otherwise, the user A is authenticated.
- 5) Respectively, A and S can calculate the share session key $K_{session} = T_r(T_s(r_a)) = T_s(T_r(r_a)) = T_{rs}(r_a)$.

2.3 Security of Liu et al.'s Protocol [5]

- 1) Fails to Prevent Password Guessing Attacks for privileged-insider of the server S.
In real environments, the user Alice may register with a number of servers by using a common password PW_A and the identity ID_A for his/her convenience. Thus, the privileged-insider of server may try to use the knowledge of user's identity and PW_A to access other servers. The details of password guessing attack in Liu's scheme are described as follows:
Step 1: In Liu's protocol, they assume that the user A and S share the hash value $h_{pw} = H(ID_A || PW_A)$.
Step 2: The privileged-insider of the server S guesses a password PW_A^* and computes $H(ID_A || PW_A^*)$.
Step 3: The privileged-insider of the server S compares $H(ID_A || PW_A^*)$ with h_{pw} .
A match in **Step 3** above indicates the correct guessing of Alice's password and the privileged-insider of server S succeeds to guess the low-entropy password $PW_A^* = PW_A$. Otherwise, the privileged-insider of server S repeats **Step 2**.

Note that above-mentioned steps can be done by off-line manner and Tang et al. [19] have modelled the password guessing attacks can be carried out between the challenger and a polynomial-time attacker.

- 2) Fails to Prevent Off-line Password Guessing Attacks for any adversary.
The details of off-line password guessing attack for any adversary in Liu's scheme are described as follows:
Step 1: In the Liu's protocol, an adversary can get all the transmitting messages, and he records four related messages $\{ID_A, r_b, T_2, T_5\}$.
Step 2: The adversary guesses a password PW_A^* and computes $H(H(ID_A || PW_A^*) \oplus r_b) \oplus T_5$.
Step 3: The adversary compares $H(H(ID_A || PW_A^*) \oplus r_b) \oplus T_5$ with T_2 .
A match in **Step 3** above indicates the correct guessing of Alice's password and the adversary succeeds to guess the low-entropy password $PW_A^* = PW_A$. Otherwise, the adversary repeats **Step 2**. The main reason is that the Liu's protocol has the design defect: Using the transmitting messages, anyone can construct a function which only including one input variable password and a related output T_2 .
- 3) Fails to Prevent Stolen-verifier attacks.
An adversary gets the verifier table from servers by a hacking way, and then the adversary can launch any other attack which called stolen-verifier attacks. There is a verification table in the server side because the server and the user have shared the hash value $h_{pw} = H(ID_A || PW_A)$. The verification table can lead three problems: security of stolen-verifier attack, hard to maintain the verification table and wasting storage space.
- 4) The complications from Off-line Password Guessing Attacks.
Firstly, if an adversary gets many passwords of users by launching off-line password guessing attacks, he can also carry out DoS (Denial of Service) attacks. Secondly, the adversary can initiate impersonation attack to cheat a legal user by playing the server S, or cheat the server S by playing the legal user. Thirdly, the adversary may be eavesdropping all the time while hiding the case of the password leaking just for getting some important information.
- 5) PLXO (Potential Loophole of XOR Operation) [20].
First of all, there exists a kind of Potential Loophole about using with \oplus in the whole Lu's scheme. The XOR operation must assure the same binary digits on both sides of.

Assume that $t = a \oplus b$, a is short and b is long. So there are three scenarios as follows:

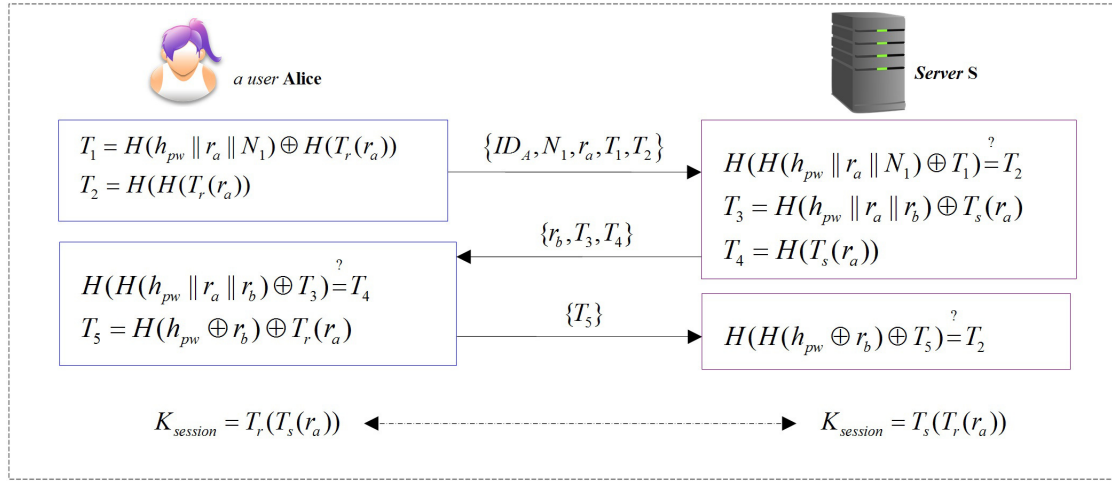


Figure 1: The process of Liu et al.'s protocol

Case 1: Extended a .

However, a may be the ID of user (such as in literature [5]), so the ID of user is not practical and friendly enough.

Case 2: Shorten b .

However, b may be a random number (such as in literature [5]), if b is shortened, it can be easily guessed. And if the protocol transmits a (may be the ID) in plaintext, anyone will get the b .

Case 3: Pad a .

Definition 4. (*Leak attack.*) *Leak attack is a kind of intercept attack that the attackers use various technologies to obtain the useful information from the messages eavesdropped from public channels.*

Definition 5. (*XOR with pad operation leaking attack.*) *This kind of attack is due to use XOR operation in a wrong way, which will lead to leak some sensitive information, and finally an adversary can get part of useful information, even the session key is not being detected. In literature [5], Trudy can launch a XOR with pad operation leaking attack.*

For pad a method, on one side, according to Kerckhoffs's principle: A cryptosystem should be secure even if everything about the system, except the key, is public knowledge. On the other side, the opposite peer must know the pad algorithm in order to decrypt the XORed cipher text. Based on above-mentioned, the pad method/algorithm must be opened, then $t = (a \parallel pad) \oplus b$, and the values of a and b must be strictly private.

For example, we consider $T_5 = H(h_{pw} \oplus r_b) \oplus T_r(r_a)$, and we assume that the $H(h_{pw} \oplus r_b)$ has l bits, $T_r(r_a)$ has m bits. The leaking bits are $(m - l)$ bits (assume $(m - l)$). The shorter of the $H(h_{pw} \oplus r_b)$, the more of leaking information about $T_r(r_a)$. The Figure 2 shows that partial of $T_r(r_a)$ will be leak.

3 The Improved Two-party PAKA Protocol with Privacy Protection

In this section, we give an improved chaotic maps-based password-authentication key agreement scheme which consists of three phases: user registration phase, the improved two-party PAKA with privacy protection phase, password changing phase.

Table 2 is the notations used in this paper.

Table 1: Notations

Symbol	Definition
ID_A, ID_S	The identities of the user and the server, respectively
PW_A	The password of the user (Alice)
R, a, b	Random numbers
$(x, T_k(x))$	Public key based on Chebyshev chaotic maps for the server
k	Secret key based on Chebyshev chaotic maps for the server
H	A secure one-way hash function
\parallel	concatenation operation
T	Timestamp

3.1 User Registration Phase

Figure 3 illustrates the user registration phase.

1) User A \rightarrow Server S: $\{ID_A, H(R \parallel PW_A)\}$.

When a user wants to be a new legal user, she chooses her identity ID_A , a random number R , and computes $H(R \parallel PW_A)$. Then Alice submits $ID_A, H(R \parallel PW_A)$ to the S via a secure channel.

2) Server S \rightarrow User A: B .

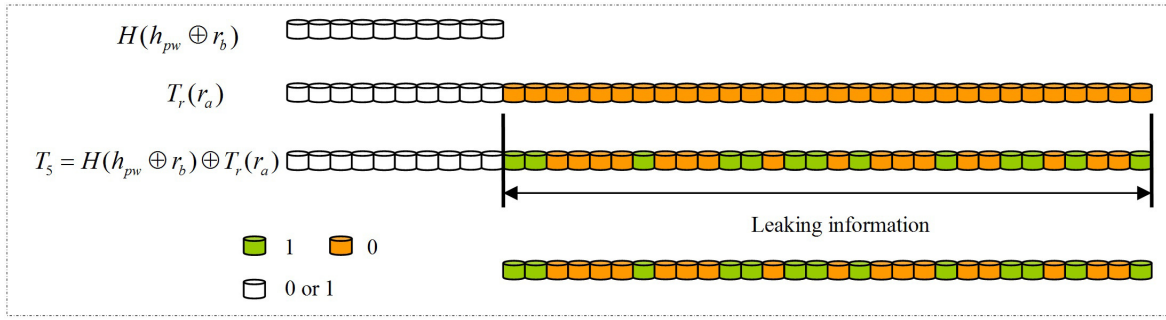


Figure 2: The process of how to leak some information

Upon receiving $ID_A, H(R||PW_A)$ from Alice, the S computes $B = H(ID_A||k) \oplus H(R||PW_A)$, where k is the secret key of the server S. Then Alice stores $\{R, B\}$ in a secure way.

3.2 The Improved Two-party PAKA with Privacy Protection Phase

This concrete process is presented in the following Figure 4.

- 1) User A \rightarrow Server S: $\{T_a(x), C_1, C_2\}$.
If Alice wishes to consult some personal issues establish with S in a anonymous way, she will input password and compute $B^* = B \oplus H(R||PW_A)$, and then choose a random integer number a and compute $T_a(x)$, $C_1 = T_a T_k(x)(ID_A||T)$, $C_2 = H(B^*||C_1||ID_S)$. After that, Alice sends $\{T_a(x), C_1, C_2\}$ to S where she wants to get the server's service.
- 2) Server S \rightarrow User A: $\{T_k(b), C_3, C_4\}$.
After receiving the message $\{T_a(x), C_1, C_2\}$, S firstly must confirm the identity of this message and check the timestamp. So based on the private key k , S computes $C_1/T_k T_a(x) = ID_A||T$ to get the source of this message and timestamp. If T is passed validation, S will compute $B^* = H(ID_A||k)$ and verifies $H(B^*||C_1||ID_S) \stackrel{?}{=} C_2$. If above equation holds, that means Alice is a legal user, or S will abort this process. After authenticating Alice, S chooses a random b and computes $C_3 = T_k T_a(x)b$, $C_4 = H(B^*||T_k(b)||T)$. Finally S sends $\{T_k(b), C_3, C_4\}$ to Alice.
- 3) User A \rightarrow Server S: $\{C_5, C_6\}$.
Because $T_a T_k(x)$ has already computed before, Alice can get $b = C_3/T_a T_k(x)$ directly. Next, Alice computes $H(B^*||T_k(b)||T)$ and verifies $H(B^*||T_k(b)||T) \stackrel{?}{=} C_4$. If above equation holds, that means S is a legal server, or Alice will abort this process. After authenticating S, Alice computes $C_5 = T_a T_k(x)T_a(b)$, $C_6 = H(T_a(b))$ and sends

$\{C_5, C_6\}$ to S. Finally, Alice computes the session key $K_{session} = T_a(T_k(b))$ locally.

- 4) After receiving the message $\{C_5, C_6\}$, S computes $T_a(b) = C_5/T_k T_a(x)$ and verifies $H(T_a(b)) \stackrel{?}{=} C_6$. If above equation holds, S will compute the session key $K_{session} = H(T_k(T_a(b)))$ locally.

3.3 Password Changing Phase

Figure 5 illustrates the password changing phase.

- 1) User A \rightarrow Server S: $\{T_a(x), C_1, C_2, C_3\}$.
When Alice wants to change her password, she chooses PW'_A , two random numbers R', a and computes $B^* = B \oplus H(R||PW_A)$, $T_a(x)$, $C_1 = T_a T_k(x)(ID_A||T)$, $C_2 = B^* \oplus H(R'||PW'_A)$, $C_3 = H(B^*||C_1||C_2)$. Then Alice sends $\{T_a(x), C_1, C_2, C_3\}$ to the S.
- 2) Server S \rightarrow User A: $\{C_4, C_5\}$.
Upon receiving $\{T_a(x), C_1, C_2, C_3\}$ from Alice, firstly must confirm the identity of this message and verify timestamp. So based on the private key k , S computes $C_1/T_k T_a(x) = ID_A||T$ to get the source of this message and timestamp. If T is passed validation, S computes $B^* = H(ID_A||k)$ and verifies $H(B^*||C_1||C_2) \stackrel{?}{=} C_3$. If above equation holds, that means Alice is a legal user, or S will abort this process. After authenticating Alice, S computes

$$\begin{aligned} H(R'||PW'_A) &= C_2 \oplus B^*, B' \\ &= H(ID_A||k) \oplus H(R'||PW'_A), \\ C_4 &= T_k T_a(x)B', \\ C_5 &= H(B'||T), \end{aligned}$$

and sends $\{C_4, C_5\}$ to Alice.

- 3) After receiving the message $\{C_4, C_5\}$, Alice computes stores $B' = C_4/T_a T_k(x)$ and verifies $H(B'||T) \stackrel{?}{=} C_5$. If above equation holds, Alice will store $\{R, B\}$ in a secure way.

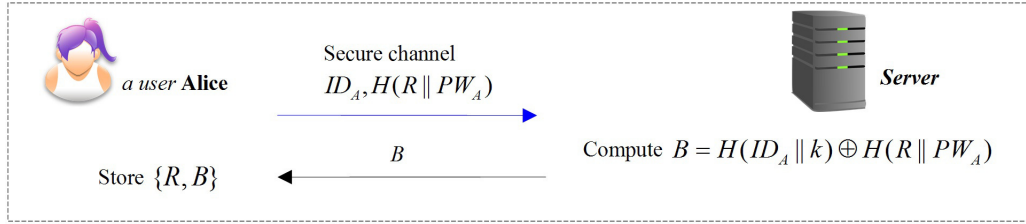


Figure 3: User registration phase

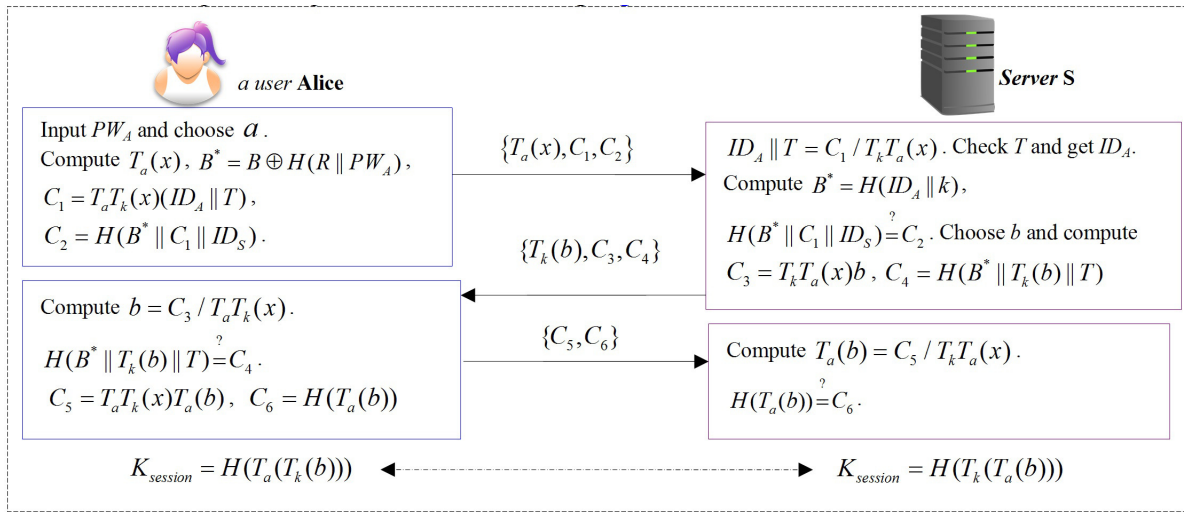


Figure 4: The improved two-party PAKA with privacy protection

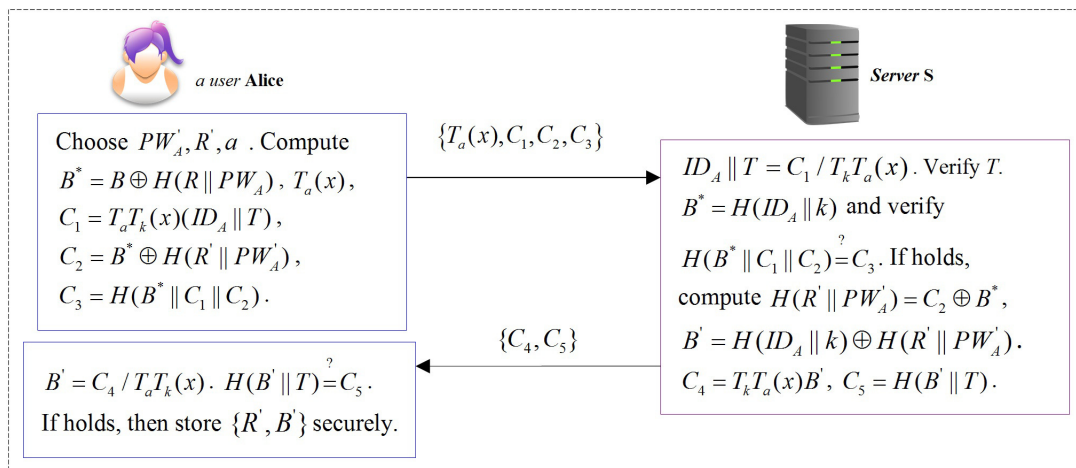


Figure 5: Password changing phase

4 Security Analysis

4.1 Security Proof Based on the BAN Logic [21]

For convenience, we first give the description of some notations (Table 2) used in the BAN logic analysis and define some main logical postulates (Table 3) of BAN logic.

According to analytic procedures of BAN logic and the requirement of deniable scheme, our NIDA scheme should satisfy the following goals in Table 4.

First of all, we transform the process of our protocol (The improved two-party PAKA with privacy protection phase) to the following idealized form.

(Alice \rightarrow Server) C_1 : Server $\triangleleft T_a(x)$, $T_a T_k(x)(ID_A || T)$,
($B^* || T_a T_k(x)(ID_A || T) || ID_S$);

(Server \rightarrow Alice) C_2 : Alice $\triangleleft T_k(b)$, $T_k T_a(x)b$, ($B^* || T_k(b) || T$);

(Alice \rightarrow Server) C_3 : Server $\triangleleft T_a T_k(x)T_a(b)$, ($T_a(b)$).

According to the description of our protocol, we could make the following assumptions about the initial state, which will be used in the analysis of our protocol in Table 5.

Based on the above assumptions, the idealized form of our protocol is analyzed as follows. The main steps of the proof are described as follows:

For C_1 : According to the ciphertext C_1 and P_4, P_7 and attributes of chaotic maps, and relating with R_1 , we could get:

S_1 : **Server** $| \equiv$ **Alice** $| \sim C_1$.

Based on the initial assumptions P_2, P_4 , and relating with R_2 , we could get:

S_2 : **Server** $| \equiv \#C_1$.

Combine $S_1, S_2, P_2, P_4, P_7, R_3$ and attributes of chaotic maps, we could get:

S_3 : **Server** $| \equiv \#ID_A, T_a(x)$, ($B^* || T_a T_k(x)(ID_A || T) || ID_S$).

Based on R_5 , we take apart S_3 and get:

S_4 : **Server** $| \equiv \#ID_A$, S_5 : **Server** $| \equiv \#T_a(x)$.

Combine S_3, S_4 and attributes of chaotic maps, we can get the fresh and privacy protection about Alice's identity. Combine S_5 and attributes of chaotic maps, we can authenticate the message $T_a(x)$ is fresh and comes from Alice exactly.

For C_2 : According to the ciphertext C_2 and P_1, P_5, P_6 and attributes of chaotic maps, and relating with R_1 , we could get:

S_6 : **Alice** $| \equiv$ **Server** $| \sim C_2$.

Based on the initial assumptions P_3, P_5 , and relating with R_2 , we could get:

S_7 : **Alice** $| \equiv \#C_2$.

Combine $S_6, S_7, P_3, P_5, P_6, R_3$ and attributes of chaotic maps, we could get:

S_8 : **Alice** $| \equiv \#T_k(b)$, ($B^* || T_k(b) || T$).

Based on R_5 , we take apart S_8 and get:

S_9 : **Alice** $| \equiv \#T_k(b)$, S_{10} : **Alice** $| \equiv \#(B^* || T_k(b) || T)$.

Combine S_8, S_9 and attributes of chaotic maps, we can get the fresh and privacy protection about $T_k(b)$. Combine S_{10} and attributes of secure chaotic maps-based hash function, we can authenticate the message $T_k(b)$ comes from Server exactly.

For C_3 : According to the ciphertext C_3 and P_7 and attributes of chaotic maps, and relating with R_1 , we could get:

S_{11} : **Server** $| \equiv$ **Alice** $| \sim C_3$.

Based on the initial assumptions P_2, P_4 , and relating with R_2 , we could get:

S_{12} : **Server** $| \equiv \#C_3$.

Combine $S_{11}, S_{12}, P_2, P_4, P_7, R_3$ and attributes of chaotic maps, we could get:

S_{13} : **Server** $| \equiv \#T_a(b)$, ($T_a(b)$).

Based on R_5 , we take apart S_3 and get:

S_{14} : **Server** $| \equiv \#T_a(b)$, S_{15} : **Server** $| \equiv \#(T_a(b))$.

Combine S_{13}, S_{14} and attributes of chaotic maps, we can get the fresh and privacy protection about $T_a(b)$. Combine S_{15} and attributes of secure chaotic maps-based hash function, we can authenticate the message $T_a(b)$ comes from Server exactly.

Combination:

Because Alice and Server communicate each other just now, they confirm the other is on-line. Moreover, since Server can get ID_A from the $T_a T_k(x)(ID_A || T)$ with his own secret key, and based on $S_4, S_5, S_{14}, S_{15}, R_4$ with chaotic maps problems, we think that the server could get the session key $K_{session} = H(T_k(T_a(b)))$ and Goal 3. $Server \equiv (Server \xrightarrow{K_{session}} Alice)$, Goal 4. $Server | \equiv Alice | \equiv (Server \xrightarrow{K_{session}} Alice)$. At the same way, based on S_9, S_{10}, R_4 with chaotic maps problems, we think that Alice could get the session key $K_{session} = T_a(T_k(b))$ and Goal 1. $Alice | \equiv (Alice \xrightarrow{K_{session}} Server)$, Goal 2. $Alice | \equiv Server | \equiv (Alice \xrightarrow{K_{session}} Server)$.

4.2 Resistance to Possible Attacks

In this section, we analyze the process of security proof privacy protection, Resistance to stolen-verifier attacks, Impersonation attack, Man-in-the-middle attack, Replay attack, Known-key security, Perfect forward secrecy and Guessing attacks (On-line or off-line) respectively.

Table 2: Notations of the BAN logic

Symbol	Definition
$P \equiv X$	The principal P believes a statement X , or P is entitled to believe X .
$\#(X)$	The formula X is fresh.
$P \Rightarrow X$	The principal P has jurisdiction over the statement X .
$P \triangleleft X$	The principal P sees the statement X .
$P \sim X$	The principal P once said the statement X .
(X, Y)	The formula X or Y is one part of the formula (X, Y) .
$\langle X \rangle_Y$	The formula X combined with the formula Y .
$\{X\}_Y$	The formula X is encrypted under the key Y .
$(X)_Y$	The formula X is chaotic maps-based hash function with the key Y .
$P \xleftrightarrow{K} Q$	The principals P and Q use the shared key K to communicate. The key K will never be discovered by any principal except P and Q .
$\xrightarrow{K} P$	The public key of P , and the secret key is described by K^{-1} .

Table 3: Logical postulates of the BAN logic

Symbol	Definition
$\frac{P \equiv P \xleftrightarrow{K} Q, P \{X\}_K}{P \equiv Q \sim X}$	The message-meaning rule (R_1)
$\frac{P \equiv \#(X)}{P \equiv \#(X, Y)}$	The freshness-conjunction rule (R_2)
$\frac{P \equiv \#(X), P \equiv Q \sim X}{P \equiv Q \equiv X}$	The nonce-verification rule (R_3)
$\frac{P \equiv Q \Rightarrow X, P \equiv Q \equiv X}{P \equiv X}$	The jurisdiction rule (R_4)
$\frac{P \equiv Q \equiv (X, Y)}{P \equiv Q \equiv X}$	The belief rules (R_5)
Remark 3: Molecule can deduce denominator for above formulas.	

Table 4: Goals of the proposed scheme

Goals	
Goal 1. $Alice \equiv (Alice \xleftrightarrow{K_{session}} Server)$;	Goal 2. $Alice \equiv Server \equiv (Alice \xleftrightarrow{K_{session}} Server)$;
Goal 3. $Server \equiv (Server \xleftrightarrow{K_{session}} Alice)$;	Goal 4. $Server \equiv Alice \equiv (Server \xleftrightarrow{K_{session}} Alice)$;

Table 5: Assumptions about the initial state of our protocol

Initial states	
$P_1 : Alice \equiv \xrightarrow{T_k(x)} Server$	
$P_2 : Server \equiv Server \xleftarrow{B^*} Alice$	$P_3 : Alice \equiv Server \xleftarrow{B^*} Alice$
$P_4 : Alice \equiv \#(a)$	$P_5 : Server \equiv \#(b)$
$P_6 : Alice \equiv Alice \xrightarrow{T_a T_k(x)} Server$	$P_7 : Server \equiv Alice \xrightarrow{T_k T_a(x)} Server$

Table 6: Security of our proposed protocol

	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14
[5](2010)	No	Mutual	No	No	Yes	Yes	No	Yes	Yes	No	No	No	No	No
[7](2015)	No	Mutual	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No
[8](2015)	No	Mutual	No	No	Yes	Yes	Yes	Yes	No	No	No	No	No	No
Ours	Yes	Mutual	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	BAN	Yes
S1: Single registration; S2: Authentication; S3: Privacy protection; S4: Resistance to stolen-verifier attack; S5: Resistance to impersonation attack; S6: man-in-the-middle attack; S7: Resistance to replay attack; S8: Known-key security; S9: Perfect forward secrecy; S10: Guessing attacks (On-line or off-line) (Including Prevent Password Guessing Attacks for privileged-insider or for any adversary) S11: Resistance to Potential Loophole of XOR Operation; S12: Update password phase S13: Formal security proof S14: Hiding timestamp Yes/No: Support/Not support														

Privacy protection. The node which possesses the secret key k can compute $T_k T_a(x)$ and get the user's ID, so only the server knows the identity of the user. Furthermore, only the user and the server can compute the B^* , so the user need not get the plaintext of identity of the server and convinces the peer is the server.

Resistance to stolen-verifier attacks. In the proposed scheme, the server side need not maintain any verification table. Thus, the stolen-verifier attack is impossible to initiate in the proposed scheme.

Impersonation attack. An adversary cannot impersonate anyone of the user and the server. The B^* and the secret key k can achieve authentication and confidentiality. The $\{a, b, T\}$ can achieve freshness and associativity of all the transmissive messages. So there is no way for an adversary to have a chance to carry out impersonation attack. Furthermore, because Alice is an identity hiding and legal user, an adversary can not impersonate Alice at all.

Man-in-the-middle attack. Because $C_i (1 \leq i \leq 6)$ contain the participants's identities, timestamp or nonces and The $\{a, b, T\}$ can achieve freshness and associativity of all the transmissive messages, a man-in-the-middle attack cannot succeed.

Replay attack. That any message of Alice was replayed by an adversary is meaningless. Because Alice is an ID hiding user, the adversary only can create a vision user to initiate the replay attack. Moreover the $\{a, b, T\}$ can achieve freshness and associativity of all the transmissive messages.

Known-key security. Since the session key $SK = T_a T_k(b) = T_k T_a(b)$ is depended on the random nonces a and b , and the generation of nonces is independent in all sessions, an adversary cannot compute the previous and the future session keys when the adversary knows one session key. And in the password update

phase, any session key is only used once, so it has known-key security attribute.

Perfect forward secrecy. In the proposed scheme, the session key $SK = T_a T_k(b) = T_k T_a(b)$ is related with a and b , which were randomly chosen by Alice and the server S respectively. Because of the intractability of the chaotic maps problems, an adversary cannot compute the previously established session keys.

Guessing attacks (On-line or off-line). Any transferred messages on the public channel have not password involved, so guessing attacks can not happen.

From the Table 6, we can see that the proposed scheme can provide privacy protection, perfect forward secrecy and so on. As a result, the proposed scheme is more secure and has much functionality compared with the recent related scheme.

5 Efficiency Analysis

Compared to RSA and ECC, Chebyshev polynomial computation problem offers smaller key sizes, faster computation, as well as memory, energy and bandwidth savings. To be more precise, on an Intel Pentium4 2600 MHz processor with 1024 MB RAM, where n and p are 1024 bits long, the computational time of a one-way hashing operation, a symmetric encryption/decryption operation, an elliptic curve point multiplication operation and Chebyshev polynomial operation is 0.0005s, 0.0087s, 0.063075s and 0.02102s separately [22]. Moreover, the computational cost of XOR operation could be ignored when compared with other operations. Table 7 shows performance comparisons between our proposed scheme and the literatures of [3, 4, 5]. we sum up these formulas into one so that it can reflect the relationship among the time of algorithms intuitively. $T_p \approx 10T_m \approx 30T_c \approx 72.6T_s \approx 1263.24T_h$, where: T_p : Time for bilinear pair operation, T_m : Time for a point scalar multiplication operation, T_c : The time for executing the $T_n(x) \bmod p$ in Chebyshev polynomial,

Table 7: Comparisons between our proposed scheme and the related literatures

Protocols(Authentication phase)		[5] (2010)	[7] (2015)	[8] (2015)	Ours
Computation	User	$11T_h + 2T_c + 6T_{xor}$	$6T_h + 2T_c + 1T_{xor}$	$6T_h + 2T_c + 3T_{xor}$	$4T_h + 2T_c + 1T_{xor}$
	Server	$11T_h + 2T_c + 5T_{xor}$	$6T_h + 2T_c + 1T_{xor}$	$6T_h + 2T_c + 4T_{xor}$	$4T_h + 2T_c$
	Total	$22T_h + 4T_c + 11T_{xor} \approx 190.432 T_h$	$12T_h + 4T_c + 2T_{xor} \approx 180.432 T_h$	$12T_h + 4T_c + 7T_{xor} \approx 180.432 T_h$	$8T_h + 4T_c + 1T_{xor} \approx 176.432 T_h$
Communication	Messages	6	2	3	3
	rounds	6	2	3	3
Design	Concise design	No	No	Yes	Yes
	Number of nonces	4	3	4	2
	Model	Random Oracle	Random Oracle	Random Oracle	Random Oracle
T_h : Time for Hash operation T_{xor} : Time for XOR operation T_c : The time for executing the $T_n(x) \bmod p$ in Chebyshev polynomial using the algorithm in literature [9]					

T_s : Time for symmetric encryption algorithm, T_h : Time for Hash operation. As in Table 6 and Table 7, we can draw a conclusion that the proposed scheme has achieved the improvement of both efficiency and security.

6 Conclusion

In the paper, we give four flaws and one loophole in Liu et al.'s scheme, and then propose an improved protocol which amends all the flaws and provides the privacy protection at the same time. But what I want to emphasize is that all the plaintexts, even timestamp, are protect by our proposed scheme for achieving privacy protection, and that is to say, the attacker can get only some ciphertexts but nothing. Finally, after comparing with related literatures respectively, we found our proposed scheme has satisfactory security, efficiency and functionality. Therefore, our protocol is more suitable for practical applications.

Acknowledgments

This work is supported by the Liaoning Provincial Natural Science Foundation of China (Grant No. 201602680).

References

- [1] P. Bergamo, P. D. Arco, A. D. Santis and L. Kocarev, "Security of public-key cryptosystems based on Chebyshev polynomials," *IEEE Transactions on Circuits and Systems*, vol. 52, no. 7, pp. 1382–1393, 2005.
- [2] M. Burrows, M. Abadi and R. Needham, "A logic of authentication," *ACM Transactions on Computer Systems*, vol. 8, no. 1, pp. 18–36, 1990.
- [3] J. Chen, J. Zhou and K.W. Wong, "A modified chaos-based joint compression and encryption scheme," *IEEE Transactions on Circuits and Systems*, vol. 58, no. 2, pp. 110–114, 2011.
- [4] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.
- [5] X. Guo and J. Zhang, "Secure group key agreement protocol based on chaotic hash," *Information Sciences*, vol. 180, no. 20, pp. 4069–4074, 2010.
- [6] C. Kai and W. C. Kuo, "A new digital signature scheme based on chaotic maps," *Nonlinear Dynamics*, vol. 74, pp. 1003–1012, 2013.
- [7] T. F. Lee, "Enhancing the security of password authenticated key agreement protocols based on chaotic maps," *Information Sciences*, vol. 290, pp. 63–71, 2015.
- [8] Y. Liu and K. Xue, "An improved secure and efficient password and chaos-based two-party key agreement protocol," *Nonlinear Dynamics*, vol. 84, no. 2, pp. 549–557, 2016.
- [9] L. Kocarev and S. Lian, "Chaos-based cryptography: A brief overview," *IEEE Circuits and Systems Magazine*, vol. 1, no. 3, pp. 6–21, 2002.
- [10] F. Özkaynak, "Cryptographically secure random number generator with chaotic additional input," *Nonlinear Dynamics*, vol. 78, no. 3, pp. 2015–2020, 2014.
- [11] Q. Tang and K. K. R. Choo, "Secure password-based authenticated group key agreement for data-sharing peer-to-peer networks," *Lecture Notes in Computer Science*, vol. 3989, Springer, pp. 162–177, 2006.
- [12] H. R. Tseng, R. H. Jan and W. Yang, "A chaotic maps-based key agreement protocol that preserves user anonymity," in *IEEE International Conference on Communications (ICC'09)*, pp. 1–6, 2009.
- [13] H. Wang, H. Zhang, J. Li and X. U. Chen, "A(3,3) visual cryptography scheme for authentication," *Journal of Shenyang Normal University (Natural Science Edition)*, vol. 31, no. 3, pp. 397–400, 2013.

- [14] X. Wang and J. Zhao, "An improved key agreement protocol based on chaos," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 12, pp. 4052–4057, 2010.
- [15] D. Xiao, X. Liao and S. Deng, "A novel key agreement protocol based on chaotic maps," *Information Sciences*, vol. 177 no. 4, pp. 1136–1142, 2007.
- [16] S. J. Xu, X. B. Chen, R. Zhang, Y. X. Yang and Y. C. Guo, "An improved chaotic cryptosystem based on circular bit shift and XOR operations," *Physics Letters A*, vol. 376, no. 10, pp. 1003–1010, 2012.
- [17] L. Zhang, "Cryptanalysis of the public key encryption based on multiple chaotic systems," *Chaos Solitons Fractals*, vol. 37, no. 3, pp. 669–674, 2008.
- [18] H. F. Zhu, "Cryptanalysis and provable improvement of a chaotic maps-based mobile dynamic ID authenticated key agreement scheme," *Security and Communication Networks*, vol. 8, no. 17, pp. 2981–2991, 2015.
- [19] H. F. Zhu, "Flexible and password-authenticated key agreement scheme based on chaotic maps for multiple servers to server architecture," *Wireless Personal Communications*, vol. 82, no. 3, pp. 1697–1718, 2015.
- [20] H. F. Zhu, "A provable privacy-protection system for multi-server environment," *Nonlinear Dynamics*, vol. 82, no. 1, pp. 835–849, 2015.
- [21] H. F. Zhu, "A provable one-way authentication key agreement scheme with user anonymity for multi-server environment," *KSII Transactions on Internet And Information Systems*, vol. 9, no. 2, pp. 811–829, 2015.
- [22] H. F. Zhu, "Sustained and authenticated of a universal construction for multiple key agreement based on chaotic maps with privacy preserving," *Journal of Internet Technology*, vol. 17, no. 5, pp. 1–10, 2016.

Biography

Hongfeng Zhu obtained his Ph.D. degree in Information Science and Engineering from Northeastern University. Hongfeng Zhu is a full associate professor of the Kexin software college at Shenyang Normal University. He is also a master's supervisor. He has research interests in wireless networks, mobile computing, cloud computing, social networks, network security and quantum cryptography. Dr. Zhu had published more than 50 international journal papers (SCI or EI journals) on the above research fields.

Yifeng Zhang he is an undergraduate from Shenyang Normal University, major in information security management. In the four years of college, after completing her studies, he enjoys reading the book related to this major. Under the guidance of the teacher, he has published four articles in EI journals.

Pre-image Resistant Cancelable Biometrics Scheme Using Bidirectional Memory Model

Mayada Tarek¹, Osama Ouda², and Taher Hamza¹

(Corresponding author: Mayada Tarek)

Department of Computer Science, Faculty of Computer and Information Sciences, Mansoura University¹

Department of Information Technology, Faculty of Computer and Information Sciences, Mansoura University²

El Gomhouria St, Mansoura, Dakahlia Governorate 35516, Egypt

(Email: mayaatarek@yahoo.com)

(Received Feb. 19, 2016; revised and accepted June 13 & July 19, 2016)

Abstract

Cancelable biometrics is a promising template protection scheme which relies on encoding the raw biometric data using non-invertible transformation function. Existing cancelable biometrics schemes ensure recoverability of compromised templates as well as users' privacy. However, these schemes cannot resist pre-image attacks. In this article, a pre-image resistant cancelable biometrics scheme is proposed, where associative memory is utilized to encode the cancelable transformation parameters with the privilege of high recognition performance. Bidirectional memory model has been suggested to memorize each user's associated key using his biometric data based on association connectors. These connector values can be safely saved in the storage along with the cancelable biometric template. The cancelable template is generated using XOR operation between the biometric data and the associated key. The simulated experiments conducted on CASIA-IrisV3-Interval dataset show that the presented resistant scheme does not affect the classification power of the raw biometric data significantly. Moreover, the resistance of the presented scheme against complete or approximate disclosure of the raw biometric template is achieved.

Keywords: *Bidirectional memory model (BAM), cancelable biometrics, pre-image attacks*

1 Introduction

Recently, protection schemes for biometrics data have gained a lot of interest because of the spread use of biometric data [7] instead of password or smart card for authenticating individuals [13, 15]. Ensuring the proper use of biometric data, that are saved in system storage as templates, is a key concern of any biometrics-based authentication system. Therefore, template protection schemes are needed for protecting these stored biometric

templates [7, 20]. Cancelable biometrics (CB) is a promising protection scheme for biometric data designed to store a distorted version, called the cancelable template, of the raw biometric data. The cancelable template is obtained using a non-invertible transformation function and stored, instead of the genuine biometric data, in the system storage [23]. It should be computationally hard to reconstruct the genuine biometric data when cancelable templates are compromised [20].

Over the past few years, various cancelable biometric methods have been presented. Ratha et al. [24, 25] proposed a cancelable scheme for fingerprints using three different transformation named (cartesian, polar and functional). In [4], a data hiding approach is used for iris template protection. Zuo et al. [36] and Rathgeb et al. [29] suggested creating a cancelable template from iris by applying row permutation to iris code. In [17], a random key is employed to convert an on-line signature data into discrete sequences that are convolved together to create the cancelable template. In [2], a new protection scheme for signatures based on homomorphic probabilistic encryption for fixed-length templates is proposed. Savvides et al. [30] proposed a cancelable biometrics filters for face recognition where different templates could be obtained from the face images by varying a random key which acts as filter. The main challenge of these cancelable biometric schemes is the significant degradation in recognition performance achieved using the genuine (unprotected) biometric systems.

Another cancelable biometrics approach has been presented by Teoh et al. [31, 33, 34] in order to increase the recognition accuracy of cancelable biometric templates. They proposed to employ a secret random number to project the raw biometric features into transformed templates. The scheme has been applied to different types of biometric modalities (e.g. [3, 16]). Rathgeb et al. [26, 27, 28] utilized Bloom filter to construct cancelable templates from iris codes. The scheme provides a rapid comparison among transformed templates using Bloom

filters as a non-invertible transform. Ouda et al. [21, 22] proposed a tokenless cancelable biometrics scheme for protecting iris codes. The scheme relies on mapping fixed-size groups of bits in an iris code into random bits using the concept of Boolean functions.

Although the complexity of reconstructing the genuine data from the cancelable templates in existing schemes is computationally as hard as random guessing, pre-images can be easily constructed from the stored cancelable templates which make these schemes vulnerable to some security breaches [9, 12, 14]. A pre-image attack aims to construct a non-genuine biometric data, which could be completely different from the genuine data but could generate a cancelable template similar to the cancelable template produced from the genuine biometric data [19].

Recently, Mayada et al. [32] proposed a novel cancelable biometrics scheme that can resist pre-image attacks. However, the recognition accuracy of their scheme is noticeably affected as a result.

In this paper, we propose a pre-image resistant cancelable biometric scheme that can pertain the recognition accuracy of the original biometric system. The proposed scheme binds biometric features and their associated cancelable transformation parameter in an associative memory model. Bidirectional associative memory (BAM) is employed in order to bind each user biometric features with his transformation key through some connector information. These connectors act as an encoded representation of a user's key and its associated biometric data as well. It is safe to store these connectors on the system storage with the cancelable transformed template. The cancelable transformation in this proposed resistant scheme is a simple XOR operation between biometric template and the associated key in order to achieve high recognition performance. Since XOR is a non-invertible operation if only the result is known, the security against pre-image attacks is guaranteed because it is infeasible to extract genuine or even an approximate values for biometric data or its associated key utilizing the compromised connectors. During authentication, the stored connectors are utilized to apply the mapping process in order to recall the associated key using input biometric data, then the cancelable template is created to be compared with the stored one.

The remainder of this article is organized as follows: the proposed resistant scheme is presented in the next section. A security analysis of the proposed scheme is given in Section 3. Experimental results are presented in Section 4, and Section 5 concludes the paper.

2 Proposed Scheme

The proposed resistant scheme focuses on producing a cancelable biometric template which withstands the pre-image attacks and also achieves high recognition performance. Most of cancelable biometric schemes suffer from the possibility of constructing an approximate biometric

features, also known as a biometric template, using the stored cancelable template if system storage is compromised [20]. This paper introduces a cancelable scheme which employs the Boolean XOR operation for implementing the cancelable transformation function. Each binary biometric template is XOR-ed with an associated random binary string to construct a cancelable template. Storing this random bit-string in the system storage or on smart cards makes biometric system susceptible to different types of attacks [8, 10]. To tackle this challenge, our proposed scheme relies on hiding the user's associated bit-string (key) along with the biometric features in an encrypted form using an associative memory. If only the resulting XOR-ed template is compromised by any attacker, the XOR operation cannot be inverted (e.g. '0' can result from '1' XOR '1' or '0' XOR '0'). The associative memory binds every biometric features with its corresponding key through association connectors known as weights. These weights could be securely stored on a central storage to recall the associated key using user's biometric features in the verification stage. The steps of our proposed resistant scheme are illustrated in Figure 1.

As depicted in Figure 1, the proposed cancelable scheme is formulated of two principle processes: firstly, constructing the BAM network weights. These weights values are utilized to connect each user associated key to its biometric data. Secondly, binding biometric template with the key in order to construct the reference cancelable template; this process is accomplished using XOR binding operation. The next subsections illustrate our proposed resistant scheme in detail.

2.1 Enrollment Process

When a new user is enrolled, a reference binary-valued template is generated using all enrolled user's samples. This reference sample is computed by calculating the mean of every bit location from all samples. If this mean value is more than or equals 0.5 then this location reference set to 1 and 0 otherwise. Algorithm 1 presents the enrollment process in detail.

Instead of storing the key associated with each user in the storage or on a token, an associative memory is utilized in order to bind each key with the corresponding biometric template. During the association phase, an associative network weights are learned for each user. During the memorization phase of BAM, an input set of p associated pattern pairs is given: $\{(X_r, Y_r) | r = 1, 2, \dots, p\}$: $X_r \in \{-1, +1\}^n$ (represent biometric template) and $Y_r \in \{-1, +1\}^n$ (represent transformation key), where bipolar representation is utilized to allow optimum patterns association [1, 35]. Out of the complete set of input patterns, only a single pattern should represent the genuine individual's biometric template binding to a genuine individual's key. Other patterns should represent non-genuine biometric templates linked to non-genuine transformation keys. In order to ensure perfect memory mapping, the other (non-genuine) patterns have to be independent from

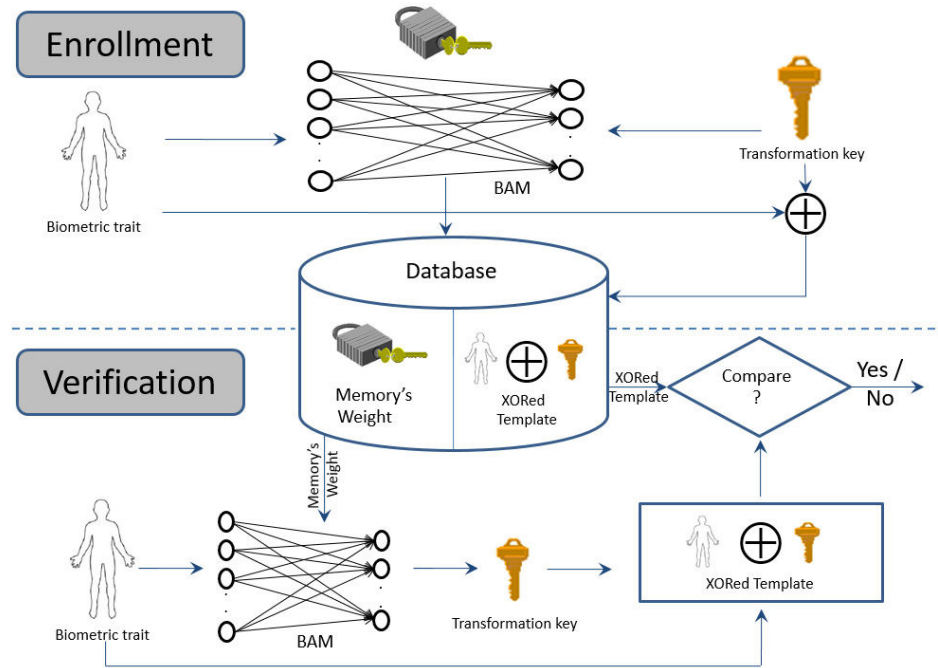


Figure 1: Overview of proposed pre-image resistant cancelable biometric scheme

the user's reference pattern. A bidirectional single layer memory network is utilized to associate two different patterns. The presented BAM model consists of an input unit of n nodes corresponding to biometric features of length n . The input layer nodes are linked to an output layer consisting of n nodes which represents a randomly constructed key of length n through W (weight matrix of size $n \times n$). The weight matrix represents an encoded representation of the cancelable transformation parameters.

In order to construct a protected non-invertible and pre-image resistant cancelable biometric template, a revocable (cancelable) transformation is needed. In our proposed method, the revocable transformation is implemented using the XOR binding operation. The proposed association model ensures that without having the biometric data, it is computationally hard to reveal any information about the genuine transformed key utilizing the stored connection weights as we will show formally in Section 3. Moreover, it is very difficult to construct an approximate version of the biometric template which can be used to produce an approximate version of the XORed cancelable template without knowing the genuine associated key value.

2.2 Verification Process

In the verification phase, the biometric features of each user are utilized to recall his/her associated key utilizing the stored BAM weights. Due to the intra-user variations of biometric data, biometric data generated from the same individual are not the same. Fortunately, however, the

presented BAM model is able to recall the stored associated key binding with the individual's biometric data [35]. Algorithm 2 illustrates the verification process in detail.

The key linked to the claimed identity is XOR-ed with the binary represented biometric data to get the cancelable template. The obtained template is matched against the stored one using the Hamming distance and the authentication process fails if the matching result exceeds a predefined threshold θ and succeeds otherwise.

3 Security Analysis

This section discusses the security properties of our proposed scheme. A secure cancelable biometrics scheme must fulfill a number of requirements; namely, diversity, revocability, non-invertability, and resistance to pre-image attacks. In the next subsections, we show how our proposed scheme can meet these requirements.

3.1 Recoverability and Diversity

The cancelable scheme is revocable if it allows generation of a new key, in case the system storage is compromised, to construct a new template for biometric data belonging to same identity. In our proposed work, the transformation random key is set in BAM network's output layer. Thus, with the possibility of constructing a new key, a new weight matrix could be generated utilizing the same individual's biometric data. Therefore, our proposed scheme satisfies the revocability property.

Algorithm 1 Proposed scheme enrollment stage

Input: A set of L training samples $\{s_1, \dots, s_L\}$ that belongs to the same class. P , number of associated patterns pairs (X, Y) .

- 1: Generate binary representation templates $\{B_1, \dots, B_L\}$ from the training samples with n -bit length.
- 2: Create the reference template B_{ref} for the binary representation training templates using the fusion approach [6] computed by:

$$\phi(i) = \frac{1}{L} \sum_{l=1}^L B_l^i \quad (1)$$

$$B_{ref}(i) = \begin{cases} 1, & \text{if } \phi(i) \geq 0.5 \\ 0, & \text{if } \phi(i) < 0.5 \end{cases} \quad (2)$$

- 3: Convert B_{ref} into bipolar representation X_{ref} .
- 4: Generate random binary sequence K_{ref} with n bits length.
- 5: Convert K_{ref} into bipolar representation Y_{ref} .
- 6: Generate the cancelable template:

$$T_{ref} = B_{ref} \oplus K_{ref} \quad (3)$$

- 7: Generate a set of associated patterns pairs (X_j, Y_j) :
- 8: $J = 2$
- 9: **while** $j \neq P$ **do**
- 10: Select sample B_j from samples belong to other classes then convert it to bipolar representation X_j .
- 11: Generate the associated random bipolar sequence Y_j .
- 12: **end while**
- 13: Randomize the associated patterns pairs (X, Y) order.
- 14: Create the association BAM weights W using learning approach defined in [1]:
- 15: $j = 1, W = \phi$
- 16: **while** $j \neq P$ **do**
- 17:

$$w_j = \bar{X}_j \cdot Y_j \quad (4)$$

$$W = W + w_j \quad (5)$$

- 18: **end while**
- 19: Store W and T_{ref} in system storage.

The length of the BAM output layer corresponds to the key length. Hence, if it contains m nodes, it allows for generating 2^m different cancelable template using 2^m different keys for each input user. On the other hand, each individual can be enrolled in different biometric systems with different cancelable templates based on each system unique key. Thus, the property of diversity is also satisfied

Algorithm 2 Proposed scheme verification stage

Input: Test sample S_{test} , and user identity I .

- 1: Generate binary representation template B_{test} from S_{test} with n bits length.
- 2: Convert B_{test} into bipolar representation X_{test} .
- 3: Retrieve the weights matrix W from biometric system storage.
- 4: Recall the binary valued key associated with X_{test} as defined in [1]:

$$K = W \cdot X_{test} \quad (6)$$

$$K_{test} = \begin{cases} 1, & \text{if } k_i \geq 0 \\ 0, & \text{if } k_i < 0 \end{cases} \quad (7)$$

- 5: Compute the cancelable test template:

$$T_{test} = B_{test} \oplus K_{test} \quad (8)$$

- 6: Compare test and reference cancelable template for the input claimed user identity I :

$$\varepsilon = \frac{\|T_{ref} \oplus T_{test}\|}{n} \quad (9)$$

- 7: Decision making for I :

$$\text{Decision} = \begin{cases} \text{Accept,} & \text{if } \varepsilon \leq \theta \\ \text{Reject,} & \text{if } \varepsilon > \theta \end{cases} \quad (10)$$

by our proposed scheme.

3.2 Non-invertability

In order to satisfy the non-invertability property, it should be computationally hard to decrypt the XORed template to retrieve either the genuine key or the genuine biometric data. Moreover, it should difficult to extract the key or the genuine biometric features using the stored BAM weights. The utilized XOR binding operation is non-invertible because it is very difficult to reverse the resulting XORed template without knowing either of its input parameters. The non-invertability of the publicly stored BAM weight matrix is acquired from the method used for generating those weights. As mentioned before in Section 2, the weight matrix is constructed using the approach expressed by Equations (4) and (5). This subsection analyzes the computational efforts needed by an adversary to disclose the genuine data utilizing the stored BAM weights.

$$\begin{bmatrix} w_{1,1} & w_{1,2} & \cdots & w_{1,n} \\ \vdots & \vdots & \ddots & \vdots \\ w_{n,1} & w_{n,2} & \cdots & w_{n,n} \end{bmatrix} = \begin{bmatrix} x_{1,1} \cdot y_{1,1} & x_{1,1} \cdot y_{1,2} & \cdots & x_{1,1} \cdot y_{1,n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{1,n} \cdot y_{1,1} & x_{1,n} \cdot y_{1,2} & \cdots & x_{1,n} \cdot y_{1,n} \end{bmatrix} + \cdots + \begin{bmatrix} x_{p,1} \cdot y_{p,1} & x_{p,1} \cdot y_{p,2} & \cdots & x_{p,1} \cdot y_{p,n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{p,n} \cdot y_{p,1} & x_{p,n} \cdot y_{p,2} & \cdots & x_{p,n} \cdot y_{p,n} \end{bmatrix} \quad (11)$$

Recall that the BAM network contains p associated vectors $\{X_r, Y_r\}$ for $r = 1, 2, \dots, p$; and the used cancelable transform is the XOR operation, i.e., Y and X must be of equal length, where X : is the biometric template represented as vector of length n , Y : is the corresponding transformation key represented as vector of length n as illustrated below:

$$\begin{aligned} x_1 &= [x_{1,1}, x_{1,2}, \dots, x_{1,n}] & y_1 &= [y_{1,1}, y_{1,2}, \dots, y_{1,n}] \\ x_2 &= [x_{2,1}, x_{2,2}, \dots, x_{2,n}] & y_2 &= [y_{2,1}, y_{2,2}, \dots, y_{2,n}] \\ &\vdots & &\vdots \\ x_p &= [x_{p,1}, x_{p,2}, \dots, x_{p,n}] & y_p &= [y_{p,1}, y_{p,2}, \dots, y_{p,n}] \end{aligned}$$

The weight matrix W of size $n \times n$, computed using Equations (4) and (5), can be constructed by matrix notations as expressed in Equation (11). When an adversary has only the values of matrix W , we analyze the computational complexity needed to reconstruct the genuine transformation key Y_s or the genuine biometric template X_s using matrix W . Each single row vector in W could be seen as a linear system of equations, e.g. the s^{th} row in W matrix which contains values: $[w_{s,1}, w_{s,2}, \dots, w_{s,n}]$, could be represented by the following linear system of equations:

$$\begin{aligned} w_{s,1} &= x_{1,s} \cdot y_{1,1} + x_{2,s} \cdot y_{2,1} + \cdots + x_{p,s} \cdot y_{p,1} \\ w_{s,2} &= x_{1,s} \cdot y_{1,2} + x_{2,s} \cdot y_{2,2} + \cdots + x_{p,s} \cdot y_{p,2} \\ &\vdots \\ w_{s,n} &= x_{1,s} \cdot y_{1,n} + x_{2,s} \cdot y_{2,n} + \cdots + x_{p,s} \cdot y_{p,n} \end{aligned}$$

This linear system of equations can be represented using matrix notations as follows:

$$\begin{bmatrix} w_{s,1} \\ w_{s,2} \\ \vdots \\ w_{s,n} \end{bmatrix} = \begin{bmatrix} y_{1,1} \\ y_{1,2} \\ \vdots \\ y_{1,n} \end{bmatrix} \cdot x_{1,s} + \begin{bmatrix} y_{2,1} \\ y_{2,2} \\ \vdots \\ y_{2,n} \end{bmatrix} \cdot x_{2,s} + \cdots + \begin{bmatrix} y_{p,1} \\ y_{p,2} \\ \vdots \\ y_{p,n} \end{bmatrix} \cdot x_{p,s} \quad (12)$$

Grouping the common factors yields:

$$\begin{bmatrix} w_{s,1} \\ w_{s,2} \\ \vdots \\ w_{s,n} \end{bmatrix} = \begin{bmatrix} y_{1,1} & y_{2,1} & \cdots & y_{p,1} \\ \vdots & \vdots & \ddots & \vdots \\ y_{1,n} & y_{2,n} & \cdots & y_{p,n} \end{bmatrix} \cdot \begin{bmatrix} x_{1,s} \\ x_{2,s} \\ \vdots \\ x_{p,s} \end{bmatrix} \quad (13)$$

By expanding Equation (13) for each row vector in W matrix, i.e. substituting s from 1 to n , each linear system could be expressed as follows:

$$\begin{bmatrix} w_{1,1} \\ w_{1,2} \\ \vdots \\ w_{1,n} \end{bmatrix} = \begin{bmatrix} y_{1,1} & y_{2,1} & \cdots & y_{p,1} \\ \vdots & \vdots & \ddots & \vdots \\ y_{1,n} & y_{2,n} & \cdots & y_{p,n} \end{bmatrix} \cdot \begin{bmatrix} x_{1,1} \\ x_{2,1} \\ \vdots \\ x_{p,1} \end{bmatrix} \quad (14)$$

$$\begin{bmatrix} w_{2,1} \\ w_{2,2} \\ \vdots \\ w_{2,n} \end{bmatrix} = \begin{bmatrix} y_{1,1} & y_{2,1} & \cdots & y_{p,1} \\ \vdots & \vdots & \ddots & \vdots \\ y_{1,n} & y_{2,n} & \cdots & y_{p,n} \end{bmatrix} \cdot \begin{bmatrix} x_{1,2} \\ x_{2,2} \\ \vdots \\ x_{p,2} \end{bmatrix} \quad (15)$$

$$\begin{bmatrix} w_{n,1} \\ w_{n,2} \\ \vdots \\ w_{n,n} \end{bmatrix} = \begin{bmatrix} y_{1,1} & y_{2,1} & \cdots & y_{p,1} \\ \vdots & \vdots & \ddots & \vdots \\ y_{1,n} & y_{2,n} & \cdots & y_{p,n} \end{bmatrix} \cdot \begin{bmatrix} x_{1,n} \\ x_{2,n} \\ \vdots \\ x_{p,n} \end{bmatrix} \quad (16)$$

Mathematically, solving each linear system given only W requires guessing the matrix Y . In order to guess the values of Y , which contains $n \times p$ unknown variables, the attacker needs at most 2^{np} trails to get the correct values of Y which satisfy all linear system equations. Thus, the computational effort needed by any attacker to disclose the linear system of equations is as hard as randomly guessing all key values. Having key length equivalent to biometric template length makes it computationally infeasible to guess key values, especially when p and n are large values. Additionally, The attacker needs extra efforts to detect the genuine biometric data linked to the genuine transformation key. This is because, as mentioned before in Section 2.1, the weight matrix W not only contains the genuine user key information associate with its genuine biometric data but also contains other non-genuine keys linked to non-genuine biometric data.

3.3 Pre-image Attack Analysis

The pre-image attackers attempt to recreate sufficiently comparable biometric templates which act as the genuine one utilizing the compromised data. In our proposed work, generating biometric data from the stored data (connection weights and cancelable template) is computationally as hard as random guessing. It is unattainable to reveal any information using only the stored XORed template without knowing either the key or biometric data as proven in the previous subsection. However, the pre-image attacker can construct a non-genuine biometric features and a non-genuine transformation key which generate enough similar XORed template. Fortunately, there is no mathematical way to construct a non-genuine biometric template that is close enough to the original one from both of the stored XORed template and the connection weights. Therefore, our proposed method is robust against pre-image attack.

Since the pre-image attacker has no way to create an approximated input patterns except through ran-

Table 1: CASIA-IrisV3-Interval properties [5]

# subjects	# classes	Total number of images	Image Resolution
249	395	2683	320 × 282

Table 2: *Experimental parameters setting*

Masek output-code		BAM Structure		XOR- parameters	
Iris array size	40 × 480 bits	# input nodes	9600	Iris' size	9600
		BAM weights size	9600 × 9600	Key size	9600
Reference iris code size	9600 bit	# output nodes	9600	XORed Template' size	9600
		# patterns	p		

dom guessing (Brute-force), the maximum number of trials needed to construct biometric data or key to disclose biometric system's data is 2^n , (where n represents the input binary-valued biometrics template length, or equivalently, the input binary-valued transformation key length). Therefore, our proposed scheme maximizes the efforts needed for this kind of attacks, especially when n is large.

4 Experimental Results

In order to evaluate our proposed work from recognition performance perspective, several experiments were performed on the standard CASIA-IrisV3-Interval database [5]. The database is partitioned into 249 subjects; each subject has his right or left or both eye' samples. Table 1 illustrates the CASIA-IrisV3-Interval database specification in detail. In order to construct iris codes for each iris dataset image, Masek code [18] was utilized to construct the genuine binary valued iris templates.

During the BAM association phase, a reference pattern for each iris was created using the approach clarified in Section 2.1. Each class reference iris code serve as an input pattern for this BAM model to be associated with a randomly generated binary key. Other training non-genuine patterns have been experimentally determined using the metric of Hamming distance by taking iris codes belong to other classes which are far enough to the class' reference iris code. Each non-genuine iris code is associated with a randomly constructed non-genuine key. Once the training phase is complete, the learned weights were stored in the system storage. The reference iris code for each iris is XORed with its associated key to construct the final stored cancelable template. Table 2 summarizes the simulated experiments parameters' values. The output binary iris array was reshaped to be formed into reference binary code by combining each array rows one followed by another. This binary iris vector and another binary sequence (key) with the same length were utilized to compose BAM network structure with set of patterns p , where the lengths of both the stored cancelable template and the input binary iris vector are equal.

To detect the appropriate number of associated pattern pairs p which achieve high recognition performance,

various experiments were executed. For each experiment, a sample of ten classes has been randomly selected from CASIA-Iris V3-Interval to testify the best number of patterns p . These experiments have been done using various number of patterns (e.g. $p = 5, p = 10, p = 30, p = 70$). Figure 2 shows the impostor and genuine matching score distributions using the metric of hamming distance from all possible comparisons. The separability between genuine and impostor distributions is measured by the decidability metrics d' [22] computed by:

$$d' = \frac{|\mu_i - \mu_g|}{\sqrt{\frac{\sigma_i^2 + \sigma_g^2}{2}}} \quad (17)$$

where μ_i and μ_g are the means and σ_i^2 and σ_g^2 are the variances of the impostor and genuine distributions, respectively. The larger decidability metrics d' value, the larger separation between impostor and genuine distributions which indicates better recognition performance. As shown in Figure 2, the obtained values of the decidability metric are 2.708, 2.56, 2.53 and 2.25 for $p = 5, p = 10, p = 30$, and $p = 70$, respectively. From security perspective, the security of our proposed scheme depends upon number of associated patterns p , i.e., the larger p value, the more efforts needed to disclose the saved cancelable template (as previously explained in Section 3). To balance both of security and recognition performance constraints for the experiment, the number of patterns is suggested to be 30.

The recognition accuracy of our proposed method is evaluated using the receiver operation characteristic (ROC) curves. Figure 3 illustrates the ROC curves of the protected iris code compared to the unprotected (genuine) codes applied on the entire CASIA-V3 iris database. The EER(%) of the genuine unprotected iris code is 1.78; the EER(%) of XORed protected iris code is 2.001, lower EER value indicates high recognition performance. As can be seen in Figure 3, our proposed scheme achieved a recognition performance comparable to the genuine unprotected system.

To compare our proposed work with other existing cancelable biometric schemes. Several cancelable schemes: Teoh [34], Rathgeb [27], Ouda [21] and Mayada [32] were selected. Table 3 illustrates this comparison from perspectives of security and performance. Moreover, the recognition accuracy comparisons are graphed using ROC curves

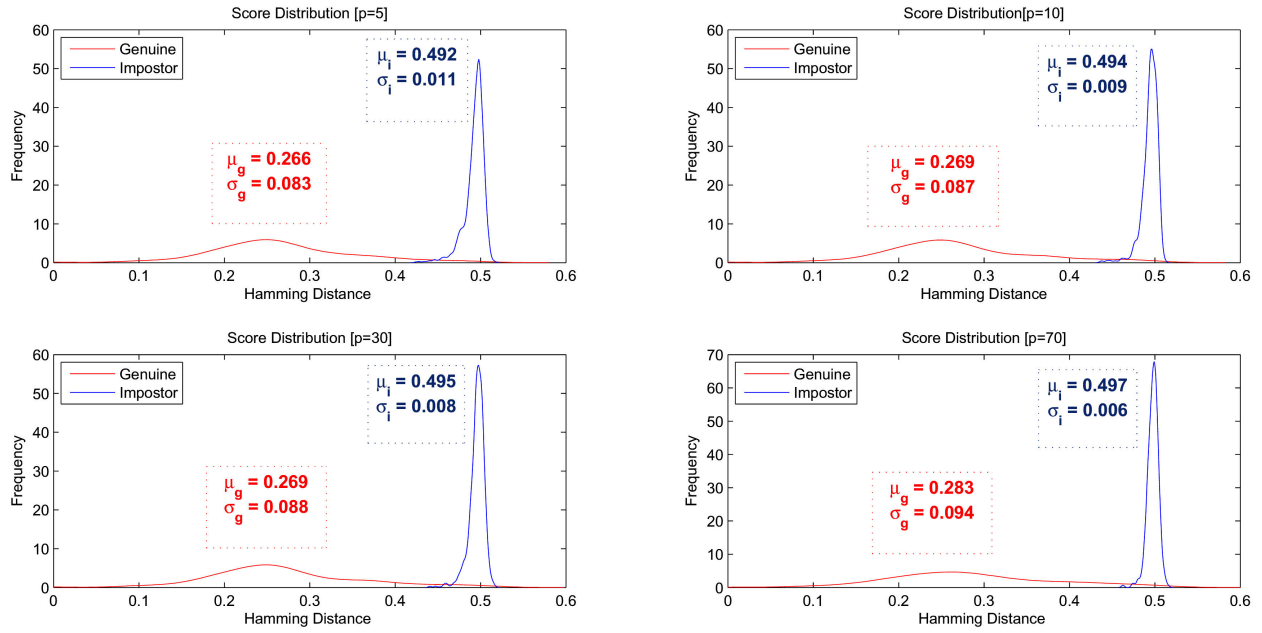
Figure 2: Impostor and genuine score distributions for different number of patterns (p)

Table 3: A comparative study analysis

Scheme	Security Strength	Pre-image attack	Performance (EER%)
Teoh [34]	Based on Token	Not protected	4.81
Rathgeb [27]	Based on secret key	Not protected	8.98
Ouda [21]	Based on public key	Not protected	5.54
Mayada [32]	Based on hidden key	Protected	3.56
Proposed	Based on hidden key	Protected	2.001

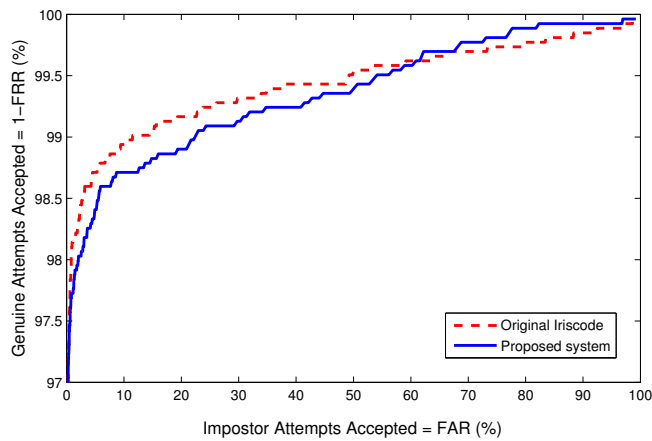


Figure 3: ROC curves of proposed and the unprotected methods

as shown in Figure 4. All experiments applied on CASIA-V3 iris database where recognition performance relies on biometric data rather than the dependency on key/token as recommended in [11].

We can infer that, our proposed work is pre-image re-

sistant scheme with the privilege of high recognition performance.

5 Conclusions

This paper proposed a pre-image resistant cancelable biometric scheme which depends on hiding the cancelable transformation parameters in an associative memory. Bidirectional associated memory network is utilized to associate each user biometric features with his genuine transformation key to encode them in connection weights. The connection weights could be safely saved in the central storage with the XORed template between the biometric features and its associated transformation key which represent the cancelable template. The security requirements of this proposed work is guaranteed while the saved connection weights can't expose the genuine biometric data or on approximate version of it, also, transformation key is secured. Additionally, our proposed scheme does not require carrying or remembering transformation key during the verification process. Evaluation analysis in terms of revocability, diversity and non-invertability shows that our proposed scheme satisfies all these proprieties. Additionally the scheme achieves high recognition

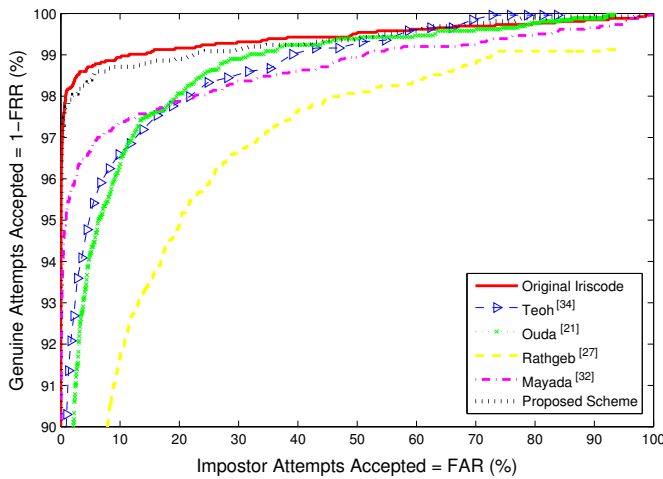


Figure 4: ROC curves of the proposed and existing cancelable biometrics schemes

accuracy when applied to CASIA-IrisV3-Interval dataset.

References

- [1] M. H. Almourish, "Image recognition using bidirectional associative memory and fuzzy image enhancement," *Journal of Science and Technology*, vol. 19, no. 1, 2014.
- [2] M. G. Barrero, J. Fierrez, J. Galbally, E. Maiorana, and P. Campisi, "Implementation of fixed-length template protection based on homomorphic encryption with application to signature biometrics," in *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, pp. 191–198, 2016.
- [3] R. Belguechi, A. Hafiane, E. Cherrier, and C. Rosenberger, "Comparative study on texture features for fingerprint recognition: application to the bihashing template protection scheme," *Journal of Electronic Imaging*, vol. 25, no. 1, 2016.
- [4] P. Campisi, E. Maiorana, and A. Neri, "Iris template protection," in *Encyclopedia of Biometrics*, pp. 1057–1065, 2015.
- [5] CASIA, *CASIA Iris Image Database*, Sept. 2016. (<http://biometrics.idealtest.org/findTotalDbByMode.do?mode=Iris>)
- [6] A. I. Desoky, H. A. Ali, and N. B. Abdel-Hamid, "Enhancing iris recognition system performance using templates fusion," *Ain Shams Engineering Journal*, vol. 3, no. 2, pp. 133–140, 2012.
- [7] N. Evans, S. Marcel, A. Ross, and A.B.J. Teoh, "Biometrics security and privacy protection," *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 17–18, 2015.
- [8] S. V. Gaddam and M. Lal, "Efficient cancellable biometric key generation scheme for cryptography," *International Journal of Network Security*, vol. 11, no. 2, pp. 61–69, 2010.
- [9] T. Gerbet, A. Kumar, and C. Lauradoux, "The power of evil choices in bloom filters," in *45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'15)*, 22–25 June 2015.
- [10] O. Kaiwartya, M. Prasad, S. Prakash, D. Samadhiya, A. H. Abdullah, and S. O. Abd Rahman, "An investigation on biometric internet security," *International Journal of Network Security*, vol. 19, no. 2, pp. 167–176, In Press, 2017.
- [11] A. Kong, K. H. Cheung, D. Zhang, M. Kamel, and J. You, "An analysis of bihashing and its variants," *Pattern Recognition*, vol. 39, no. 7, pp. 1359–1368, 2006.
- [12] P. Lacharme, "Analysis of the iriscode bioencoding scheme," *International Journal of Computer Science and Security*, vol. 6, no. 5, pp. 315–321, 2012.
- [13] C. C. Lee, C. H. Liu, and M. S. Hwang, "Guessing attacks on strong-password authentication protocol," *International Journal of Network Security*, vol. 15, no. 1, pp. 64–67, 2013.
- [14] Y. Lee, Y. Chung, and K. Moon, "Inverse operation and preimage attack on bihashing," in *Proceedings of The International IEEE Workshop on Computational Intelligence in Biometrics: Theory, Algorithms, and Applications*, pp. 1–8, Nashville, TN, 2009.
- [15] C. T. Li and M. S. Hwang, "An online biometrics-based secret sharing scheme for multiparty cryptosystem using smart cards," *International Journal of Innovative Computing, Information and Control*, vol. 6, no. 5, pp. 2181–2188, 2010.
- [16] Y. Liu, "Bihashing for human acoustic signature based on random projection," *Canadian Journal of Electrical and Computer Engineering*, vol. 38, no. 3, pp. 266–273, 2015.
- [17] E. Maiorana, P. Campisi, J. Fierrez, J. Ortega-Garcia, and A. Neri, "Cancelable templates for sequence-based biometrics with application to on-line signature recognition," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 40, no. 3, pp. 525–538, 2010.
- [18] L. Masek and P. Kovesi, "Matlab source code for a biometric identification system based on iris patterns," Tech. Rep. RFC 2627, The School of Computer Science and Software Engineering, Western Australia University, 2003.
- [19] A. Nagara, K. Nandakumar, and A.K. Jain, "Biometric template transformation: A security analysis," in *Proceedings of The SPIE, Electronic Imaging, Media Forensics and Security XII*, pp. 1–15, San Jose, USA, 2010.
- [20] D. C. L. Ngo, A. B. J. Teoh, and J. Hu, *Biometric Security*, Cambridge Scholars Publishing, 2015.
- [21] O. Ouda, N. Tsumura, and T. Nakaguchi, "A reliable tokenless cancelable biometrics scheme for protecting iriscode," *IEICE Transaction on Information and Systems*, vol. E93-D, no. 7, pp. 1878–1888, 2010.

- [22] O. Ouda, N. Tsumura, and T. Nakaguchi, "On the security of bioencoding based cancelable biometrics," *IEICE Transaction on Information and Systems*, vol. E94-D, no. 9, pp. 1768–1778, 2011.
- [23] V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable biometrics: A review," *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 54–65, 2015.
- [24] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 561–572, 2007.
- [25] N. K. Ratha, J. H. Connell, R. M. Bolle, and S. Chikkerur, "Cancelable biometrics: a case study in fingerprints," in *Proceedings of The 18th International Conference on Pattern Recognition*, pp. 1–13, Hong Kong, 2006.
- [26] C. Rathgeb, F. Breiting, H. Baier, and C. Busch, "Towards bloom filter-based indexing of iris biometric data," in *IEEE International Conference on Biometrics (ICB'15)*, pp. 422–429, 2015.
- [27] C. Rathgeb, F. Breiting, C. Busch, and H. Baier, "On the application of bloom filters to iris biometrics," *IET Journal on Biometrics*, vol. 3, no. 4, pp. 207–218, 2014.
- [28] C. Rathgeb and C. Busch, "Cancelable multi-biometrics: Mixing iris-codes based on adaptive bloom filters," *Elsevier Computers and Security*, vol. 42, pp. 1–12, 2014.
- [29] C. Rathgeb and A. Uhl, "Secure iris recognition based on local intensity variations," in *Proceedings of The International Conference on Image Analysis and Recognition*, pp. 266–275, Portugal, 2010.
- [30] M. Savvides, V. kumar, and P.K. khosla, "Cancelable biometric filters for face recognition," in *Proceedings of The 17th International Conference on Pattern Recognition*, pp. 922–925, USA, 2004.
- [31] M. A. Syarif, T. S. Ong, A. B. J. Teoh, and C. Tee, *Improved Biohashing Method Based on Most Intensive Histogram Block Location*, pp. 644–652, Springer, 2014.
- [32] M. Tarek, O. Ouda, and T. Hamza, "Robust cancelable biometrics scheme based on neural networks," *IET Journal on Biometrics*, vol. 5, no. 3, pp. 220–228, 2016.
- [33] A. B. J. Teoh and L. Y. Chong, "Secure speech template protection in speaker verification system," *Speech Communication*, vol. 52, no. 2, pp. 150–163, 2010.
- [34] A. B. J. Teoh, D. C. L. Ngo, and A. Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognition*, vol. 37, no. 11, pp. 2245–2255, 2004.
- [35] G. Zakar, *Artificial Neural Networks*, CreateSpace Independent Publishing Platform, 2016.
- [36] J. Zuo, N. K. Ratha, and J. H. Connell, "Cancelable iris biometric," in *Proceedings of The 19th International Conference on Pattern Recognition*, pp. 1–4, NY, USA, 2008.

Biography

Mayada Tarek received her B.S. degree in 2007 and her M.S. degree in 2011, both in Department of Computer Science, Mansoura University, Egypt. She is currently pursuing here Ph.D. degree in Computer Science. Here current research interests include Pattern Recognition, Information Security, Biometrics, and Soft Computing Techniques.

Osama Ouda received his B.S. in Computer Science from Mansoura University, Egypt, in 2000, his M.S. in Computer Science from Ain-Shams University, Egypt, in 2007, and his Ph.D. in Computer and Information Sciences from Chiba University, Japan, in 2011. From November 2013 to May 2014, he was a research fellow at iProBe laboratory, Michigan State University, East Lansing, USA. Currently, he is an assistant professor in the Department of Information Technology, Mansoura University, Egypt. Dr. Ouda is a member of IEEE since 2011. His research interests include information security, biometrics, image processing and machine learning.

Taher Hamza received his B.S degree in 1975 and his M.S. degree in 1979, both in Department of Mathematics, Mansoura University, Egypt. Ph.D degree in 1986 from St Andrews University, Scotland, UK. His current research interests include Artificial Intelligence, Expert Systems, Biometrics, and Machine Learning.

Propagation Model with Varying Population Size of Removable Memory Device Virus

Cong Jin¹, Xiaoyan Wang²

(Corresponding author: Cong Jin)

School of Computer, Central China Normal University¹

Wuhan 430079, P.R. China

Department of Electronic Information, Zhengzhou Electric Power College²

Zhengzhou 450000, P.R. China

(Email: jincong@mail.ccnu.edu.cn)

(Received Mar. 8, 2016; revised and accepted May 20 & July 19, 2016)

Abstract

Removable memory device (RMD) is one of main way for propagating computer virus. In this paper, a dynamic propagation model of RMD-virus with varying population size is discussed. Unlike other computer virus propagation models, the proposed model mainly considers the RMD-virus propagation between host and RMD, which is embodied by introducing the RMD state and new propagation rate. Furthermore, to control the RMD-virus, three threshold parameters are obtained. The simulation results show that the proposed model can serve as a basis for understanding and simulating RMD-virus.

Keywords: Computer virus, propagation model, RMD-SIR model, RMD-virus

1 Introduction

Computer virus propagation mainly depends on two ways: network and removable memory device (RMD). In this paper, RMD represents all mobile devices related to computer, including flash disk, mobile phones, digital cameras, mobile hard disk, memory card etc. The virus to propagate through network and RMD is called as network virus and RMD-virus respectively.

There are significant similarities between the propagation of computer virus and biological epidemics [3, 10, 13]. Epidemiological propagation model of computer virus was based on two simplifications: (1) At any given time, each host in the total population is one of a finite number of states, e.g., susceptible, removed, exposed, infected and detected etc. (2) The virus transmission can be translated into a probability of a host infecting another one. Some epidemiological models, such as Susceptible-Infected-Recovered (SIR) model, have been considered by possible ways for obtaining the propagation behavior of computer virus with various states (e.g., susceptible

(S), infected (I), and recovered (R)) and their transitions [2, 6, 7].

In this paper, we will discuss a RMD-virus propagation model, namely RMD-SIR, which is an extension of the SIR [8] model by adding the RMD state and transmission RMD state. We will analyze the RMD-virus-free equilibrium (RVFE) to derive the important parameter. The RMD-SIR provides an opportunity to study the behavior of RMD-virus propagation.

In former studies of computer virus propagation, the total number of hosts always is assumed constant. However, in reality, the population size (i.e., the number of hosts) is varying with time due to the network and off network of hosts. To study the propagation of RMD-virus with different host size, we assume the total host size is varying with time. Similarity, the total RMD number is also varying with time.

The remainder of this paper is organized as follows. Section 2 proposes a dynamic propagation model of RMD-virus based on dynamic propagation rates. Section 3 analyzes the stability of the RMD-SIR system, and Section 4 represents the dynamic property of the host population sizes. Section 5 represents some numerical results. Finally, conclusions are given in Section 6.

2 Description of RMD-SIR Model

For RMD-SIR model, we have following assumptions: (1). The total population size N of hosts and total population size n of RMDs are varying with time t . (2). All RMDs can exchange information with more than one host. This assumption is reasonable for RMD. (3). Even user has found the host or RMD to be infected, and he can still continue to acquire information from this host or RMD, such as the computers in print shop or internet bar. (4). Once hosts are vaccinated, they can gain permanent immunity and no longer be infected by this RMD-virus.

In RMD-SIR model, the two new RMD states, S_u and I_u corresponding to the host states S_c and I_c in SIR model, are added into the traditional SIR model. The new propagation rates are β_{cu} and β_{uc} respectively, where β_{cu} is the the propagation rate from host to RMD and β_{uc} propagation rate from RMD to host. So, there are five states and state transitions in RMD-SIR model, which is shown in Figure 1.

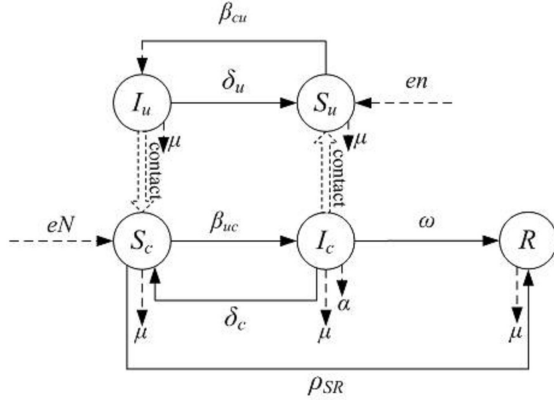


Figure 1: RMD-SIR model

2.1 States and State Transition in RMD-SIR Model

The total population of hosts is partitioned into three groups, and any host can potentially be one of these groups at any time t : (1) S (Susceptible): All hosts in this group have not been infected by RMD-virus, only when these hosts contact with an infected RMD, they can be infected by the RMD-virus, indicated by S_c . (2) I (Infected): All hosts in this group have been infected by the RMD-virus, indicated by I_c . (3) R (Removed): All hosts in this group have been vaccinated and immunized to the RMD-virus, indicated by R .

The total population of RMD is partitioned into two groups: (1) S (Susceptible): All RMDs in this group easily infect virus, only when RMDs insert into an infected host, RMDs are infected by the virus, indicated by S_u . (2) I (Infected): All RMDs in this group have been infected by the virus, indicated by I_u . Where, c and u , as the subscripts, indicate the states of the host and RMD, respectively.

Initially, all hosts are in S -state. Once RMD-virus intrudes into the system, these hosts may change their states according to the following rules:

- $S_c \rightarrow R$, using countermeasure of immunization.
- $S_c \rightarrow I_c$, infected by an infected RMD.
- $I_c \rightarrow R$, using immunization after virus stopping and cleaning in host.

- $I_c \rightarrow S_c$, do not capture immunization ability after RMD-virus stopping and cleaning in host.
- $S_u \rightarrow I_u$, infected by an infected host.
- $I_u \rightarrow S_u$, after RMD-virus cleaning, because RMD dose not have immunization ability itself, the remove RMD-virus in RMD must depend on clearing RMD-virus capability of host.

In Figure 1, each circular represents the states of host or RMD. And the directed lines denote the potential transition paths from one state to another.

We assume the hosts subject to the uniformly distribution. More specifically, we assume that the local density of the total hosts is a constant though the total population size $N(t) = S_c(t) + I_c(t) + R(t)$ may vary with time t . Here $S_c(t)$, $I_c(t)$ and $R(t)$ denote the sizes of the $S_c(t)$, $I_c(t)$ and R classes at any time t , respectively. Similarly, the total population size $n(t)$ of RMD is varying with time t , denoted by $n(t) = S_u(t) + I_u(t)$.

Let $e > 0$ and $\mu > 0$ be birth rate and mortality rate not due to the RMD-virus respectively. Many researchers assume the birth rate and mortality rate are same [12]. In practice, these two parameters are not equivalent. It is assumed that all newborns are susceptible and direct transmission can be neglected. Let α be the death rate for the infectious hosts suffer a RMD-virus, it means the probability of infected hosts not to be used due to the RMD-virus. For convenience, we explain the notations used in this paper. The details are listed in Table 1.

$1/n$ is the proportion of contacting between susceptible hosts and infective RMDs, and $1/N$ is the proportion of contacting between susceptible RMDs and infective hosts. For convenience, the replacement rates of host and RMD are set to be μ . This assumption is consistent with the actual situation, because in practice, the replacement frequency between the host and RMD is very close.

2.2 RMD-virus Propagation Model

The RMDs in the RMD-SIR model can be formulated by following equation:

$$\begin{cases} \frac{dS_u(t)}{dt} = en(t) - \beta_{cu}S_u(t)I_c(t)/N + \delta_u I_u(t) - \mu S_u(t) \\ \frac{dI_u(t)}{dt} = \beta_{cu}S_u(t)I_c(t)/N - \delta_u I_u(t) - \mu I_u(t). \end{cases} \quad (1)$$

The hosts in RMD-SIR model can be formulated by following equation:

$$\begin{cases} \frac{dS_c(t)}{dt} = eN(t) + \delta_c I_c(t) - \beta_{uc}S_c(t)I_u(t)/n - \mu S_c(t) - \rho_{SR}S_c(t) \\ \frac{dI_c(t)}{dt} = \beta_{uc}S_c(t)I_u(t)/n - (\mu + \omega + \delta_c + \alpha)I_c(t) \\ \frac{dR(t)}{dt} = \omega I_c(t) + \rho_{SR}S_c(t) - \mu R(t). \end{cases} \quad (2)$$

Table 1: Notations and definitions

Notation	Definition
$S_u(t)$	Number of susceptible RMD at time t
$I_u(t)$	Number of Infected RMD at time t
$S_c(t)$	Number of susceptible hosts at time t
$I_c(t)$	Number of infected hosts at time t
$R(t)$	Number of vaccinated hosts at time t
N	Total number of hosts under consideration
n	Total number of RMD under consideration
e	Birth rate
μ	Replacement rate not due to the RMD-virus
β_{cu}	RMD-virus propagation rate from host to RMD
β_{uc}	RMD-virus propagation rate from RMD to host
δ_u	Recovery rate of host from state I to S_c
δ_c	Recovery rate of RMD from state I to S_u
α	Death rate due to the RMD-virus
ω	Rate at which infected hosts are vaccinated or treated
ρ_{SR}	Rate at which S hosts are vaccinated or treated

Combine (1) and (2) as:

$$\begin{cases} \frac{dS_u(t)}{dt} = en(t) - \beta_{cu}S_u(t)I_c(t)/N + \delta_u I_u(t) - \mu S_u(t) \\ \frac{dI_u(t)}{dt} = \beta_{cu}S_u(t)I_c(t)/N - \delta_u I_u(t) - \mu I_u(t) \\ \frac{dS_c(t)}{dt} = eN(t) + \delta_c I_c(t) - \beta_{uc}S_c(t)I_u(t)/n - \mu S_c(t) - \rho_{SR}S_c(t) \\ \frac{dI_c(t)}{dt} = \beta_{uc}S_c(t)I_u(t)/n - (\mu + \omega + \delta_c + \alpha) I_c(t) \\ \frac{dR(t)}{dt} = \omega I_c(t) + \rho_{SR}S_c(t) - \mu R(t). \end{cases} \quad (3)$$

Where

$$\begin{cases} \frac{dN(t)}{dt} = (e - \mu)N(t) - \alpha I_c(t) \\ \frac{dn(t)}{dt} = (e - \mu)n(t). \end{cases} \quad (4)$$

When $N(t)$ is not constant, it is often necessary to consider the proportions of individuals in five epidemiological classes, namely, $s_u = S_u/n$, $i_u = I_u/n$, $s_c = S_c/N$, $i_c = I_c/N$, $r = R/N$. We use $'$ to replace d/dt , according to the derivation formula $s'_u = (\frac{S_u}{n})' = (\frac{S'_u n - S_u n'}{n^2})$, we get $s'_u = e - \beta_{cu}s_u i_c + \delta_u i_u - es_u$, then it is easy to verify that s_u, i_u, s_c, i_c, r satisfy the following system of differential equations

$$\begin{cases} s'_u = e - \beta_{cu}s_u i_c + \delta_u i_u - es_u \\ i'_u = \beta_{cu}s_u i_c - \delta_u i_u - ei_u \\ s'_c = e - \beta_{uc}s_c i_u - (\rho_{SR} + e)s_c + \alpha i_c s_c \\ i'_c = \beta_{uc}s_c i_u - (\omega + \delta_c + \alpha + e)i_c + \alpha i_c^2 \\ r' = \omega i_c + \rho_{SR}S_c - er + \alpha i_c r. \end{cases} \quad (5)$$

We add the restricted conditions $s_u + i_u = 1$, $s_c + i_c + r = 1$. We also notice that the variable r does not appear in the first four equations of (5), and we can first study the

reduced system

$$\begin{cases} s'_u = e - \beta_{cu}s_u i_c + \delta_u i_u - es_u \\ i'_u = \beta_{cu}s_u i_c - \delta_u i_u - ei_u \\ s'_c = e - \beta_{uc}s_c i_u - (\rho_{SR} + e)s_c + \alpha i_c s_c \\ i'_c = \beta_{uc}s_c i_u - (\omega + \delta_c + \alpha + e)i_c + \alpha i_c^2. \end{cases} \quad (6)$$

3 Stability Analysis for Equilibrium

Stable states of model (6) satisfy the following equations:

$$\begin{cases} s'_u = 0 \\ i'_u = 0 \\ s'_c = 0 \\ i'_c = 0. \end{cases} \quad (7)$$

Let $i'_c = 0$, we have

$$i_c^* = i_u^* = 0, s_u^* = 1, s_c^* = \frac{e}{e + \rho_{SR}}. \quad (8)$$

For the case of $i_c^* = i_u^* = 0$, we have the RVFE as follows

$$EQ_{vf} = P_0 = (s_{u1}^*, i_{u1}^*, s_{c1}^*, i_{c1}^*) = (1, 0, \frac{e}{e + \rho_{SR}}, 0). \quad (9)$$

For the case of $i_c^* > 0$, $i_u^* > 0$, we will verify the existence of the RMD-virus-epidemic equilibrium (RVFE) in Subsection 3.3.

3.1 Basic Reproduction Number of Model

It was easy to calculate the RVFE $EQ_{vf} = (1, 0, \frac{e}{e + \rho_{SR}}, 0)$ of model (6). Let $X = (s_u, i_u, s_c, i_c)$, then the model (6)

can be written as $X' = F(X) - Z(X)$. Where

$$F(X) = \begin{pmatrix} \beta_{cu}s_u i_c \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$Z(X) = \begin{pmatrix} \delta_u i_u + e i_u \\ -\beta_{uc}s_c i_u + (\omega + \delta_c + \alpha + e)i_c + \alpha i_c^2 \\ -e + \beta_{cu}s_u i_c - \delta_u i_u + e s_u \\ -e + \beta_{uc}s_c i_u + (\rho_{SR} + e)s_c - \alpha i_c s_c \end{pmatrix} \quad (10)$$

At RVFE P_0 , Jacobian matrices of $F(X)$ and $Z(X)$ are shown as follows

$$DF(P_0) = \begin{pmatrix} F_{2 \times 2} & 0_{2 \times 2} \\ 0_{2 \times 2} & 0_{2 \times 2} \end{pmatrix}$$

$$DZ(P_0) = \begin{pmatrix} Z_{2 \times 2} & 0_{2 \times 2} \\ Z_{2 \times 2}^1 & Z_{2 \times 2}^2 \end{pmatrix}$$

Where,

$$F_{2 \times 2} = \begin{pmatrix} 0 & \beta_{cu} \\ 0 & 0 \end{pmatrix},$$

$$Z_{2 \times 2} = \begin{pmatrix} \delta_u + e & 0 \\ \frac{-e\beta_{uc}}{e+\rho_{SR}} & \omega + \delta_c + \alpha + e \end{pmatrix},$$

$$Z_{2 \times 2}^1 = \begin{pmatrix} -\delta_u & \beta_{cu} \\ \frac{e\beta_{uc}}{e+\rho_{SR}} & \frac{-\alpha e}{e+\rho_{SR}} \end{pmatrix},$$

$$Z_{2 \times 2}^2 = \begin{pmatrix} e & 0 \\ 0 & \rho_{SR} + e \end{pmatrix},$$

$F_{2 \times 2} Z_{2 \times 2}^{-1}$ was the next generation matrix [9] for model (6). The spectral radius of the matrix $F_{2 \times 2} Z_{2 \times 2}^{-1}$ is

$$\rho(F_{2 \times 2} Z_{2 \times 2}^{-1}) = \frac{e\beta_{cu}\beta_{uc}}{(\delta_u + e)(\omega + \delta_c + \alpha + e)(e + \rho_{SR})}. \quad (11)$$

According to Theorem 2 in [5], the basic reproduction number of model (6) is

$$R_0 = \frac{e\beta_{cu}\beta_{uc}}{(\delta_u + e)(\omega + \delta_c + \alpha + e)(e + \rho_{SR})} \quad (12)$$

where, R_0 is the threshold parameter.

3.2 RVFE and Its Stability

3.2.1 Locally Stability of the RVFE

Clearly, all parameters of P_0 are positive. Jacobian matrix of (6), at an arbitrary point $P(s_u, i_u, s_c, i_c)$, is Equation (13).

The Jacobian matrix $J(P)$, at P_0 , is Equation (14).

The eigenpolynomial of $J(P_0)$ is Equation (15), then

$$(\lambda + e)[\lambda + (\rho_{SR} + e)](\lambda^2 + (\delta_u + e + \omega + \delta_c + \alpha + e)\lambda + (\delta_u + e)(\omega + \delta_c + \alpha + e) - \frac{e\beta_{cu}\beta_{uc}}{\rho_{SR} + e}) = 0 \quad (16)$$

The stability of P_0 is equivalent to all eigenvalues of (16) being with negative real parts, which can be guaranteed by

$$R_0 = \frac{e\beta_{cu}\beta_{uc}}{(\delta_u + e)(\omega + \delta_c + \alpha + e)(e + \rho_{SR})} < 1 \quad (17)$$

When $R_0 > 1$, Equation (10) has one positive root and three negative roots. So, the RVFE P_0 is locally asymptotically stable if $R_0 < 1$ and unstable if $R_0 > 1$. So, we have following Lemma 1.

Lemma 1. *RVFE P_0 is locally asymptotically stable if $R_0 < 1$.*

3.2.2 Global Stability of the RVFE

In this subsection, we show that the parameter restrictions of local stability of the RVFE guarantee its global stability. Here we define another threshold parameter

$$\hat{R}_0 = \frac{\beta_{cu}\beta_{uc}}{(\delta_u + e)(\omega + \delta_c + \alpha + e)} \quad (18)$$

It notices that $\hat{R}_0 < 1$ guarantees $R_0 < 1$.

Theorem 1. *RVFE P_0 of (6) is globally asymptotically stable $\hat{R}_0 \leq 1$; it is unstable if $R_0 > 1$. In the latter case, the solutions of (6) starting sufficiently close to P_0 move away from P_0 .*

Proof. We proof the global stability of P_0 by constructing a suitable Lyapunov function [11] $V = \beta_{cu}i_u + (\delta_u + e)i_c$. Differentiating V along (6), we obtains Equation (19).

The maximum value of (19) is achieved at the extreme points: $A_1(0, 0, 0, 0)$, $A_2(1, 0, 0, 0)$, $A_3(0, 1, 0, 0)$, $A_4(0, 0, 1, 0)$, $A_5(0, 0, 0, 1)$. It is easy to verify that the situations at these five points are shown in Table 2.

Table 2: Situations of five points

$A_1(0,0,0,0)$	$V' _{(5)}=0, \text{when } R_0 \leq 1$
$A_2(1,0,0,0)$	$V' _{(5)}=0, \text{when } R_0 \leq 1$
$A_3(0,1,0,0)$	$V' _{(5)}=0, \text{when } R_0 \leq 1$
$A_4(0,0,1,0)$	$V' _{(5)}=0, \text{when } R_0 \leq 1$
$A_5(0,0,0,1)$	$V' _{(5)}=0, \text{if } \hat{R}_0=1$

Let (19) be 0, i.e., $V'|_{(5)} = 0$ if $i_c = i_u = 0$ or $\hat{R}_0 = 1$. The maximum invariant set in $\{(s_u, i_u, s_c, i_c) \in \Delta | V'|_{(5)} = 0\}$ is the singleton $\{P_0\}$. By LaSalle's Invariance Principle ([4], Chapter 2, Theorem 6.4), the RVFE P_0 is globally asymptotically stable when $\hat{R}_0 \leq 1$.

If $R_0 > 1$, we define $V_2 = \beta_{uc}i_u + (\delta_u + e)i_c$. So, we have Equation (20).

Observe that $V_2'|_{(5)} > 0$ for s_u sufficiently close to $e/(e + \rho_{SR})$ except when $i_u = i_c = 0$. Solutions starting sufficiently close to P_0 leave a neighborhood of P_0 except those on the invariant s_c -axis, where (4) reduces to $s'_c = e - (\rho_{SR} + e)s_c$ and thus $s_c(t) \rightarrow e/(\rho_{SR} + e)$ as $t \rightarrow \infty$, completing the proof. \square

$$J(P) = \begin{bmatrix} -\beta_{cu}i_c - e & \delta_u & 0 & -\beta_{cu}s_u \\ \beta_{cu}i_c & -\delta_u - e & 0 & \beta_{cu} \\ 0 & -\beta_{uc}s_c & -\beta_{uc}i_c - (\rho_{SR} + e) + \alpha i_c & \alpha s_c \\ 0 & \beta_{uc}s_c & \beta_{uc}i_u & -(\omega + \delta_c + \alpha + e) + 2\alpha i_c \end{bmatrix} \quad (13)$$

$$J(P_0) = \begin{bmatrix} -e & \delta_u & 0 & -\beta_{cu} \\ 0 & -(\delta_u + e) & 0 & \beta_{cu} \\ 0 & -\beta_{uc}s_{c1}^* & -(\rho_{SR} + e) & \alpha s_{c1}^* \\ 0 & \beta_{uc}s_{c1}^* & 0 & -(\omega + \delta_c + \alpha + e) \end{bmatrix} \quad (14)$$

Theorem 1 points out that the threshold parameters R_0 and \hat{R}_0 give whether the infected hosts and RMDs to be promptly eliminated locally and globally respectively. Reducing R_0 value to less than unity can eradicate virus with a small magnitude. However, when \hat{R}_0 is adjusted less than or equal to unity, the virus can be eradicated even with a large magnitude. R_0 and \hat{R}_0 can be explained as the virus propagate by increasing inflow of susceptible and the infectious individuals, while weakening the outflow of the infected and susceptible.

3.3 Existence of the Local Equilibrium (LE)

Subsection 3.2.2 shows that the RVFE is globally asymptotically stable when $R_0 \leq 1$. This implies that, if there is not LE, the virus can be eliminated in the end. From the view of virus propagation, it is more important to investigate the existence of LE.

Suppose that $P_*(s_{u*}, i_{u*}, s_{c*}, i_{c*})$ is a LE. From Equation (6), its coordinate should satisfy

$$\begin{cases} e - \beta_{cu}s_{u*}i_{c*} + \delta_u i_{u*} - e s_{u*} = 0 \\ \beta_{cu}s_{u*}i_{c*} - \delta_u i_{u*} - e i_{u*} = 0 \\ e - \beta_{uc}s_{c*}i_{u*} - (\rho_{SR} + e)s_{c*} + \alpha i_{c*}s_{c*} = 0 \\ \beta_{uc}s_{c*}i_{u*} - (\omega + \delta_c + \alpha + e)i_{c*} + \alpha i_{c*}^2 = 0 \end{cases} \quad (21)$$

Where $s_{u*} > 0$, $i_{u*} > 0$, $s_{c*} > 0$, $i_{c*} > 0$. Using these inequalities, we have $(\rho_{SR} + e - \alpha i_{c*})(1 - s_{c*} - i_{c*}) = \omega i_{c*} + \delta_u(1 - s_{u*})$, which gives the following range of i_{c*} ,

$$0 < i_{c*} < \min\{1, (\rho_{SR} + e)/\alpha\} \quad (22)$$

We notice that, from Equation (22), when α is less than the ρ_{SR} , or e , or $\rho_{SR} + e$, i_{c*} will lie in the interval $(0, 1)$. Eliminating s_{u*} , i_{u*} , s_{c*} from Equation (12), i_{c*} satisfies Equation (23).

Where R_0 is defined by Equation (12). Furthermore, s_{u*} , i_{u*} , s_{c*} can be uniquely determined by Equation (24).

In (24), $s_{u*} > 0$, $i_{u*} > 0$, and $s_{c*} > 0$ are satisfied respectively, they can be guaranteed by the fact that $0 < i_{c*} < 1$ and $R_0 > 1$. Let $x \rightarrow f(x) \in R^n$ be a smooth vector field defined for x in an open set $D \subset R^n$, where

$$f(i_{c*}) = R_0,$$

$$f(i_c) = \left(1 - \frac{\alpha}{\omega + \delta_c + \alpha + e}i_c\right)\left(1 - \frac{\alpha - \beta_{uc}\beta_{uc}}{\rho_{SR} + e}i_c\right)\left(1 + \frac{\beta_{cu}}{\delta_u + e}i_c\right) \quad (25)$$

Case 1: When $(\rho_{SR} + e) < \alpha$ and $0 < i_{c*}^* < 1$, the three roots of $f(i)$ are $i_1 = (\omega + \delta_c + \alpha + e)/\alpha$, $i_2 = (\rho_{SR} + e)/(\alpha - \beta_{uc}\beta_{uc})$, and $i_3 = -(\delta_u + e)/\beta_{cu}$. They all lie outside $[0, 1]$ when $R_0 > 1$. Furthermore, $f(0)=1$ and $f(1) = (\omega + \delta_c + e)(\rho_{SR} + e + \beta_{cu}\beta_{uc} - \alpha)(\delta_u + e + \beta_{cu})/(\omega + \delta_c + e + \alpha)(\rho_{SR} + e)(\delta_u + e) > R_0$.

Case 2: When $0 < i_{c*}^* < (\rho_{SR} + e)/\alpha$, the three roots of $f(i)$ all lie outside $[0, (\rho_{SR} + e)/\alpha]$ when $\rho_{SR} < (\omega + \delta_c + \alpha)$ and $R_0 > 1$. Furthermore, $f(0)=1$ and $f((\rho_{SR} + e)/\alpha) = \beta_{cu}\beta_{uc}(\omega + \delta_c + \alpha - \rho_{SR})(\alpha(\delta_u + e) + \beta_{cu}(\rho_{SR} + e))/\alpha^2(\omega + \delta_c + \alpha + e)(\delta_u + e) > R_0$.

These two cases lead to the conclusion that, when $R_0 > 1$, the line $y=R_0$ has exactly one intersection $(i_{c*}, f(i_{c*}))$ with the graph of $f(i_c)$ that satisfies Equation (22). So, we can obtain the following result.

Theorem 2. Suppose that $R_0 > 1$, then model (6) has an interior equilibrium $P_*(s_{u*}, i_{u*}, s_{c*}, i_{c*})$ and its coordinates satisfy Equations (21)-(23).

4 Analysis of the Population Sizes

In the previous sections, we investigate the global dynamics of the system (5) and obtain restrictive conditions of the parameter for RMD-virus. Are these conclusions compatible with the original system (3)? In this section, we focus on finding out the correlations between them.

We now study the dynamics of $(S_u(t), I_u(t), S_c(t), I_c(t), R(t))$, $n(t) = S_u(t) + I_u(t)$ and $N(t) = S_c(t) + I_c(t) + R(t)$, which are governed by systems (3) and (4). In fact, R does not appear in the first four equation system (3),

$$|\lambda E - J(P_0)| = \begin{bmatrix} \lambda + e & -\delta_u & 0 & \beta_{cu} \\ 0 & \lambda + (\delta_u + e) & 0 & -\beta_{cu} \\ 0 & \beta_{uc}s_{c1}^* & \lambda + (\rho_{SR} + e) & -\alpha s_{c1}^* \\ 0 & -\beta_{uc}s_{c1}^* & 0 & \lambda + (\omega + \delta_c + \alpha + e) \end{bmatrix} \quad (15)$$

$$\begin{aligned} V'|_{(5)} &= \beta_{uc}[\beta_{cu}s_u i_c - (\delta_u + e)i_u] + (\delta_u + e)[\beta_{uc}s_c i_u - (\omega + \delta_c + \alpha + e)i_c + \alpha i_c^2] \\ &= \beta_{uc}\beta_{cu}s_u i_c - \beta_{uc}(\delta_u + e)i_u + (\delta_u + e)\beta_{uc}s_c i_u - (\delta_u + e)(\omega + \delta_c + \alpha + e)i_c + (\delta_u + e)\alpha i_c^2 \\ &= i_c[\beta_{uc}\beta_{cu}s_u - (\delta_u + e)(\omega + \delta_c + \alpha + e) + (\delta_u + e)\alpha i_c] + i_u\beta_{uc}(\delta_u + e)(s_c - 1) \end{aligned} \quad (19)$$

which allows us to study the equivalent system

$$\begin{cases} \frac{dS_u(t)}{dt} = e n(t) - \beta_{cu}S_u(t)I_c(t)/N + \delta_u I_u(t) - \mu S_u(t) \\ \frac{dI_u(t)}{dt} = \beta_{cu}S_u(t)I_c(t)/N - \delta_u I_u(t) - \mu I_u(t) \\ \frac{dS_c(t)}{dt} = e N(t) + \delta_c I_c(t) - \beta_{uc}S_c(t)I_u(t)/n - \mu S_c(t) - \rho_{SR}S_c(t) \\ \frac{dI_c(t)}{dt} = \beta_{uc}S_c(t)I_u(t)/n - (\mu + \omega + \delta_c + \alpha) I_c(t) \\ \frac{dN(t)}{dt} = (e - \mu)N(t) - \alpha I_c(t) \\ \frac{dn(t)}{dt} = (e - \mu)n(t) \end{cases} \quad (26)$$

In its feasible region, $\Sigma = \{(S_u, I_u, S_c, I_c, N, n) \in R_+^6 | 0 \leq S_u + I_u \leq n, 0 \leq S_c + I_c \leq N\}$. Where, R_+^6 is a non-negative real number of 6-dimensional space.

If $e < \mu$ and $\alpha \geq 0$, or $e \leq \mu$ and $\alpha > 0$, Equation (26) implies that total host population $N(t) \rightarrow 0$ monotonically as $t \rightarrow \infty$ for all solutions with $I_u > 0$ and $I_c > 0$, namely the RMD-virus is initially present. If $e = \mu$ and $\alpha = 0$, $N(t)$ and $n(t)$ remain constant so that (26) degeneracy to a model with constant population, whose dynamic behaviors are very similar to (5) and (6).

In the rest of this section, we assume that $e > \mu$, $\alpha > 0$ or $e > \mu$, $\alpha = 0$. The latter does not incorporate RMD-virus related death in host population, and the whole population will increase exponentially.

Let $f(x) = \left(1 - \frac{\alpha}{\omega + \delta_c + \alpha + e}x\right) \left(1 - \frac{\alpha - \beta_{uc}\beta_{cu}}{\rho_{SR} + e}x\right) \left(1 + \frac{\beta_{cu}}{\delta_u + e}x\right)$, where $f(x)$ is the cubic polynomial defined in (25). Let $\tilde{R}_0 = f((e - \mu)/\alpha)$, the parameters \tilde{R}_0 play key roles in the dynamics of the population sizes.

Theorem 3. If $\tilde{R}_0 \neq R_0$, system (26) has only a trivial equilibrium $\tilde{P}_0(0, 0, 0, 0, 0, 0)$. If $\tilde{R}_0 = R_0$ system (26) has a line of equilibrium points:

$$\begin{aligned} &\left(\frac{e\tilde{n}_* - \mu\tilde{I}_{u*}}{\mu}, \frac{(\omega + \alpha + \mu + \delta_c)(e - \mu)(\mu + \rho_{SR})\tilde{n}_*}{\beta_{uc}[e + (\omega + \alpha + \mu + \delta_c)(e - \mu)/\alpha]}, \right. \\ &\left. \frac{[e + (\omega + \alpha + \mu + 2\delta_c)(e - \mu)/\alpha]\tilde{N}_*}{\mu + \rho_{SR}}, \frac{(e - \mu)\tilde{N}_*}{\alpha}, \right. \\ &\left. \tilde{N}_*, \tilde{n}_* \right). \end{aligned}$$

Where, \tilde{N}_* and \tilde{n}_* are arbitrary positive number. positive number.

Proof. We now consider the case $e > \mu$ and $\alpha > 0$. System (26) also has trivial equilibrium $\tilde{P}_0(0, 0, 0, 0, 0, 0)$.

Our interest is to determine whether there is a LE in system (26). Suppose $\tilde{P}_*(\tilde{S}_{u*}, \tilde{I}_{u*}, \tilde{S}_{c*}, \tilde{I}_{c*}, \tilde{N}_*, \tilde{n}_*)$ is a LE of system (26). Let the right-hand side of (21) equal to zero, we have

$$\begin{aligned} 0 &= e - \beta_{cu} \frac{\tilde{S}_{u*}}{\tilde{n}_*} \frac{\tilde{I}_{c*}}{\tilde{N}_*} + \delta_u \frac{\tilde{I}_{c*}}{\tilde{n}_*} - \mu \frac{\tilde{S}_{u*}}{\tilde{n}_*} \\ \tilde{S}_{u*} &= \frac{e\tilde{n}_* - \mu\tilde{I}_{u*}}{\mu} \Rightarrow \frac{\tilde{S}_{u*}}{\tilde{n}_*} = \frac{e - \mu\tilde{I}_{u*}/\tilde{n}_*}{\mu} \\ \frac{\tilde{I}_{u*}}{\tilde{n}_*} &= \frac{(\omega + \alpha + \mu + \delta_c)\tilde{I}_{c*}/\tilde{N}_*}{\beta_{uc}\tilde{S}_{c*}/\tilde{N}_*} \\ \tilde{S}_{c*} &= \frac{e\tilde{N}_* + (\omega + \alpha + \mu + \delta_c)\tilde{I}_{c*}}{\mu + \rho_{SR}} \\ \Rightarrow \frac{\tilde{S}_{c*}}{\tilde{N}_*} &= \frac{e + (\omega + \alpha + \mu + 2\delta_c)\tilde{I}_{c*}/\tilde{N}_*}{\mu + \rho_{SR}} \\ \frac{\tilde{I}_{c*}}{\tilde{N}_*} &= \frac{e - \mu}{\alpha} \end{aligned}$$

Eliminating \tilde{S}_{u*} , \tilde{I}_{u*} , \tilde{S}_{c*} , \tilde{I}_{c*} , \tilde{N}_* and \tilde{n}_* from these following condition

$$\frac{\beta_{cu}e(e - \mu)}{\alpha\mu} = \frac{(\omega + \alpha + \mu + \delta_c)(e - \mu)(\mu + \rho_{SR})}{\beta_{uc}[e + (\omega + \alpha + \mu + 2\delta_c)(e - \mu)]} [(\delta_u + e) + \frac{\beta_{cu}(e - \mu)}{\alpha}] \quad (27)$$

which is equivalent to Equation (28).

If $R_0 \leq 1$, then the infected hosts vanish. The RMD-virus does not suppress the growth of the host population so that $N(t)$, $n(t)$, $S_c(t)$, $S_u(t)$ tend to infinity exponentially with an exponential rate $e - \mu$ as $t \rightarrow \infty$.

Theorem 1 shows that when $\tilde{R}_0 \leq 1$, $(s_u(t), i_u(t), s_c(t), i_c(t), r(t)) \rightarrow (1, 0, e/(e + \rho_{SR}), 0, \rho_{SR}/(e + \rho_{SR}))$ exponentially as $t \rightarrow \infty$. According to system (4), we let

$$N'(t) = ((e - \mu) - \alpha i_c)N. \quad (29)$$

We therefore claim that $N(t)$ increases exponentially due to the fact that $i_c(t) \rightarrow 0$ as $t \rightarrow \infty$ [1]. The trajectories of $S_c(t)$ and $R(t)$ tend to infinity due to the facts that $s_c(t) = S_c(t)/N(t) \rightarrow e/(e + \rho_{SR})$ and $r(t) = R(t)/N(t) \rightarrow \rho_{SR}/(e + \rho_{SR})$ respectively, which are independent of \tilde{R}_0 . So, we can see the behavior of $I_u(t)$, $I_c(t)$ and $R(t)$. \square

$$\begin{aligned}
V_2'|_{(5)} &= \beta_{uc}[\beta_{cu}s_u i_c - (\delta_u + e)i_u] + (\delta_u + e)[\beta_{uc}s_c i_u - (\omega + \delta_c + \alpha + e)i_c + \alpha i_c^2] \\
&= \beta_{uc}\beta_{cu}s_u i_c - \beta_{uc}(\delta_u + e)i_u + (\delta_u + e)\beta_{uc}s_c i_u - (\delta_u + e)(\omega + \delta_c + \alpha + e)i_c + (\delta_u + e)\alpha i_c^2 \\
&= i_c[\beta_{uc}\beta_{cu}s_u - (\delta_u + e)(\omega + \delta_c + \alpha + e) + (\delta_u + e)\alpha i_c] + i_u\beta_{uc}(\delta_u + e)(s_c - 1)
\end{aligned} \tag{20}$$

$$\begin{aligned}
&e\beta_{uc}\beta_{cu}i_{c*} - [(\omega + \delta_c + \alpha + e)i_{c*} - \alpha i_{c*}^2] \times [(\rho_{SR} + e) - \alpha i_{c*} + \beta_{uc}\beta_{cu}i_{c*}] \times [(\delta_u + e) - \beta_{cu}i_{c*}] = 0 \\
&\Rightarrow [(\omega + \delta_c + \alpha + e) - \alpha i_{c*}] \times [(\rho_{SR} + e) - \alpha i_{c*} + \beta_{uc}\beta_{cu}i_{c*}] \times [(\delta_u + e) + \beta_{cu}i_{c*}] = e\beta_{uc}\beta_{cu} \\
&\Rightarrow \left(1 - \frac{\alpha}{\omega + \delta_c + \alpha + e}\right) \left(1 - \frac{\alpha - \beta_{uc}\beta_{cu}}{\rho_{SR} + e}\right) \left(1 + \frac{\beta_{cu}}{\delta_u + e}i_{c*}\right) = R_0
\end{aligned} \tag{23}$$

Theorem 4. Suppose $R_0 > 1$ and $\alpha < \beta_{uc}$. As $t \rightarrow \infty$:

When $\tilde{R}_0 > R_0$, $(S_u(t), I_u(t), S_c(t), I_c(t), R(t), N(t), n(t)) \rightarrow (\infty, \infty, \infty, \infty, \infty, \infty, \infty)$;

When $\tilde{R}_0 < R_0$, $(S_u(t), I_u(t), S_c(t), I_c(t), R(t), N(t), n(t)) \rightarrow (0, 0, 0, 0, 0, 0, 0)$;

When $\tilde{R}_0 = R_0$, $(S_u(t), I_u(t), S_c(t), I_c(t), R(t), N(t), n(t)) \rightarrow (\tilde{S}_{u*}, \tilde{I}_{u*}, \tilde{S}_{c*}, \tilde{I}_{c*}, \tilde{R}_*, \tilde{N}_*, \tilde{n}_*)$.

Proof. Since $\tilde{R}_0 = f\left(\frac{e-\mu}{\alpha}\right)$ and $R_0 = f(i_{c*})$, from the analysis of function f in Subsection 3.3, we know that $\tilde{R}_0 > R_0$ or $\tilde{R}_0 < R_0$ is equivalent to the relations $e - \mu - \alpha i_{c*} > 0$ or $e - \mu - \alpha i_{c*} < 0$ respectively. $N' = (e - \mu)N - \alpha I_c N$ can be rewritten as

$$N' = [(e - \mu - \alpha i_{c*}) - \alpha(i_c - i_{c*})]N. \tag{30}$$

If $e - \mu - \alpha i_{c*} > 0$, $N(t) \rightarrow \infty (t \rightarrow \infty)$ in (30), which implies $(S_u(t), I_u(t), S_c(t), I_c(t), R(t)) \rightarrow (\infty, \infty, \infty, \infty, \infty)$ as $t \rightarrow \infty$; if $e - \mu - \alpha i_{c*} < 0$, $N(t) \rightarrow 0 (t \rightarrow \infty)$ in (30), which implies $(S_u(t), I_u(t), S_c(t), I_c(t), R(t)) \rightarrow (0, 0, 0, 0, 0)$ as $t \rightarrow \infty$; if $e - \mu - \alpha i_{c*} = 0$, $N(t) \rightarrow \tilde{N}_* (t \rightarrow \infty)$ in (30), which implies as $(S_u(t), I_u(t), S_c(t), I_c(t), R(t)) \rightarrow (\tilde{S}_{u*}, \tilde{I}_{u*}, \tilde{S}_{c*}, \tilde{I}_{c*}, \tilde{R}_*)$.

When $e - \mu > 0$ and $\alpha = 0$, system (26) has only the trivial equilibrium $\tilde{P}_*(0, 0, 0, 0, 0, 0)$. In this case, $(S_u(t), I_u(t), S_c(t), I_c(t), R(t), N(t), n(t)) \rightarrow (\infty, \infty, \infty, \infty, \infty, \infty, \infty)$. Hence the trivial equilibrium \tilde{P}_* is unstable. \square

5 Simulation Experiment

We first introduce the numerical experiment environments and then provide some results based on RMD-virus propagation control. As shown in Table 3, the parameters of RMD-SIR have two types: the system and the state transition parameters.

Generally, the values of the system parameters were fixed in the experiments unless we explicitly specified the changes. Moreover, the initial state of the system, i.e., $S_c(0), I_c(0), R(0), S_u(0), I_u(0)$, can have a great impact for the propagation of RMD-virus. Typically, we assume that $I_c(0)$ is relatively low at the beginning of the RMD-virus propagation. We set $S_c(0), I_c(0), R(0), S_u(0), I_u(0)$ value are 9990, 10, 0, 5000, 0 respectively. The antivirus

Table 3: Parameters used in experiments

Parameter	Value	Parameter	Value
$N(0)$	10000	ρ_{SR}	Not fixed
$n(0)$	5000	α	Not fixed
μ	0.0002	e	0.005
$R(0)$	$N-S(0)-I(0)$	$I(0)$	10

countermeasure of real-time immunization is relative low with $\rho_{SR}=0.002$.

5.1 Effect of RMD-virus Control with R_0

When $R_0 < 1$, the RVFE is globally asymptotically stable, as show in Figure 2.

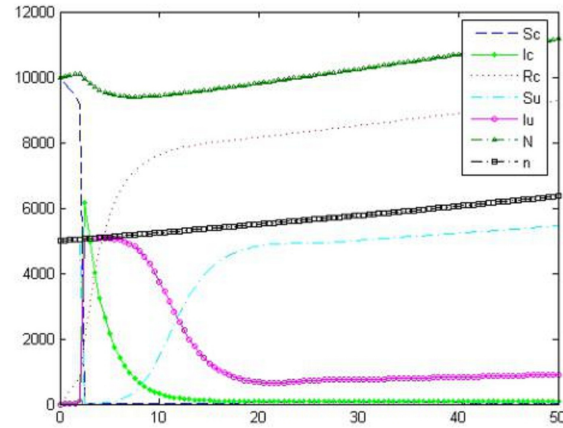


Figure 2: RMD-virus propagation results with $\hat{R}_0=0.85$ and $R_0=0.605$. The parameter values are $e=0.005$, $\mu=0.0002$, $\rho_{SR}=0.002$, $\alpha=0.06$, $\beta_{uc}=0.15$ and $\beta_{cu}=0.16$

In Figure 2, the host I_c and S_c states eventually tend to 0, and R state increases with time t and the total number N . The proposed model is stable with $R_0 < 1$. From the Figure 2, we can draw several conclusions:

- 1) I_u and S_u are basic opposite trend, there are two reasons: one is RMD only has two states, another is

$$\begin{cases} s_{u*} = 1 - i_{u*} \\ i_{u*} = \frac{\beta_{cu} i_{c*}}{\beta_{cu} i_{c*} + (\delta_u + e)} \\ s_{c*} = \frac{e[\beta_{cu} i_{c*} + (\delta_u + e)]}{\beta_{cu} \beta_{uc} i_{c*} + [(\rho_{SE} + e) - \alpha i_{c*}] \times [\beta_{cu} i_{c*} + (\delta_u + e)]} \end{cases} \quad (24)$$

$$\widetilde{R}_0 = f\left(\frac{e - \mu}{\alpha}\right) = \left(1 - \frac{e - \mu}{\omega + \delta_c + \alpha + e}\right) \left(1 - \frac{(\alpha - \beta_{uc} \beta_{cu})(e - \mu)}{(\rho_{SR} + e)\alpha}\right) \left(1 + \frac{\beta_{cu}(e - \mu)}{(\delta_u + e)\alpha}\right) = R_0 \quad (28)$$

the value of μ is very small, only 0.00022. But I_u does not tend to 0 with time t , because new RMDs are assumed that S_u state and RMD dose not have R state.

- 2) When almost all of RMD will be infected, the number n in Figure 2 is close to 5000 at climax, it is the total number of RMD. As RMD can not detect and remove viruses, when outbreak of RMD-virus takes place, almost all users have not taken countermeasures, or there are no countermeasures appearing. So at this moment, all RMDs that contact with the infected hosts will be infected.
- 3) With the moment of I_c climax, peak time of I_u also will come. They are basically at the same time, even early than I_c . That is, when outbreak of RMD-virus propagation between I_c and I_u takes place, the two objects I_c and I_u are the same important, the RMD-virus propagation will not outbreak if lack any one.
- 4) The peak time of I_u sustains longer than I_c , because it depends on hosts to clear RMD-virus or the format of RMD-virus. That is to say, resistant RMD-virus is more difficult than host virus.

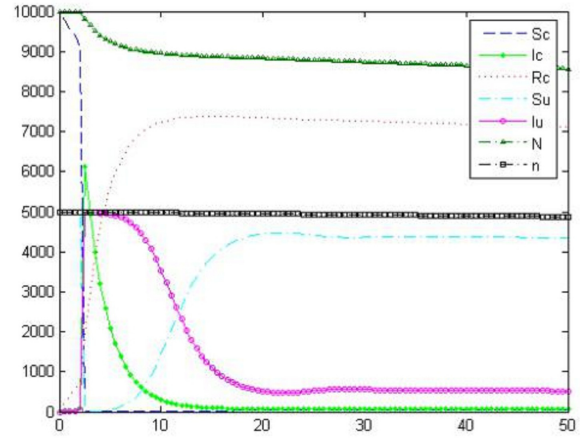


Figure 3: RMD-virus propagation results with $e=0.005$, $\mu=0.0055$, $\alpha=0.06$, $e-\mu<0$

5.2 Impact of e and u on $N(t)$ and $n(t)$

We know that, if $e < \mu$ and $\alpha \geq 0$ or $e \leq \mu$ and $\alpha > 0$, the total host population $N(t) \rightarrow 0$ monotonically as $t \rightarrow \infty$ for all solutions with $I_u > 0$ and $I_c > 0$. As shown in Figure 3, $N(t)$ and $n(t)$ descent with time t , and R and S_u also descent with time t , they all tend to 0 as $t \rightarrow \infty$.

If $e=\mu$ and $\alpha=0$, $N(t)$ and $n(t)$ remain constant so that system (26) degenerates into a model with constant population, their dynamic behaviors are very similar to (5) and (6). As shown in Figure 4, two straight lines of $N(t)$ and $n(t)$ are horizontal, namely they are constant. R state and $N(t)$ are almost parallel, S_u and I_u are also almost parallel with $n(t)$ to later. However, the number of hosts in R state does not equal the N , which indicates that not all the hosts have the ability of immunity, even the RMD-virus has been controlled.

This situation shows that the host population does not consider RMD-virus-related death, so impacting factors on $N(t)$ and $n(t)$ are same, namely $e-\mu$. On other hand, in the whole simulation process, the values of e and μ do not change, and the increasing speed of $N(t)$ and $n(t)$

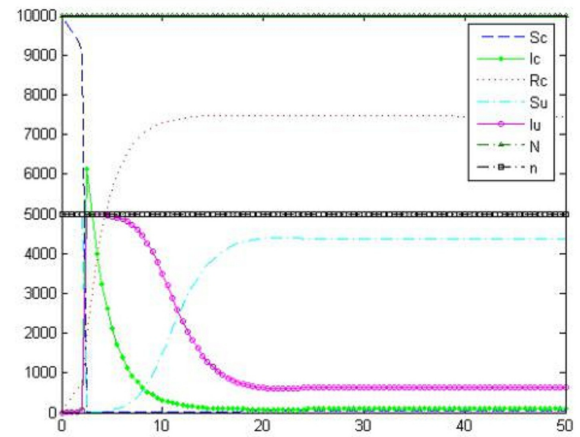


Figure 4: RMD-virus propagation results with $e-\mu=0$ and $\alpha=0$

is uniform. As shown in Figure 5, the increasing rate of $N(t)$ and $n(t)$ are essentially the same.

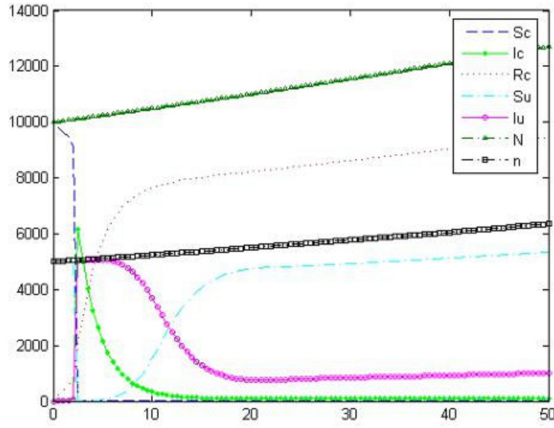


Figure 5: RMD-virus propagation results with $e-\mu>0$ and $\alpha=0$

5.3 Impact of β_{uc} and β_{cu} on Model

We have known that β_{uc} indicates the RMD-virus propagate probability from RMD to host, β_{cu} indicates propagate probability from host to RMD. The bigger β_{uc} means that few users take countermeasures against the RMD-virus and little ability to remove the RMD-virus in initial period. The bigger β_{cu} means that more and more infected, but the solution countermeasures is inefficient, and which indicates that the virus outbreak is coming. The relationship between β_{uc} and β_{cu} whole periods of propagation process

These analytic results can help researchers to study various fact of RMD-virus propagation and new effective countermeasure to clear RMD-virus. So, the study of the relationship between β_{uc} and β_{cu} is necessary. If constant, we let $\lambda = \beta_{cu}/\beta_{uc}$. The value of λ impacts simulation results of the RMD-SIR model. Figure 6 shows simulation results when changing λ .

From Figure 6, we can see that λ can impact the speed of I_u declining. The relationship between β_{uc} and β_{cu} impacts the whole speed of removing RMD-virus. Therefore, this is key point in the RMD-virus propagation model. Through correctly handling this relationship, we can quickly eliminate RMD-virus. In Figure 6(a), the peak value of I_c is about 7800, but in Figure 6(b), it is only about 6300, and the minimum value of I_u is less than Figure 6(a)'s. The bigger λ indicates β_{cu} is larger than β_{uc} , that is to say, the RMD-virus propagation from host to RMD is faster than propagation speed from RMD to host, which can cause more RMDs infected by infected hosts. After RMD-virus breaking out, I_c and I_u should decline with with effective countermeasure, but the higher

β_{cu} can cause more RMDs infected, at this time, remove RMD-virus from RMDs need some time. For example, in actual life, the RMDs also are infected after being cleared. In other words, we should keep λ with a smaller value; which can faster eliminate RMD-virus. To this purpose, β_{cu} should keep smaller. So relative to β_{uc} , β_{cu} is more worth considerable.

6 Conclusion

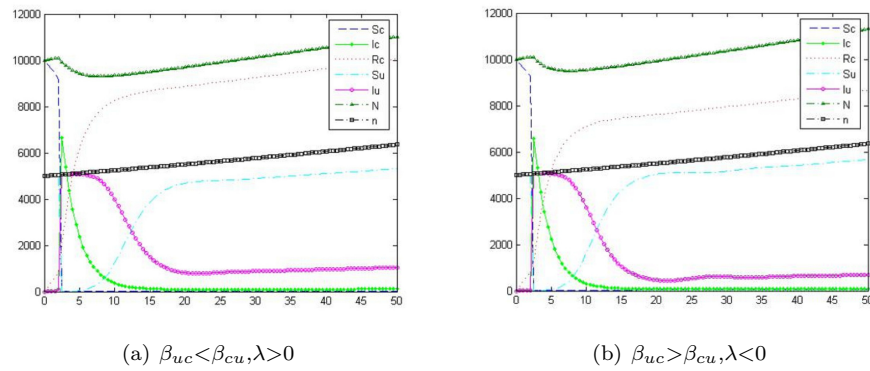
The objective of this paper is to establish the RMD-virus propagation model, and then to find out control methods of RMD-virus propagation for eliminating virus. We proposed the RMD-SIR model with varying population size based on epidemiologic model SIR and obtained the conditions by the asymptotically stability of RVFE. We get the basic reproduction number R_0 , furthermore, other threshold parameters, e.g. \hat{R}_0 and \bar{R}_0 , are also obtained govern the RMD-virus propagation, which involve the total number of infective nodes and their proportion in all nodes. We analyzed the trend of each state in RMD-SIR model with varying $N(t)$ and $n(t)$. The simulation results show that the proposed model can help us for understanding and simulating RMD-virus propagation. The future work will focus on exploring more complex RMD-virus propagation model, which may require more specify parameters to analyze the more effective method of controlling RMD-virus propagation. We will also study some countermeasures by building up a practical and effective defense system against RMD-virus.

Acknowledgments

This work was supported by the fundamental research funds for central university (Grant No. CCNU15GF007).

References

- [1] D. Gilbarg and N. S. Trudinger *Elliptic Partial Differential Equations of Second Order*, 2015.
- [2] C. Jin, S. W. Jin, and H. Y. Tan, "Computer virus propagation model based on bounded rationality evolutionary game theory," *Security and Communication Networks*, vol. 16, no. 2, pp. 210–218, 2013.
- [3] C. Jin, J. Liu, and Q. H. Deng, "Network virus propagation model based on effects of removing time and user vigilance," *International Journal of Network Security*, vol. 9, no. 2, pp. 156–163, 2009.
- [4] V. V. Klinshov, V. I. Nekorkin, and J. Kurths, "Stability threshold approach for complex dynamical systems," *New Journal of Physics*, vol. 18, no. 1, 2016.
- [5] A. Korobeinikov and P. K. Maini, "A lyapunov function and global properties for sir and seir epidemiological models with nonlinear incidence," *Mathematical Biosciences and Engineering*, vol. 1, no. 1, pp. 57–60, 2004.

Figure 6: RMD-virus propagation results impacted by β_{uc} and β_{cu}

- [6] B. K. Mishra, "Mathematical model on attack of worm and virus in computer network," *International Journal of Future Generation Communication and Networking*, vol. 9, no. 6, pp. 245–254, 2016.
- [7] Y. Muroya and T. Kuniya, "Global stability of nonresident computer virus models," *Mathematical Methods in the Applied Sciences*, vol. 38, no. 2, pp. 281–295, 2015.
- [8] S. P. Thunga and R. K. Neelisetti, "Identifying metamorphic virus using n-grams and hidden markov model," *International Conference on Advances in Computing, Communications and Informatics*, pp. 2016–2022, 2015.
- [9] F. W. Wang, Y. K. Zhang, C. G. Wang, J. Ma, and S. Moon, "Stability analysis of a seiqv epidemic model for rapid spreading worms," *Computers & Security*, vol. 29, no. 4, pp. 410–418, 2010.
- [10] L. X. Yang and X. Yang, "The spread of computer viruses under the influence of removable storage devices," *Applied Mathematics and Computation*, vol. 219, no. 8, pp. 3914–3922, 2012.
- [11] L. X. Yang, X. Yang, L. Wen, and J. Liu, "A novel computer virus propagation model and its dynamics," *International Journal of Computer Mathematics*, vol. 89, no. 17, pp. 2307–2314, 2012.
- [12] H. Yuan and G. Q. Chen, "Network virus-epidemic model with the point-to-group information propagation," *Applied Mathematics and Computation*, vol. 206, no. 1, pp. 357–367, 2008.
- [13] Q. Zhu, X. Yang, L. X. Yang, and X. Zhang, "A mixing propagation model of computer viruses and countermeasures," *Nonlinear Dynamics*, vol. 73, no. 3, pp. 1433–1441, 2013.

Biography

Cong Jin is a full professor of the school of computer, Central China Normal University, China. She has published more than 150 papers on information security, signal processing, and algorithm design and analysis. Her main research interests include computer network security, digital image processing, and software reliability prediction, etc.

Xiaoyan Wang is a teacher at the department of electronic information, Zhengzhou Electric Power College, China. She has published nearly 10 papers on information security. Her main research interests include network security, and computer virus detection, etc.

Provably Authenticated Group Key Agreement based on Braid Groups – The Dynamic Case

Pipat Hiranvanichakorn

Graduate School of Applied Statistics, National Institute of Development Administration Bangkok

118, Seri Thai Road, Klong-Chan, Bangkok, Bangkok 10240, Thailand

(Email: pipat@as.nida.ac.th)

(Received Jan. 28, 2016; revised and accepted Apr. 23 & July 31, 2016)

Abstract

Most group key agreement protocols make use of modular exponential operations which require extensive computing resources in devices. Thus, they are unsuitable for resource-constrained devices such as mobile phones, smart cards and intelligent watches. This paper proposes a group key agreement protocol based on braid groups which requires only multiplication operations. The proposed protocol is a scalable one and needs only two rounds for setting a secure group communication. To prevent a man-in-the-middle attack, exchanged messages are simply authenticated by using users' long-term public and private keys instead of signatures. Authentication proofs are also made by using well-known BAN logic. The protocol is designed for dynamic group communication in which member join, member leave, group merge and group partition are discussed. The proposed algorithms take advantage of precomputed values achieved in previous sessions to update keys in subsequent session. This makes the scheme generate fewer communicating messages and lessens user devices' computation. Comparisons of security and complexity among several two-round protocols are also discussed in this article.

Keywords: Authenticated group key agreement, BAN authentication logic, braid groups

1 Introduction

Group communication has been widely studied in recent times because it has many commercial applications. These include, amongst others, audio-video conference, pay-per-view, audio-video broadcasting, stock quote services, collaborate tasks, and so on. Many of these applications require security services such as, data confidentiality, data integrity and data authentication, during transmission. Group key management can be used for generating group session key in order to provide secure communication. There are two main types of group key management protocols: group key distribution and group key agreement. In group key distribution scheme,

the group session key is generated and distributed by a central trusted party via secure channel. The main disadvantage of this scheme is that it needs both a trust authority as well as the availability of secure channels. Furthermore, the scheme suffers from security risks when there is a single point of failure. A group key agreement scheme, by contrast, allows all authorized group members to work together to establish a group session key. These schemes [1, 3, 5, 6, 9, 12, 15, 16, 18, 21] have been studied widely in recent years because they are considered to be scalable.

Most group key agreement protocols are based on Diffie-Hellman as well as Elliptic Curve two-party key exchange protocol and they require exponential operations [3, 7, 8, 9, 12, 14, 15, 16, 18]. However, there are studies based on braid groups which require only multiplication operations [1, 6, 10, 11, 13, 19, 20]. For instance, Lee et al. [13] has proposed an authenticated group key agreement protocol for designated groups based on braid groups. In authenticated group key protocol, each member is assured that no users outside the group can find out the session key. The key disadvantage of this work is that the number of rounds needed in the work is linear to the number of group members. In each round, some calculated values have to be sent from user i to user $i + 1$ for further calculation. Therefore the scheme can suffer from long delays at some participants in the group. In a recent paper [1], Aneksrup and Hiranvanichakorn proposed a dynamic group key agreement based on braid groups and a key tree structure. In a dynamic group, parties may join and leave the group any given number of times. This scheme needs $O(n)$ rounds for n -parties group initialization, constant rounds in the case that the user n is the group director for join operation, and $O(n)$ rounds in worst case for leave operation. However, an $O(n)$ -round protocol is considered not to be scalable and suffers from long network delays. To get around these problems, some researchers have turned to constant-round protocols. Nevertheless, those works are still based on exponential operation cryptosystems [7, 8, 12, 14, 21].

In the paper by Hwang et al. [8], a framework for extending a two-party key exchange protocol to a contrib-

tory group key one has been proposed by using a ring structure of participants. Hwang et al. applied their work to Diffie-Hellman key exchange, resulting in a two-round group key agreement protocol. However, Lee et al. [14] pointed out that Hwang et al.'s scheme has some flaws when applied to a dynamic group. Lee et al. also introduced an improvement to the algorithm to get rid of the flaws. Nonetheless, it can be shown in this paper that Lee et al.'s algorithm as well as several ring-structure protocols still suffer some flaws when they are applied in dynamic environment.

In this paper, an authenticated group key agreement protocol using braid group cryptography is proposed. The proposed protocol needs only two rounds and uses a ring structure of participants. Authentication between communicating users can be simply done by using users' long-term private and public keys instead of digital signature scheme. The protocol is a dynamic case in which member join, member leave, group merge and group partition are discussed. In the protocol, precomputed values in previous sessions are used for updating session keys in subsequent session. This can generate fewer exchanged messages and lessen users' computation than previously proposed protocols. In addition, an authentication proof using BAN authentication logic [4, 17] is given in this article. The proof for the proposed group key agreement is different from the authentication proof given in Lee et al. [14]. Security and performance analysis of the proposed protocol are also discussed. Finally, comparisons among ring-structure protocols are illustrated.

The rest of this paper is organized as follows. Section 2 provides some preliminaries of braid group cryptography. A provably authenticated key exchange protocol based on braid groups is described in Section 3. In Section 4, some reviews of previous group key agreement protocols and their security analysis are given. The proposed authenticated group key agreement protocol for dynamic group is described in Section 5. Section 6 offers a security analysis of the proposed protocol showing the authentication proof. In Section 7, security analysis of the protocol against some well-known attacks and some comparisons among ring-structure protocols are provided. The conclusion is given in Section 8.

2 Preliminaries

This section gives a brief description of braid groups, some hard problems in braid groups as well as a well-known key exchange protocol proposed by Ko et al. [11]. For more information on braid groups, please refer to papers [2, 10, 11].

The n -braid group B_n is the group generated by generators $\sigma_1, \dots, \sigma_{n-1}$ with the relations,

- 1) $\sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j$ where $|i - j| = 1$, e.g. $\sigma_3 \sigma_2 \sigma_3 = \sigma_2 \sigma_3 \sigma_2$;
- 2) $\sigma_i \sigma_j = \sigma_j \sigma_i$ where $|i - j| \geq 2$, e.g. $\sigma_5 \sigma_3 = \sigma_3 \sigma_5$.

Each element of the group B_n is called an n -braid. There are a number of mathematically hard problems in braid groups, one of the most famous of which is the Generalized Conjugacy Search Problem (GCSP). GCSP states that two braids x and y are conjugate if there exists a braid a such that $y = axa^{-1}$, where a^{-1} is the inverse of a . For $m < n$, B_m which is a subgroup of B_n generated by $\sigma_1, \dots, \sigma_{m-1}$, the hardness of GCSP is as follows.

- Given $(x, y) \in B_n \times B_n$ such that $y = bxb^{-1}$ for some $b \in B_m$, $m \leq n$.
- The objective is to find $a \in B_m$ such that $y = axa^{-1}$.

It is considered to be the case that, for sufficiently large braids, it is easy to compute y from b and x . However, exponential time is needed to compute a , even when y and x are known.

In paper [11], Ko et al. has also stated that for $a, b \in B_n$, it is hard to guess a or b from ab .

GCSP is applied in several cryptographic protocols [1, 6, 10, 11, 13, 19, 20]. There are also several attempts to solve GCSP in braid groups. In a paper [10], Ko et al. has stated that the attacks on braid cryptosystems were successful because the current ways of random key generation almost always result in weaker instances of the conjugacy problem. They then proposed several ways of generating secure keys for braid cryptography.

2.1 Ko-Lee Key Agreement Protocol

Ko et al. has proposed a well-known key agreement protocol based on GCSP. The protocol includes the following steps.

- 1) Preparation step: When A (lice) and B (ob) want to establish a shared key, an appropriate pair of integers (l, r) and a sufficiently complicated $(l + r)$ braid $x \in B_{l+r}$ are selected and published as system parameters.
- 2) Key agreement implementation:
 - (a) A chooses a random secret braid $a \in LB_l$, where LB_l is a subgroup of B_{l+r} and generated by $\sigma_1, \dots, \sigma_{l-1}$. A then sends $y_1 = axa^{-1}$ to B . The braid y_1 is considered to be A 's public key.
 - (b) B chooses a random secret braid $b \in LB_r$, where LB_r is a subgroup of B_{l+r} and generated by $\sigma_{l+1}, \dots, \sigma_{l+r-1}$. B then sends $y_2 = bxb^{-1}$ to A . The braid y_2 is also considered to be B 's public key. By the commutative property of braid groups, we have $ab = ba$.
 - (c) Upon receiving y_2 , A computes the shared key, $k_{AB} = ay_2a^{-1} = abxb^{-1}a^{-1}$.
 - (d) B can also compute $k_{AB} = by_1b^{-1} = baxa^{-1}b^{-1} = abxb^{-1}a^{-1}$.

In the above scheme, even if $E(\text{ve})$ sees the message axa^{-1} (and bxb^{-1}), she needs exponential time to compute a (and b). Therefore, it is very hard for her to find out the shared key.

3 Provably Authenticated Key Exchange Protocol

As the public keys of A and B described in Subsection 2.1 are not authenticated, the key exchange scheme is vulnerable to man-in-the-middle attack. If $E(\text{ve})$ substitutes A (or B)'s public key with her public key, then the protocol fails.

This section describes an authenticated key exchange protocol in which each party's public key is authenticated and sent to the other party. By using the authenticated public key, a secure scheme for key exchange can be obtained. This proposed protocol is based on the scheme described in paper [13]. A formal proof of the correctness of the proposed scheme based on BAN authentication logic [4] is also given here. The notations used in this protocol are listed in Table 1.

Table 1: Notations

Notations	Description
$x \in B_{l+r}$	A sufficiently complicated $(l+r)$ -braid;
$\alpha_A \in LB_l$	A long-term private key of A , where LB_l is a sub group of B_{l+r} and generated by $\sigma_1, \dots, \sigma_{l-1}$;
$\alpha_B \in LB_r$	A long-term private key of B , where LB_r is a sub group of B_{l+r} and generated by $\sigma_{l+1}, \dots, \sigma_{l+r-1}$;
$P_A = \alpha_A x \alpha_A^{-1}$	A long-term public key of A ;
$P_B = \alpha_B x \alpha_B^{-1}$	A long-term public key of B ;
$\beta_A \in LB_l$	A session private key of A ;
$\beta_B \in LB_r$	A session private key of B ;
$p_A = \beta_A x \beta_A^{-1}$	A session public key of A ;
$p_B = \beta_B x \beta_B^{-1}$	A session public key of B ;
K_{AB}	A long-term common secret shared by A and B ;
k_{AB}	A shared session key of A and B .

The steps of the protocol are as follows.

- (a) A uses α_A and P_B to compute

$$\begin{aligned} K_{AB} &= \alpha_A P_B \alpha_A^{-1} \\ &= \alpha_A \alpha_B x \alpha_B^{-1} \alpha_A^{-1}. \end{aligned}$$

- (b) B uses α_B and P_A to compute

$$\begin{aligned} K_{AB} &= \alpha_B P_A \alpha_B^{-1} \\ &= \alpha_B \alpha_A x \alpha_A^{-1} \alpha_B^{-1} \\ &= \alpha_A \alpha_B x \alpha_B^{-1} \alpha_A^{-1}. \end{aligned}$$

- (c) A computes authenticated public key $Ap_A = K_{AB}(\beta_A x \beta_A^{-1})K_{AB}^{-1}$ and sends it to B .

- (d) Upon receiving Ap_A , B uses K_{AB} which he has computed in step (b) to get $p_A = \beta_A x \beta_A^{-1}$. B can then compute the shared session key $k_{AB} = \beta_B \beta_A x \beta_A^{-1} \beta_B^{-1} = \beta_A \beta_B x \beta_B^{-1} \beta_A^{-1}$.

- (e) In a similar way to Steps (c) and (d), when A receives $Ap_B = K_{AB}(\beta_B x \beta_B^{-1})K_{AB}^{-1}$ from B , she can also compute the shared session key, $k_{AB} = \beta_A \beta_B x \beta_B^{-1} \beta_A^{-1}$.

According to the described scheme, $E(\text{ve})$ may intercept both Ap_A and Ap_B but she can substitute neither p_A nor p_B with her public key because she does not know K_{AB} . Therefore, the proposed scheme is considered to be immune to man-in-the-middle attack.

3.1 Proof of Authenticated Public Key

In the authenticated two-party key exchange scheme described above, each user has to believe the session public key received from the other party. Therefore, a proof of authenticated public key, which B has received from A , is done using BAN logic [4]. The notations used in this paper follow those of BAN logic.

In the above protocol, A sends an authenticated public key to B , i.e. $A \rightarrow B : K_{AB}(p_A)K_{AB}^{-1}$. The message can be transformed into the idealized form as $A \rightarrow B : \{p_A\}_{K_{AB}}$.

The goal is to prove that B believes p_A . To analyze the protocol, the following assumptions are made. B believes $A \xrightarrow{K_{AB}} B$, B believes fresh (p_A) , B believes A controls (p_A) . The steps of the proof are as follows:

- 1) B believes $A \xrightarrow{K_{AB}} B$ and B sees $\{p_A\}_{K_{AB}}$, then B believes A said p_A .
- 2) B believes fresh (p_A) and B believes A said p_A , then B believes A believes p_A .
- 3) B believes A controls p_A and B believes A believes p_A , then B believes p_A .

In the similar way, we can obtain the proof that A also believes p_B .

4 Security Analysis of Some Group Key Agreement Protocols

In the paper [1], an authenticated group key agreement protocol based on braid groups has been proposed. However, the number of rounds needed in the paper is linear to the number of group members. In each round some calculated values have to be sent from user i to user $i+1$ for further calculation. Therefore, the scheme can suffer from some long delays at some participants in the group.

In the paper [8], Hwang et al. has proposed a group key exchange scheme which needs only two rounds. The protocol is supposed to be scalable. However, in paper [14], Lee et al. has shown that Hwang et al.'s scheme does not provide forward and backward secrecy in dynamic environment. Lee et al. also gives an improvement of the scheme to remedy the problems.

In the following subsections, a brief description of Lee et al.'s scheme and a demonstration that the scheme does not preserve backward secrecy is given. Here, backward secrecy means that a new member should not be able to decrypt the multicast data sent before his joining, and forward secrecy means that a former member should not be able to decrypt the multicast data sent after his leaving [5]. In addition, security analysis of other two works [7, 12] using ring structure of participants is also discussed.

4.1 Lee et al.'s Scheme

In Lee et al.'s scheme [14], when users $U_1, \dots, U_i, \dots, U_n$ want to establish a secure communication, each member U_i performs the secure Diffie-Hellman two-party key exchange with his/her neighbors U_{i-1} and U_{i+1} and then negotiates the shared keys $k_{U_{i-1}U_i}$ and $k_{U_iU_{i+1}}$ as shown in Figure 1. It should be noted that, $k_{U_nU_1}$ is negotiated by U_n and U_1 . Each user U_i then computes a value $Z_i = k_{U_{i-1}U_i} \oplus k_{U_iU_{i+1}}$ and broadcasts this value to other members. Note that, Z_n is computed as $k_{U_{n-1}U_n} \oplus k_{U_nU_1}$. Upon receiving all Z_j , where $j \neq i$ from other members, each user U_i can compute the other members' shared keys inductively as follows:

$$\begin{aligned} k_{U_{i+1}U_{i+2}} &= Z_{i+1} \oplus k_{U_iU_{i+1}}, \\ k_{U_{i+2}U_{i+3}} &= Z_{i+2} \oplus k_{U_{i+1}U_{i+2}}, \\ &\vdots \\ k_{U_nU_1} &= Z_n \oplus k_{U_{n-1}U_n}, \\ k_{U_1U_2} &= Z_1 \oplus k_{U_nU_1}, \\ &\vdots \\ k_{U_{i-2}U_{i-1}} &= Z_{i-2} \oplus k_{U_{i-3}U_{i-2}}. \end{aligned}$$

Each user U_i can then compute group shared key sk as $sk = H_0(k_{U_1U_2} \parallel k_{U_2U_3} \cdots \parallel k_{U_{n-1}U_n} \parallel k_{U_nU_1})$, where $H_0()$ is a public one-way hash function from $\{1,0\}^*$ to $\{1,0\}^q$, where q is a security parameter.

The above scheme needs only two rounds to achieve the group shared key. However, when a new member joins the group, the scheme experiences a number of issues. In the protocol, when a new member U_{n+1} joins the group, he/she has to perform a two-party key exchange with his neighbors U_n and U_1 to obtain $k_{U_nU_{n+1}}$ and $k_{U_{n+1}U_1}$. Then new Z_n , Z_{n+1} and Z_1 of users U_n , U_{n+1} and U_1 are computed as $Z_n = k_{U_{n-1}U_n} \oplus k_{U_nU_{n+1}}$, $Z_{n+1} = k_{U_nU_{n+1}} \oplus k_{U_{n+1}U_1}$ and $Z_1 = k_{U_{n+1}U_1} \oplus k_{U_1U_2}$, respectively. All users then broadcast their computed Z values. Upon receiving all Z values, each user computes

$k_{U_1U_2}, k_{U_2U_3}, \dots, k_{U_{n-1}U_n}, k_{U_nU_{n+1}}, k_{U_{n+1}U_1}$. Finally each user can compute the new session key as $sk = H_0(k_{U_1U_2} \parallel k_{U_2U_3} \cdots \parallel k_{U_{n-1}U_n} \parallel k_{U_nU_{n+1}} \parallel k_{U_{n+1}U_1})$.

The flaw in this scheme is that a new member can use the calculated $k_{U_1U_2}, k_{U_2U_3}, \dots, k_{U_{n-1}U_n}$ which are the same as in the previous session and the value of the previous Z_n denoted by $(Z_n)_p$ which he/she saw in the previous session to compute $k_{U_nU_1} = (Z_n)_p \oplus k_{U_{n-1}U_n}$ of the previous session. Therefore, the new member can compute the shared key in the previous session as well.

A simple way to remedy the flaw is to make each member of the new group start the scheme from the beginning step of two-party key exchange with his/her neighbors when a new member joins the group. This should be done in the same way as the leave protocol described in Lee et al.'s work [14]. However, this can generate a lot of exchanged and broadcast messages in the network. This problem also arises when several groups want to merge together. To prevent such problems, a scheme which generates fewer messages and lessen users' computation is given in Section 5.

4.2 Dutta and Barua' Scheme

In the join algorithm of this scheme [7], a seed $x = H(sk)$, where sk is the group key of n users in the previous session and $H()$ is a hash function, is used for generating the new group key in the join session. A ring of U_1, U_2, U_n and a new user U_{n+1} is formed. In this ring, U_1 uses x_1 , U_2 uses x , U_n uses x_n and U_{n+1} uses x_{n+1} as their private keys to perform key exchange and compute new group key. This scheme is vulnerable to known session key attack because an adversary who knows the group key in the previous session (in the case that he/she calls Function *reveal()* as described in paper [3]) can compute x and then shared keys between U_2 and his/her neighbors. The adversary can eventually compute the new group key.

In the leave algorithm, the remaining members in the group form a new ring. Only left-right neighbors of the leaving users choose new session private keys, and perform key exchange in order to establish new shared keys. Other members in the ring use their precomputed shared keys obtained in the previous session. These members of the new ring then use their shared keys to compute the new session group key. Since the leaving users also know these precomputed shared keys in the previous session, they can compute the new group key. Thus this scheme cannot preserve forward secrecy.

4.3 Kumar and Tripathi' Scheme

In the join algorithm of this scheme [12], a ring of U_1, U_n and U_{n+1} is formed to compute a shared key K . U_1 then encrypts K by using the previous session group key SK and broadcasts the encrypted message to all other members of the old group. Upon receiving this K value, all members compute the new group key as $SK_{new} = H(SK \parallel K)$. Therefore, this scheme is vulnerable to

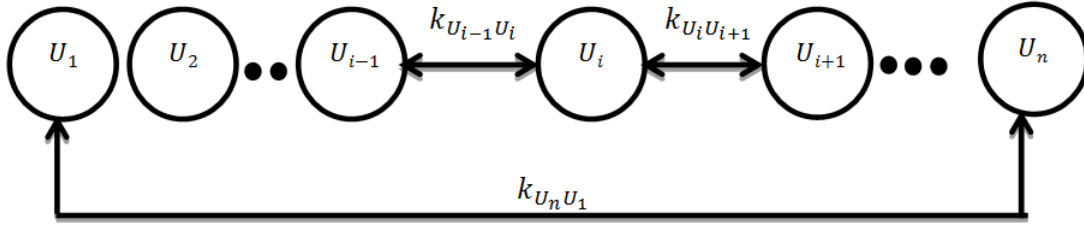


Figure 1: The structure of Lee et al.'s group key agreement

known session key attack because an adversary who knows the group key in the previous session can recover K and then compute the new group key.

Similarly to Dutta and Barua' leave algorithm, Kumar and Tripathi' one also takes advantage of some users' pre-computed shared keys obtained in the previous session to compute the new session group key. Since the leaving users also know these precomputed shared keys in the previous session, they can compute the new group key. Thus this scheme does not preserve forward secrecy.

5 Authenticated Group Key Agreement Based on Braid Groups

In this section, the authenticated key exchange scheme described in Section 3 is extended so that it can be used in an authenticated group key agreement.

Suppose there are n subgroups $B_{l_1}, B_{l_2}, \dots, B_{l_n}$ of l -braid group B_l , where $l = l_1 + l_2 + \dots + l_n$. Let $U_1 \dots U_i \dots U_n$ be n users participating in the group communication protocol. Two complicated braids x and $x_1 \in B_l$ are published as system parameters. A long-term private key of each U_i is $\alpha_{U_i} \in B_{l_i}$ and the computed long-term public key is $P_{U_i} = \alpha_{U_i} x \alpha_{U_i}^{-1}$.

5.1 Group Initialization

Let $U_1 \dots U_i \dots U_m$, where $m \subset n$, be m users wishing to establish a secure group communication. These users are arranged in a predefined order of a ring. Each user U_i performs the secure authenticated two-party key exchange with his/her neighbors U_{i-1} and U_{i+1} . Note that U_m performs key exchange with U_{m-1} and U_1 .

As described in Section 3, U_i and U_{i+1} can compute a shared secret $K_{U_i U_{i+1}} = \alpha_{U_i} \alpha_{U_{i+1}} x \alpha_{U_{i+1}}^{-1} \alpha_{U_i}^{-1}$ by using their long-term private and public keys. The steps of group initialization are as follows.

- 1) U_i chooses $x_{i,i+1} \in B_{l_i} \cup B_{l_{i+1}}$ and session private key $\beta_{U_i} \in B_{l_i}$, and computes a session public key $p_{U_i} = \beta_{U_i} x_{i,i+1} \beta_{U_i}^{-1}$.

- 2) U_i sends $x_{i,i+1}$ and an authenticated public key $K_{U_i U_{i+1}} x_1 (\beta_{U_i} x_{i,i+1} \beta_{U_i}^{-1}) K_{U_i U_{i+1}}^{-1}$ to U_{i+1} . It is noted that x_1 is used for making $K_{U_i U_{i+1}} x_1 (\beta_{U_i} x_{i,i+1} \beta_{U_i}^{-1}) K_{U_i U_{i+1}}^{-1}$ and $x_1 (\beta_{U_i} x_{i,i+1} \beta_{U_i}^{-1})$ at the same length in order to be immune to Length-based attack [10].
- 3) U_{i+1} uses x_1 and the shared secret $K_{U_i U_{i+1}}$ to verify the message, and then obtains U_i 's session public key $\beta_{U_i} x_{i,i+1} \beta_{U_i}^{-1}$.
- 4) U_{i+1} computes the shared key $k_{U_i U_{i+1}} = \beta_{U_{i+1}} \beta_{U_i} x_{i,i+1} \beta_{U_i}^{-1} \beta_{U_{i+1}}^{-1}$ by using his/her session private key $\beta_{U_{i+1}} \in B_{l_{i+1}}$.
- 5) In the same way as described above, U_{i+1} sends an authenticated public key $K_{U_i U_{i+1}} x_1 (\beta_{U_{i+1}} x_{i,i+1} \beta_{U_{i+1}}^{-1}) K_{U_i U_{i+1}}^{-1}$ to U_i . Upon receiving U_{i+1} 's authenticated public key, U_i can compute the shared key $k_{U_i U_{i+1}} = \beta_{U_i} \beta_{U_{i+1}} x_{i,i+1} \beta_{U_{i+1}}^{-1} \beta_{U_i}^{-1}$, since $\beta_{U_{i+1}} \beta_{U_i} = \beta_{U_i} \beta_{U_{i+1}}$.
- 6) In the same way, U_i and U_{i-1} can also compute the shared key $k_{U_{i-1} U_i} = \beta_{U_i} \beta_{U_{i-1}} x_{i-1,i} \beta_{U_{i-1}}^{-1} \beta_{U_i}^{-1}$, where $x_{i-1,i} \in B_{l_{i-1}} \cup B_{l_i}$, and $\beta_{U_{i-1}} \in B_{l_{i-1}}$ is U_{i-1} 's session private key.
- 7) Each user U_i computes a value $Z_{U_i} = (k_{U_{i-1} U_i})^{-1} k_{U_i U_{i+1}}$ and broadcasts the value to other members. Note that $Z_{U_m} = (k_{U_{m-1} U_m})^{-1} k_{U_m U_1}$.
- 8) When each user U_i obtains all Z_{U_j} , where $1 \leq j \leq m$ and $j \neq i$, from other members, he/she checks whether the received Z_{U_j} values come from the existing group members by computing

$$\begin{aligned} Z_0 &= Z_{U_1} Z_{U_2} \dots Z_{U_m} \\ &= (k_{U_m U_1})^{-1} k_{U_1 U_2} (k_{U_1 U_2})^{-1} k_{U_2 U_3} \dots \\ &\quad (k_{U_{m-2} U_{m-1}})^{-1} k_{U_{m-1} U_m} (k_{U_{m-1} U_m})^{-1} k_{U_m U_1}. \end{aligned}$$

If all Z_{U_j} come from the existing group members, then the value Z_0 is equal to the identity braid. When a user finds out that Z_0 is not the identity braid, he/she will broadcast an error message. Upon receiving the error message, each user halts the scheme.

- 9) If Z_0 is the identity braid, each user U_i which has $k_{U_{i-1}U_i}$ and $k_{U_iU_{i+1}}$, begins to compute the shared keys of other members as follows:

$$\begin{aligned} k_{U_{i+1}U_{i+2}} &= k_{U_iU_{i+1}} Z_{U_{i+1}} \\ &= k_{U_iU_{i+1}} (k_{U_iU_{i+1}})^{-1} k_{U_{i+1}U_{i+2}} \\ k_{U_{i+2}U_{i+3}} &= k_{U_{i+1}U_{i+2}} Z_{U_{i+2}} \\ &= k_{U_{i+1}U_{i+2}} (k_{U_{i+1}U_{i+2}})^{-1} k_{U_{i+2}U_{i+3}} \\ &\vdots \\ k_{U_{i-2}U_{i-1}} &= k_{U_{i-3}U_{i-2}} Z_{U_{i-2}} \\ &= k_{U_{i-3}U_{i-2}} (k_{U_{i-3}U_{i-2}})^{-1} k_{U_{i-2}U_{i-1}}. \end{aligned}$$

- 10) After collecting all shared keys, each user computes a seed $sd = k_{U_1U_2} k_{U_2U_3} \cdots k_{U_{m-1}U_m}$ and the group session key $sk_G = (sd)x(sd)^{-1}$. Note that $sd \in B_{l_1} \cup B_{l_2} \cup \cdots \cup B_{l_m}$ and $sk_G \in B_l$.

Complexity: The group initialization needs two rounds. In the first round, $O(m)$ unicast messages are sent for key exchange. Each user computes $O(1)$ braid multiplication. In the second round, $O(m)$ broadcast messages are used for sending shared keys. Each user has to compute $O(m)$ braid multiplication in order to achieve the seed and the common group key.

5.2 Member Join

When a new user U_{m+1} wants to join the group, a user in the existing group can present himself/herself as the group representative U_r and performs key exchange with user U_{m+1} in order to construct a new group key.

Let $\alpha_{U_r} \in B_{l_r}$ and $P_{U_r} = \alpha_{U_r} x \alpha_{U_r}^{-1} \in B_l$ be the long-term private key and public key of U_r . In addition $\alpha_{U_{m+1}} \in B_{l_{m+1}}$ and $P_{U_{m+1}} = \alpha_{U_{m+1}} x \alpha_{U_{m+1}}^{-1}$ be the keys of U_{m+1} . Note that Users U_r and U_{m+1} can establish a shared secret $K_{U_rU_{m+1}} = \alpha_{U_r} \alpha_{U_{m+1}} x \alpha_{U_{m+1}}^{-1} \alpha_{U_r}^{-1}$ with each other. The steps needed to establish a new group key are as follows.

- (a) User U_r chooses a braid $x_{G,m+1} \in B_{l_1} \cup B_{l_2} \cup \cdots \cup B_{l_m} \cup B_{l_{m+1}}$ and sends it together with the authenticated blind seed $K_{U_rU_{m+1}} x_1 (sd) x_{G,m+1} (sd)^{-1} K_{U_rU_{m+1}}^{-1}$ to U_{m+1} . It is noted that sd is the seed obtained in the previous session.
- (b) Upon receiving the authenticated blind seed, U_{m+1} uses $K_{U_rU_{m+1}}$ and x_1 to recover $(sd) x_{G,m+1} (sd)^{-1}$ and computes the seed of the new group as

$$sd_{nG} = \beta_{U_{m+1}} (sd) x_{G,m+1} (sd)^{-1} \beta_{U_{m+1}}^{-1},$$

where $\beta_{U_{m+1}} \in B_{l_{m+1}}$ is user U_{m+1} 's session private key. U_{m+1} then computes the new group key $sk_{nG} = (sd_{nG}) x (sd_{nG})^{-1}$.

- (c) In a similar way, U_r can compute the seed of the new group $sd_{nG} = (sd) \beta_{U_{m+1}} x_{G,m+1} \beta_{U_{m+1}}^{-1} (sd)^{-1}$ by using the value $K_{U_rU_{m+1}} x_1 (\beta_{U_{m+1}} x_{G,m+1} \beta_{U_{m+1}}^{-1}) K_{U_rU_{m+1}}^{-1}$ received from U_{m+1} . Then U_r uses the seed to compute the new group key sk_{nG} .
- (d) U_r broadcasts $(sd) x_1 sd_{nG} x_1^{-1} (sd)^{-1}$ to all members of the previous group.
- (e) Upon receiving the broadcast value, each user of the previous group uses the previous seed sd and x_1 to recover the new seed sd_{nG} and then computes the new group key sk_{nG} .

In the case that many users, e.g. U_{m+1} , U_{m+2} and U_{m+3} want to join the group simultaneously, U_r can use the seed sd of the old group to establish an intermediate group with U_{m+1} , U_{m+2} and U_{m+3} by adopting the group initialization described in Subsection 5.1. After computing the new seed sd_{nG} , U_r can use the scheme described above to send the new seed to other members of the old group.

Complexity: When there are m' users want to join the group, this algorithm needs three rounds. In the first round, $O(m')$ unicast messages are sent for key exchange. Each user computes $O(1)$ braid multiplication. In the second round, $O(m')$ broadcast messages are used for sending users' shared keys. Each of $m+1$ users has to compute $O(m')$ braid multiplication in order to achieve the new seed and group key. In the third round, one broadcast message is sent from the representative to other members in the old group. Each member computes $O(1)$ braid multiplication in order to achieve the new seed.

5.3 Member Leave

When a member leaves a group of m members, each remaining member can choose a new session private key and starts the protocol with his/her neighbors from the step containing the two-party key exchange, to construct a new session key for $m-1$ members in the way described in Subsection 5.1. By performing such scheme, forward secrecy is preserved. However, this scheme generates many messages in the network. A scheme which can reduce communicating messages is described below.

Let us consider a scenario where there are 6 members in the existing group, and user U_4 wants to leave the group. The steps of the leave algorithm are as follows.

- (a) U_3 performs an authenticated two-party key exchange with user U_5 to obtain a shared key $k_{U_3U_5} = \beta_{U_3} \beta_{U_5} x_{3,5} \beta_{U_5}^{-1} \beta_{U_3}^{-1}$, where $x_{3,5} \in B_{l_3} \cup B_{l_5}$, and β_{U_3}, β_{U_5} are U_3 and U_5 session private keys, respectively.
- (b) U_3 and U_5 computes a new seed $sd_{nG} = k_{U_3U_5} sd (k_{U_3U_5})^{-1}$ where sd is the seed of the old group. They then compute the new group key $sk_{nG} = (sd_{nG}) x (sd_{nG})^{-1}$.

- (c) U_3 then uses authenticated messages $(K_{U_3U_i}) (sd) x_1 sd_{nG} x_1^{-1} (sd)^{-1} (K_{U_3U_i})^{-1}$ to send the seed to the remaining members U_i in the group, where $K_{U_3U_i} = \alpha_{U_3} \alpha_{U_i} x \alpha_{U_3}^{-1} \alpha_{U_i}^{-1}$, $i = 1, 2, 6$.
- (d) Upon receiving the authenticated message, U_i uses $K_{U_3U_i}$, sd and x_1 to recover sd_{nG} .
- (d) U_{rG2} sends the new seed to the remaining members of $G2$ by using the method described in Subsection 5.2.
- (e) In a similar way, U_{rG1} computes the new seed and common group key by using the authenticated blind seed received from $G2$ and sends the new seed to the remaining members of $G1$.

In the case that m' users leave the group simultaneously, left-right neighbors of the leaving users form an intermediate group in order to compute a shared secret among them. They then use this secret and the seed obtained in the previous session to compute the new seed, and send the authenticated seed to the remaining members in the group.

Complexity: The leave algorithm needs three rounds in case that there are m' users leave a group of m users. In the first round, $O(m^*)$ unicast messages, where m^* is $\min(m - m', m')$, are sent for establishing key exchange between the left-right neighbors of the leaving users. In the second round, $O(m^*)$ broadcast messages are sent and each participating user computes $O(m^*)$ braid multiplication in order to achieve the new seed and group key. In the third round, $O(m - m')$ unicast messages are used for sending the new seed to the remaining members in the group. Upon receiving the message, each user has to compute $O(1)$ braid multiplication in order to recover the seed and compute the new group key.

5.4 Group Merge

The join protocol described in Subsection 5.2 can be extended for merging two or more groups together. The idea is that the representative of each group uses the existing seed to perform two-party key exchange with each other to establish a new seed and group key. Then the representative of each group sends the new seed to other members of the group. In this subsection, an example of the merging scheme for two groups $G1$ and $G2$ is described.

For simplicity, let $U_1 \dots U_{rG1} \dots U_m$ be members of $G1$ and $U_{m+1} \dots U_{rG2} \dots U_n$ be members of $G2$. U_{rG1} and U_{rG2} are users who claim to be representatives of group $G1$ and $G2$, respectively. Let $sd_{G1} \in B_{l_1} \cup B_{l_2} \cup \dots \cup B_{l_m}$ and $sd_{G2} \in B_{l_{m+1}} \cup B_{l_{m+2}} \cup \dots \cup B_{l_n}$ be the seeds of $G1$ and $G2$, respectively. The steps of the protocol are as follows.

- (a) U_{rG1} and U_{rG2} compute a shared secret $K_{U_{rG1}U_{rG2}} \in B_l$ by using their long-term private and public keys as described in Section 3.
- (b) U_{rG1} chooses a braid $x_{G1,G2} \in B_{l_1} \cup B_{l_2} \cup \dots \cup B_{l_m} \cup B_{l_{m+1}} \cup \dots \cup B_{l_{n-1}} \cup B_{l_n}$ and sends it together with the authenticated blind seed $K_{U_{rG1}U_{rG2}} x_1 (sd_{G1}) x_{G1,G2} (sd_{G1})^{-1} (K_{U_{rG1}U_{rG2}})^{-1}$ to U_{rG2} .
- (c) Upon receiving the authenticated blind seed, U_{rG2} computes the new seed $sd_{nG} = (sd_{G2}) (sd_{G1}) x_{G1,G2} (sd_{G1})^{-1} (sd_{G2})^{-1}$ and the new group key $sk_{nG} = (sd_{nG}) x (sd_{nG})^{-1}$.

Everyone in the merging group can now securely communicate by using the new session group key with backward secrecy.

Complexity: When there are J groups which want to merge together, this algorithm needs three rounds. In the first round, $O(J)$ unicast messages are sent by group representatives for key exchange. Each representative computes $O(1)$ braid multiplication in order to obtain shared keys. In the second round, $O(J)$ broadcast messages are used for sending shared keys. Each group representative has to compute $O(J)$ braid multiplication in order to achieve the new seed and group key. In the third round, one broadcast message is sent from each group representative to the remaining members in the group. The remaining members of each group computes $O(1)$ braid multiplication in order to recover the new seed.

5.5 Group Partition

A group can be partitioned into two or more groups. Group partition scheme can be done by letting all members of each new group work together to establish a new group key, by adopting the group initialization scheme described in Subsection 5.1 and using a new session private key for each user.

In this subsection, the extension of the leave protocol for group partition is described. For simplicity, we consider a scenario in which there are 10 members in the existing group. The group are then partitioned into two groups. The first one has seven users, i.e. $U_1, U_2, U_5, U_6, U_7, U_9$ and U_{10} . Users U_3, U_4 and U_8 are members of the second group. Let us consider the scenario of the first group which U_3, U_4 and U_8 leave the group. The left-right neighbors of the leaving users, i.e. U_2, U_5, U_7 and U_9 then choose new session private keys and work together to establish an intermediate seed sd_{iG} by using the group initialization scheme. Each user of the intermediate group then computes a new seed $sd_{nG} = sd_{iG} sd(sd_{iG})^{-1}$, where sd is the seed obtained in the previous session. U_5 which is the right-handed neighbor of the leaving user U_4 then sends the authenticated seed, as described in 5.3, to U_6 which is the remaining group member on the right-handed side of U_5 . U_9 also sends the authenticated seed to U_{10} and U_1 which are the remaining group members on the right-handed side of U_9 . As the leaving users do not know sd_{iG} , they cannot compute sd_{nG} . Therefore this scheme can preserve forward secrecy. U_3, U_4 and U_8 can also compute the new seed and shared key of their group by using the same approach.

Complexity: Suppose a group of m users is partitioned into J groups, each new group has m_j members, where

$j = 1$ to J . The partition algorithm needs three rounds for each group. In the first round, $O(m_j^*)$ unicast messages, where m_j^* is $\min(m - m_j, m_j)$, are sent for two-party key exchange between participating users in each group. In the second round, $O(m_j^*)$ broadcast messages are sent, and each participating user in each group computes $O(m_j^*)$ braid multiplication in order to achieve the new seed and group key. In the third round, $O(m_j)$ unicast messages are used for sending the new seed to the remaining members in each group. Upon receiving the message, each user has to compute $O(1)$ braid multiplication in order to recover the seed and compute the group key.

6 Authentication Proof of the Group Key Agreement

In this section, an authentication proof of the proposed group-key-agreement protocol is shown using BAN Logic. This proof is different from the authentication proof given in Lee et al's work [14]. The notations used in this work follow those in paper [4]. As described in Subsection 5.1, each user U_i can compute a shared secret (key) with his/her neighbors, i.e. U_i believes $U_i \xrightarrow{k_{U_i U_{i+1}}} U_{i+1}$ and U_i believes $U_i \xrightarrow{k_{U_{i-1} U_i}} U_{i-1}$.

Further, when each user U_i receives all Z values from other members, he/she uses these values to compute $k_{U_1 U_2}$, $k_{U_2 U_3}$, \dots , $k_{U_{m-1} U_m}$ and uses them to compute the session seed and group key.

The aim of this proof is to thus show that U_i can believe $k_{U_1 U_2}$ because it is the shared secret (key) between U_1 and U_2 in the existing group, and U_i can believe $k_{U_2 U_3}$ because it is the shared secret (key) between U_2 and U_3 , and so on. U_i can then use these values to compute the seed and group key. This means that the aim of the proof is to show that the following statement is satisfied under the proposed group-key-agreement protocol:

$$U_i \text{ believes } (U_1 \xrightarrow{k_{U_1 U_2}} U_2, U_2 \xrightarrow{k_{U_2 U_3}} U_3, \dots, U_{i+1} \xrightarrow{k_{U_{i+1} U_{i+2}}} U_{i+2}, \dots, U_{m-1} \xrightarrow{k_{U_{m-1} U_m}} U_m).$$

At the group initialization stage, each user U_i receives the broadcast messages Z from other members of the group. These messages can be transformed into the idealized forms as follows:

$$U_{i+1} \rightarrow U_i : \{N_{i+1}, U_{i+1} \xrightarrow{k_{U_{i+1} U_{i+2}}} U_{i+2}\}_{k_{U_i U_{i+1}}}.$$

$$U_{i+2} \rightarrow U_i : \{N_{i+2}, U_{i+2} \xrightarrow{k_{U_{i+2} U_{i+3}}} U_{i+3}\}_{k_{U_{i+1} U_{i+2}}}.$$

$$U_{i+3} \rightarrow U_i : \{N_{i+3}, U_{i+3} \xrightarrow{k_{U_{i+3} U_{i+4}}} U_{i+4}\}_{k_{U_{i+2} U_{i+3}}}.$$

⋮

$$U_{i-1} \rightarrow U_i : \{N_{i-1}, U_{i-1} \xrightarrow{k_{U_{i-1} U_i}} U_i\}_{k_{U_{i-2} U_{i-1}}}.$$

In this form $N_1, N_2, \dots, N_{i+1}, N_{i+2}, \dots, N_m$ are nonces.

To analyze the protocol, the following assumptions are made.

U_i believes fresh $(N_1, N_2, \dots, N_{i+1}, N_{i+2}, \dots, N_m)$

U_i believes U_{i+1} controls $U_{i+1} \xrightarrow{k_{U_{i+1} U_{i+2}}} U_{i+2}$,

U_i believes U_{i+2} controls $U_{i+2} \xrightarrow{k_{U_{i+2} U_{i+3}}} U_{i+3}$,

⋮

U_i believes U_{i-1} controls $U_{i-1} \xrightarrow{k_{U_{i-1} U_i}} U_i$.

The main steps for the proof are as follows:

- 1) U_i believes $U_i \xrightarrow{k_{U_i U_{i+1}}} U_{i+1}$ and U_i sees $\{N_{i+1}, U_{i+1} \xrightarrow{k_{U_{i+1} U_{i+2}}} U_{i+2}\}_{k_{U_i U_{i+1}}}$, then U_i believes U_{i+1} said $(N_{i+1}, U_{i+1} \xrightarrow{k_{U_{i+1} U_{i+2}}} U_{i+2})$.
- 2) U_i believes fresh (N_{i+1}) and U_i believes U_{i+1} said $(N_{i+1}, U_{i+1} \xrightarrow{k_{U_{i+1} U_{i+2}}} U_{i+2})$, then U_i believes U_{i+1} believes $(N_{i+1}, U_{i+1} \xrightarrow{k_{U_{i+1} U_{i+2}}} U_{i+2})$.

The conjunction can be broken and this yields the result that

$$U_i \text{ believes } U_{i+1} \text{ believes } U_{i+1} \xrightarrow{k_{U_{i+1} U_{i+2}}} U_{i+2}.$$

- 3) U_i believes U_{i+1} controls $U_{i+1} \xrightarrow{k_{U_{i+1} U_{i+2}}} U_{i+2}$ and U_i believes U_{i+1} believes $U_{i+1} \xrightarrow{k_{U_{i+1} U_{i+2}}} U_{i+2}$, then U_i believes $U_{i+1} \xrightarrow{k_{U_{i+1} U_{i+2}}} U_{i+2}$.

The above conclusion means that U_i can believe $k_{U_{i+1} U_{i+2}}$ which may be used by U_{i+2} to send a message. This can be written in the form

$$U_i \text{ believes } U_i \xrightarrow{k_{U_{i+1} U_{i+2}}} U_{i+2}.$$

- 4) U_i believes $U_i \xrightarrow{k_{U_{i+1} U_{i+2}}} U_{i+2}$ and U_i sees $\{N_{i+2}, U_{i+2} \xrightarrow{k_{U_{i+2} U_{i+3}}} U_{i+3}\}_{k_{U_{i+1} U_{i+2}}}$, then U_i believes U_{i+2} said $(N_{i+2}, U_{i+2} \xrightarrow{k_{U_{i+2} U_{i+3}}} U_{i+3})$.

- 5) U_i believes fresh (N_{i+2}) and U_i believes U_{i+2} said $(N_{i+2}, U_{i+2} \xrightarrow{k_{U_{i+2} U_{i+3}}} U_{i+3})$, then U_i believes U_{i+2} believes $(N_{i+2}, U_{i+2} \xrightarrow{k_{U_{i+2} U_{i+3}}} U_{i+3})$.

The conjunction can be broken and this yields the result that U_i believes U_{i+2} believes $U_{i+2} \xrightarrow{k_{U_{i+2} U_{i+3}}} U_{i+3}$.

6) U_i believes U_{i+2} controls $U_{i+2} \xrightarrow{k_{U_{i+2}U_{i+3}}} U_{i+3}$ and U_i believes U_{i+2} believes $U_{i+2} \xrightarrow{k_{U_{i+2}U_{i+3}}} U_{i+3}$, then U_i believes $U_{i+2} \xrightarrow{k_{U_{i+2}U_{i+3}}} U_{i+3}$. The above conclusion means that U_i can believe $k_{U_{i+2}U_{i+3}}$ which may be used by U_{i+3} to send a message. This can be written in the form U_i believes $U_i \xrightarrow{k_{U_{i+2}U_{i+3}}} U_{i+3}$. By repeating the steps above, we obtain the following result. U_i believes ($U_1 \xrightarrow{k_{U_1U_2}} U_2, U_2 \xrightarrow{k_{U_2U_3}} U_3, \dots, U_{i+3} \xrightarrow{k_{U_{i+3}U_{i+4}}} U_{i+4}, \dots, U_{m-1} \xrightarrow{k_{U_{m-1}U_m}} U_m$).

Therefore we have shown that the statement is satisfied under the proposed protocol, and U_i can use these shared keys to compute the session seed and group key.

In the member join protocol described in Subsection 5.2, the new group key is obtained by allowing U_r to perform an authenticated key exchange, using the seed obtained in the previous session, with the new member using his/her private key. U_r then broadcasts the new seed to other members of the former group using the old seed which is known only to members of the group. Therefore, all members of the former group believe received seed and use the seed to compute the new group key. This is similar to the merge protocol.

As for leave protocol, the left-handed neighbor of the leaving member sends the new seed to each member of the new group by authenticating and hiding the new seed in a secret known to only him/herself and each member. Therefore, each member of the new group believes the received seed and uses it to compute the new group key.

7 Security Analysis

In this section, security analysis of the proposed protocol is first discussed. Comparisons among ring-structure based protocols are then illustrated. In papers [7, 12], the proposed group-key-agreement protocols were analyzed by applying the toy game [3]. However, they still suffer some flaws because the communicating messages flowing in each session are not well analyzed. Here, we will emphasize on analyzing the messages exchanged in each session. As group initialization of the ring-structure protocols has been well discussed by Hwang et al. [8] as well as Dutta and Barua [7], security analysis of the algorithm is omitted. Here, we will discuss on join and leave algorithms. Merge and partition algorithms will not be discussed as they have similar features as join and leave algorithms respectively.

7.1 Analysis of Join Algorithm

As for single join, two types of messages are used. The first is exchanged messages between the representative of the existing group and the new user in order to compute the new seed.

These are $K_{U_r, U_{m+1}} x_1 (sd) x_{G, m+1} (sd)^{-1} K_{U_r, U_{m+1}}^{-1}$ and $K_{U_r, U_{m+1}} x_1 (\beta_{U_{m+1}} x_{G, m+1} \beta_{U_{m+1}}^{-1}) K_{U_r, U_{m+1}}^{-1}$. The second is the message $(sd) x_1 sd_{nG} x_1^{-1} (sd)^{-1}$ sent by the representative to the remaining members of the group. The new user can analyze $(sd) x_{G, m+1} (sd)^{-1}$ and $(sd) x_1 sd_{nG} x_1^{-1} (sd)^{-1}$. However, he/she cannot compute sd though he/she knows $x_1, x_{G, m+1}$ and sd_{nG} , because of the hardness of GCSP. Therefore the algorithm does preserve backward secrecy.

If an adversary can know the group key of the previous session, i.e. $(sd) x (sd)^{-1}$, he/she still cannot compute sd because of the hardness of GCSP. Therefore he/she cannot compute the new seed. The algorithm is thus immune to known session key attack.

If an adversary can know the long-term private keys of the representative and/or of the new user, he/she can compute $K_{U_r, U_{m+1}}$ and can see $x_1 (sd) x_{G, m+1} (sd)^{-1}$. However, he/she cannot compute for sd . Therefore the algorithm preserves perfect forward secrecy.

7.2 Analysis of Leave Algorithm

In the single-leave algorithm, authenticated public keys are exchanged between the left neighbor U_{lt} , and the right one U_{rt} of the leaving user in order to compute new shared key $k_{U_{lt}U_{rt}}$ between them. The new seed of the group is computed as $sd_{nG} = k_{U_{lt}U_{rt}} sd (k_{U_{lt}U_{rt}})^{-1}$, where sd is the seed of the old group. U_{lt} then sends the new seed to each remaining member of the group by using the message $(K_{U_{lt}U_i} (sd) x_1 sd_{nG} x_1^{-1} (sd)^{-1} (K_{U_{lt}U_i})^{-1})$, where $K_{U_{lt}U_i} = \alpha_{U_{lt}} \alpha_{U_i} x \alpha_{U_i}^{-1} \alpha_{U_{lt}}^{-1}$.

Each remaining member of the group uses $K_{U_{lt}U_i}$, sd and x_1 to extract the new seed. Although the leaving user knows sd and x_1 , he/she cannot compute sd_{nG} because he/she knows neither $k_{U_{lt}U_{rt}}$ nor $K_{U_{lt}U_i}$. Therefore the algorithm does preserve forward secrecy.

If an adversary can know the group key $(sd) x (sd)^{-1}$ in the previous session, he/she still cannot compute sd because of the hardness of GCSP. Therefore the algorithm is immune to known session key attack.

If an adversary can know the long-term private keys of U_{lt} and/or U_i , he/she can compute $K_{U_{lt}U_i}$, and can see $(sd) x_1 sd_{nG} x_1^{-1} (sd)^{-1}$. However, he/she can compute neither sd nor sd_{nG} . Therefore the algorithm preserves perfect forward secrecy.

7.3 Comparisons among Ring-Structure based Protocols

Table 2 illustrates comparisons of security and complexity among several ring-structure based protocols. According to the comparisons, we can see that the proposed protocol outperforms other protocols.

Table 2: Comparison table

Protocol	Authentication		Group Operation	Comment	NoU	NoB	NoO
	Techniques	NoR					
<i>Hwang et al. [8]</i>	Not mentioned	*	Initialization	Yes	$O(m)$	$O(m)$	$O(m)$
<i>Dutta&Barua [7]</i>	Signatures	1	Initialization	Yes	$O(m)$	$O(m)$	$O(m)$
			Join	C2	*	*	*
			Leave	C4	*	*	*
<i>Lee et al. [14]</i>	Not mentioned	*	Initialization	Yes	$O(m)$	$O(m)$	$O(m)$
			Join	C3	*	*	*
			Leave	Yes	$O(m)$	$O(m)$	$O(m)$
<i>Kumar&Tripathi [12]</i>	Signatures	1	Initialization	Yes	$O(m)$	$O(m)$	$O(m)$
			Join	C2	*	*	*
			Leave	C4	*	*	*
<i>Zhu [21]</i>	Long-term keys &Session keys	4	Initialization	Yes	$O(m)$	$O(m)$	$O(m)$
			Join	Yes	$O(m')$ $m' = 1$	$O(m)$	$O(m)$
			Leave	Yes	$O(m')$ $m' = 1$	$O(m)$	$O(m)$
<i>Proposed Protocol</i>	Long-term keys	1	Initialization	Yes	$O(m)$	$O(m)$	$O(m)$
			Join	Yes	$O(m')$	$O(m')$	$O(m')$
			Leave	Yes	$O(m - m')$	$O(m^*)$	$O(m^*)$
			Merge	Yes	$O(J)$	$O(J)$	$O(J)$
			Partition	Yes	$O(m_j)$	$O(m_j^*)$	$O(m_j^*)$

NoR: number of rounds.

NoU: number of unicast messages.

NoB: number of broadcast messages.

NoO: number of operations.

C2: the protocol is vulnerable to known session key attack.

C3: the protocol does not preserve backward secrecy.

C4: the protocol does not preserve forward secrecy.

***** : it is not discussed because this algorithm has some flaws or it is not mentioned.

Join: a group of m users becomes a group of $m + m'$ users

Leave: m' users leave from a group of m users. $m^* = \min(m', m - m')$

Merge: J groups merge into one group

Partition: one group of m users becomes J groups, each group has m_j users, $m_j^* = \min(m_j, m - m_j)$.

In the protocol, NoU, NoB and NoO are considered for each group

8 Conclusion

In this paper, braid group cryptography which requires only multiplication operations is adopted to establish a session group key. In order to prevent a man-in-the-middle attack, exchanged messages are authenticated using long-term private and public keys of group members. The proposed scheme is a scalable one. It needs only two rounds for initializing a group. In dynamic case, the scheme needs three rounds but with only few users involved. According to the comparisons among ring-structure based protocols, our protocol outperforms several protocols. An authentication proof is also shown in this paper using the well-known BAN logic. Although the proposed protocol is based on braid group cryptography, the framework can be applied to several cryptosystems including Diffie-Hellman, Elliptic Curve and chaotic maps.

References

- [1] T. Aneksrup and P. Hiranvanichakorn, "Efficient group key agreement on tree-based braid groups," *Computer and Information Science*, vol. 4, no. 1, pp. 14–27, 2011.
- [2] E. Artin, "Theory of braids," *Annals of Mathematics*, vol. 48, no. 1, pp. 101–126, 1947.
- [3] E. Bresson, O. Chevassut, and D. Pointcheval, "Provably authenticated group diffie-hellman key exchange - The dynamic case," *Proceedings of Advances on Cryptology (Asiacrypt'01)*, pp. 290–309, 2001.
- [4] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Transactions on Computer Systems*, vol. 8, no. 1, pp. 18–36, 1990.
- [5] K. C. Chan and S. H. Chan, "Key management approaches to offer data confidentiality for secure multicasts," *IEEE Network*, vol. 17, no. 5, pp. 30–39, 2003.
- [6] A. Chaturvedi and S. Lal, "An authenticated key agreement protocol using conjugacy problem in braid groups," *International Journal of Network Security*, vol. 6, no. 2, pp. 181–184, 2008.
- [7] R. Dutta and R. Barua, "Provably secure constant round contributory group key agreement in dynamic setting," *IEEE Transactions on Information Theory*, vol. 54, no. 5, pp. 2007–2025, 2008.
- [8] J. Y. Hwang, S. M. Lee, and D. H. Lee, "Scalable key exchange transformation: from two party to group," *Electronic Letters*, vol. 40, no. 12, pp. 728–729, 2004.
- [9] Y. Kim, A. Perrig, and G. Tsudik, "Tree-based group key agreement," *ACM Transactions on Information and System Security*, vol. 7, no. 1, pp. 60–96, 2004.
- [10] K. H. Ko, J. W. Lee, and T. Thomas, "Towards generating secure keys for braid cryptography," *Designs, Codes and Cryptography*, vol. 45, no. 3, pp. 317–333, 2007.
- [11] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. S. Kang, and C. Park, "New public key cryptosystem using braid groups," *Proceedings of Advances on Cryptography (Crypto'00)*, pp. 166–183, 2000.
- [12] A. Kumar and S. Tripathi, "Anonymous ID-based group key agreement protocol without pairing," *International Journal of Network Security*, vol. 18, no. 2, pp. 263–273, 2016.
- [13] H. K. Lee, H. S. Lee, and Y. R. Lee, "An authenticated group key agreement protocol on braid groups," *IACR Cryptology ePrint Archive*, 18, 2003. (<https://eprint.iacr.org/2003/018.pdf>)
- [14] J. S. Lee, C. C. Chang, and K. J. Wei, "Provably secure conference key distribution mechanism preserving the forward and backward secrecy," *International Journal of Network Security*, vol. 16, no. 2, pp. 405–410, 2013.
- [15] D. Li and S. Sampalli, "Group rekeying scheme for dynamic peer group security in collaborative networks," *International Journal of Network Security*, vol. 18, no. 5, pp. 946–959, 2016.
- [16] V. S. Naresh and N. V. E. S. Murthy, "Elliptic curve based dynamic contributory group key agreement protocol for secure group communication over ad-hoc networks," *International Journal of Network Security*, vol. 17, no. 5, pp. 588–596, 2015.
- [17] Q. Qian, Y. L. Jia, and R. Zhang, "A lightweight RFID security protocol based on elliptic curve cryptography," *International Journal of Network Security*, vol. 18, no. 2, pp. 354–361, 2016.
- [18] R. S. Ranjani, D. L. Bhaskari, and P. S. Avadhani, "An extended identity based authenticated asymmetric group key agreement protocol," *International Journal of Network Security*, vol. 17, no. 5, pp. 510–516, 2015.
- [19] G. K. Verma, "A proxy blind signature scheme over braid groups," *International Journal of Network Security*, vol. 9, no. 3, pp. 214–217, 2009.
- [20] G. K. Verma, "Probable security proof of a blind signature scheme over braid groups," *International Journal of Network Security*, vol. 12, no. 2, pp. 118–120, 2011.
- [21] H. F. Zhu, "Secure chaotic maps-based group key agreement scheme with privacy preserving," *International Journal of Network Security*, vol. 18, no. 6, pp. 1001–1009, 2016.

Biography

Pipat Hiranvanichakorn received the B.E. degree in Electrical Engineering from Chulalongkorn University, Thailand, in 1977 and the M.E. and D.E. degrees in Information Processing from Tokyo Institute of Technology, Japan, in 1982 and 1985. He is currently an associate professor of Computer Science at School of Applied Statistics, National Institute of Development Administration, Thailand. His current research interests include natural language processing, computer networks, cryptography and information security.

An Evolutionary Multi-objective Approach for Modelling Network Security

Seyed Mahmood Hashemi, Jingsha He

(Corresponding author: Seyed Mahmood Hashemi)

School of Software Engineering, Beijing University of Technology, Chain

Beijing Engineering Research Center for IoT Software and Systems

(Email: Hashemi2138@yahoo.com)

(Received Feb. 20, 2016; revised and accepted July 19 & July 31, 2016)

Abstract

Security is the most important issue in a network system. Administrators can more easily understand threats to the network by using a model. In this paper, we present an approach for modelling a network that considers the benefits of the network as well as its limitations. In our approach, we model the system as an optimization problem, which is solved using three algorithms. As the proposed approach is stochastic, it works very efficiently in a network environment. This paper, presents a mathematical model of the system. Model provides easy comprehend of system. Presented model is based on multi-objective optimization problem. One parameter in the presented model is security and another parameter is user productivity. Security is the most important issue in a network system. Administrators can more easily understand threats to the network by using a model. In this paper, we present an approach for modelling a network that considers the benefits of the network as well as its limitations.

Keywords: Modelling network security, multi-objective approach, network system, optimization

1 Introduction

A model is a tool that facilitates creating a representation of the target object, thereby helping the users to understand that object. A model is necessary for understanding network systems, because these systems typically comprise many sub-systems and having knowledge about all sub-systems is practically impossible. The importance of a model of a network system increases when considering security. Security is the most important issue in a network system and a higher degree of security is constantly being sought. Focusing on security, we can divide network systems into two main groups: open and closed systems. In the first group, network systems are free to join the network. In other words, all machines in the network can access their assets. Despite the open system, no machine

in the network can access the assets of a closed system. In practice, because this division is absolute, many network systems fall between open and closed systems in the real world. The main goal of a security model is to represent the security level of a network system.

Security is the generic term for a collection of techniques and tools designed to protect data and prevent counter attacks [7]. Security involves three aspects: confidentiality means hiding the contents of a file, integrity means detecting tampering, and availability means ensuring access to assets. All three security aspects can be applied using an authorization system. In this context, confidentiality means unauthorized disclosure of information, integrity means unauthorized modification, and availability means denial of unauthorized access to information. A security model clearly depicts the level of authorization for each sub-system.

The major benefit of a network is user productivity. In other words, a network is created to facilitate access to users favorite data resources. Therefore, application of security should not be limited to users access to assets.

Contrarily, certain constraints are applicable to an authorization system. The main constraint is an economic one. Given that the financial resources of an organization are normally limited, costs must be constrained. As such, there are two conflicting goals for security (increasing authority as well as user productivity) and one constraint (the economic issue). Any network security model must consider the goals and the constraint. In this paper, we present a model based on evolutionary multi-objective optimization (EMO). We use an evolutionary algorithm because it can adapt to the dynamic nature of a network, and multi-objective optimization because it allows us to optimize a number of conflicting objectives. EMO allows us to optimize Confidentiality, Integrity, Availability and User Productivity simultaneously.

The rest of this paper is organized as follows: In Section 2, we define a number of preliminaries that are needed for our proposed algorithm. We also present an overview of related research. In Section 3, we introduce our pro-

posed algorithm together with our experimental results. Finally, our conclusions are presented in Section 4.

2 Related Works

The evolution of the current industrial context and the increase of competition pressure, has led companies to adopt new concepts of management [4]. The implementation of the most important part of the plan phase, consisting of the definition of an appropriate global management plan QSE (Quality, Security and Environment) has been proposed [3]. This implementation is based on the multi-objective influence diagrams (MIDs) [21]. The proposed approach has three phases: Plan phase, Do phase and Check & Art phase. The first phase gathers all quality, security and environmental objectives issued from the requirements, and then analyzes them. In this phase we can define a global management QSE plan. The second phase has the input of the global management plan QSE and the corresponding global monitoring plan generated from the plan phase and will also implement the selected treatments. In the third phase, finalization of the process of integration occurs through measuring the effectiveness of different decisions. Neubauer et al. provide a structured and repeatable process that includes: defining evaluation criteria according to corporate requirements, strategy, assessing and/or refining the existing IT security infrastructure, identifying stakeholder preferences (risks, boundaries), determining the solution space of all efficient (Pareto optimal) safeguard portfolios, and interactively selecting the individually best safeguard portfolio [23]. This paper tries to combine different benefits and costs into one formula. This presents a problem because the authors do not present a multi-objective optimization problem. Kumar et al. focus on PGP (pretty good privacy) [19], which was shown by Zimmerman in 1991 to provide security with available cryptographic algorithms [27]. Algorithms are chosen according to the user requirements of time, cost and required security level. Kumar et al. answer the question: How do you choose appropriate algorithms, from the available pool, to suit the user requirements of time, cost and security? They assign a security level to an algorithm according to its performance P. Authors of [29] investigate security models, which consider risk assessment approaches to be applied for threat modelling, network hardening and risk analysis. Overall, security models can be classified based on the methodologies used to optimally invest into computer security. We have specified the following:

- Risk assessment models;
- Cost-benefit models;
- Game models;
- Multi-objective decision support models.

Cost-benefit analysis looks into intangible costs/returns and addresses the perspective of time. The simplicity

of the frameworks can give suitable investment solutions for low risk investments. However, these methods do not consider uncertainty and give misleading indications for long-term investments. In [30], the risk assessment involves a calculation of risk in relation to financial returns, rather than the defined risk of possible losses related to degradation of information security. They demonstrate a novel approach of selecting security countermeasures with respect to both investment cost and the risk of possible degradation of CIA. Their security countermeasure is represented as a binary value. Also, they thought security solutions can be classified based on the function they provide. The main challenge Information System (IS) managers face is to strike an appropriate balance between risk exposure and the opportunity to mitigate risk through investments in security. Thus, the authors of [17] propose a decision analytical approach, but the paper does not present a formula for multi-objective optimization. Service provisioning (SP) is defined as the set of interrelated decisions in order to select a service (by a server) to attend to a request (by a client). In [25], the results of the author case study provides evidence in support of the notion that the use of imitation (recall) in DPSP (dynamic provider of service provision) cipher selection process reduces its overheads dramatically. In paper [24], the authors introduce a novel presentation for cyber security problems using the formalization of a Multi-Objective Distributed Constraint Optimization Problem (MO-DCOP). An MO-DCOP is the extension of a mono-objective Distributed Constraint Optimization Problem (DCOP) which is a fundamental problem that can formalize various applications related to multi-agent cooperation. They develop a novel algorithm called Branch and Bound search algorithm (BnB) for solving a cyber security problem. This algorithm utilizes the well-known and widely used branch and bound technique and depth-first search strategy and finds all trade-off solutions. The purpose of any risk analysis is providing decision makers with the best possible information about the probability of loss [6]. Behnia et al. compare several different approaches for risk analysis and declare the weakness and strength for each of them.

3 Preliminaries

In this section, we discuss other approaches for modelling network systems, which can be divided into two groups: attack trees and stochastic models.

3.1 Attack Tree

An attack tree is one of the main methods for system modelling. In this approach, assets and their related threats are specified simply. Figure 1 shows an example of an attack tree [31], in which nodes depict the desired actions and edges show the required processes. Depending on the type of tree and the type of protection system, nodes and edges may have different values.

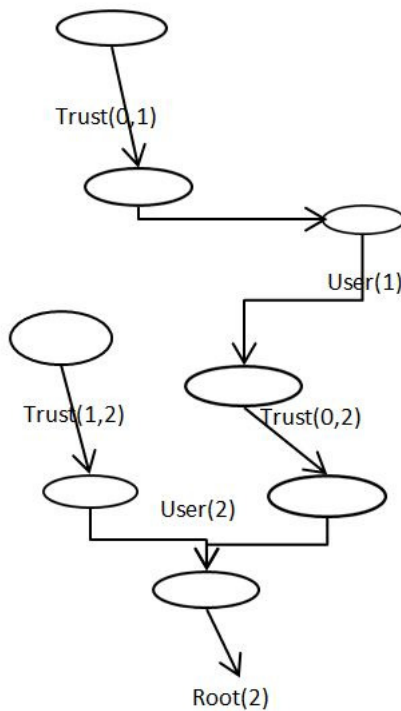


Figure 1: Attack tree

The attack tree models attacking behavior by enumerating all attack scenarios aimed at compromising the root goal. The attack tree model has three components: the root, branches, and leaves. Challenges between security policies and threats are represented by leaves. Branches, which are classified as AND/OR types, move the result from a sub-tree to its ancestor. This process continues until the value reaches the root, at which stage the administrator can make a decision based on the value in the root. Despite the varied use of attack trees, they do suffer from certain problems. Not all useful information about vulnerable systems can be translated into an attack tree. This is a very serious problem because subsequent analysis is sensitive to correct values in the leaves. Because security is a trade-off between user productivity and enhanced security levels, each partner of the system endpoints could have different requirements. Moreover, because an attack tree is static, it is valid for only a limited time.

Many researchers have endeavored to extend the attack tree to suit their target application.

- Dugan et al. presented fault trees [11], which use additional elements such as dependency gates. Fault trees model events according to their exponential distribution. However, there is no evidence that the probability of attack success follows an exponential distribution.
- Fung et al. proposed a MANET network [13]. Their study incorporated the notion of survivability into attack trees. Survivability analysis finds those sys-

tem components susceptible to attacks and analyzes their ability to survive such attacks.

- Bistarelli et al. proposed the defense tree [8]. Their study, which included quantitative metrics such as return on investment and return on attack, extended the attack tree by using countermeasures to address intrusion attempts at the leaves of the trees.
- Dalton et al. proposed a conversion tree [10]. In this work, steady-state analysis of the resulting generalized stochastic Petri net was performed. Details of attack scenarios can be found in [16].

3.2 Stochastic Model

Stochastic models convert the state of the system to a Markov chain, and then analyze it using a steady-state transition matrix. The term stochastic means predicting a set of possible outcomes by their probabilities.

The main property of a Markov chain is that no state can influence the next state. In other words, the probability of any particular future behavior of the process is not altered by additional knowledge about its past behavior. A Markov process is completely defined once its transition probability matrix and initial state have been defined.

Stochastic models have been used extensively in research studies:

- Mandan et al. proposed a model of the behavior of an intrusion tolerant system [20]. This work uses a generic state diagram as a semi-Markov process model that is later solved using an embedded discrete time Markov chain. Quantitative analysis of the model produces two useful metrics: steady-state availability and mean time to security failure.
- Sallhammer et al. used a stochastic model for security and dependability evaluation [26]. This work used game theory to model attack behavior.

3.2.1 Multi-objective Optimization

Optimization is a common topic in many scientific fields. When the target of an optimization problem is a single object, we can model the problem as a single-objective optimization problem. Conversely, if the problem has multiple objectives, we model the problem as a multi-objective optimization problem. However, in many problems, objectives conflict with each other. A multi-objective optimization problem is defined as follows [2].

“A vector of decision variables which satisfies constraints and optimizes a vector function whose elements represent the objective functions. These functions form a mathematical description of performance criteria which are usually in conflict with each other. Hence, the term ‘optimize’ means finding such a solution which would give the values of all the objective functions acceptable to the decision maker”.

Real world applications frequently have several conflicting objectives. Recently, there has been increased research focus on EMO algorithms. Multi-objective optimization problems (MOPs) are defined as follows [9]:

$$\begin{aligned} &\text{Optimize} \quad [f_1(X), f_2(X), \dots, f_k(X)] \\ &\text{Subject to:} \quad g_i(X) \leq 0; i = 1, 2, \dots, m \\ &\quad \quad \quad h_j(X) = 0; j = 1, 2, \dots, p \end{aligned} \quad (1)$$

where k is the number of objectives, X is a vector of decision variables, m is the number of inequality constraints, and p is the number of equality constraints. The notion of “optimize” in Equation (1) implies setting the decision variables in such a way as to achieve Pareto optimality. We say that a vector of decision variables $X^* \in \mathcal{F}$ is *Pareto optimal* if there does not exist another $X \in \mathcal{F}$ such that $f_i(X) \leq f_i(X^*)$ for all $i = 1, \dots, k$ and $f_j(X) < f_j(X^*)$ for at least one j . If vector X^* is included in the *Pareto-optimal* set, it is called a non-dominated solution. A vector $\vec{u} = (u_1, u_2, \dots, u_k)$ is said to *dominate* vector $\vec{v} = (v_1, v_2, \dots, v_k)$ (denoted by $\vec{u} \preceq \vec{v}$) if and only if \vec{u} is partially more optimum than \vec{v} , i.e., $\forall i \in \{1, \dots, k\} \Rightarrow u_i \leq v_i, \exists j \in \{1, \dots, k\} \Rightarrow u_j < v_j$.

Many algorithms have been developed to solve MOPs. In this paper, we use three of these: multi-objective simulated annealing (AMOSA), multi-objective genetic algorithm (MOGA), and multi-objective bee colony (MOBC).

A. Multi-objective Simulated Annealing (AMOSA)

The basic concept in simulated annealing is the evolution of the solution by simulating decreasing temperature (tmp) in the material, where a higher temperature denotes greater modification of the solution in a generation. If the temperature of a hot material decreases very quickly, its internal structure may change and the material could become hard and brittle. Decreasing the temperature slowly yields higher homogeneity and less brittle material. Evolution of the solution occurs at specific temperature profiles. In the first few iterations, a diverse set of initial solutions for the problem are produced at a higher temperature. These solutions are then evolved while the temperature decreases to obtain their local optima. In a multi-objective situation, there are non-dominated solutions that must be kept in the archive as candidates for the optimal solution.

AMOSA was proposed in [5]. During the execution of the AMOSA algorithm, two solutions exist: the current-so and new-so. Comparison of the two solutions yields one of three states: (i) current-so dominates new-so, (ii) current-so and new-so are non-dominated with respect to each other, and (iii) new-so dominates current-so.

If new-so is dominated by current-so, there may be solutions in the archive that dominate new-so. New-so is

accepted into the archive based on the probability:

$$p = \frac{1}{1 + \exp(\Delta * \text{tmp})'} \quad (2)$$

where Δ is the difference between new-so and the other solutions that dominate new-so. If there are A solutions in the archive,

$$\Delta = (\sum_{i=1}^A \Delta_i + \Delta) / (A + 1) \quad (3)$$

Solutions can escape from local optima and reach the neighborhood of the global optima by this probable acceptance.

If new-so is dominated by some solutions in the archive, Equation (3) is modified to:

$$\Delta = (\sum_{i=1}^A \Delta_i) / A. \quad (4)$$

If new-so is not dominated by any of the members in the archive, new-so is set to current-so and is added to the archive.

If new-so dominates some solutions in the archive, new-so is set to current-so and is added to the archive. In addition, any solutions in the archive that are dominated by new-so, are removed.

If new-so is dominated by some solutions in the archive, Equation (2) is changed to:

$$p = \frac{1}{1 + \exp(-\Delta)'} \quad (5)$$

where Δ is the minimum difference between new-so and the dominating solutions in the archive. New-so is set to current-so with probability Equation (5). If new-so is not dominated by any of the solutions in the archive, it is set to current-so and added to the archive. If new-so dominates some solutions in the archive, it is set to current-so and added to the archive, while all dominated solutions are removed from the archive.

B. Multi-objective Genetic Algorithm (MOGA)

MOGA, which is based on a single-objective genetic algorithm [12], [15] and [18], comprises various stages. In the first stage, a population of individuals (chromosomes) is created. The number of individuals in the population (pop-size) is determined by the programmer. Each individual contains certain fields, where the number of fields in an individual is equal to the number of variables in the problem, which must be optimum. Each individual has the potential to reach the optimum point, at which optimal values are set in the corresponding fields in the individual. In the first stage of MOGA, all individuals in the population are initialized with random values. The algorithm runs until the stopping conditions are met. There are three types of stopping conditions. The first of these is special values; when the values of individuals are equal

to the default values, the algorithm terminates. The second type of stopping condition occurs when the values of individuals no longer change. The last type of stopping condition is the number of iterations. When the number of iterations of the algorithm reaches the given threshold value (max-generation), the algorithm terminates.

Given that MOGA is an evolutionary algorithm, it is executed for a number of iterations, where each iteration of MOGA is called a generation, inspired by Darwinian evolutionary theory. The programmer can control the evolutionary nature of MOGA using the number of generations. This means that despite the deterministic optimization method, which is controlled by the number of inputs, the programmer can vary the number of generations. In the first generation, individuals are initialized with random values. The values of individuals are changed in each generation using two operators: mutation and cross-over. In mutation, one field of an individual is changed to a different value. There are a number of different methods for mutation, which describe the quality of the altered values. In cross-over, two individuals are combined to produce a new individual. After the genetic algorithm operators (mutation and cross-over) have been applied, several individuals are selected for the next generation. Selection is done stochastically according to the fitness of the individual.

The goal of the optimization algorithm is to find the optimal point. Optimal points can be divided into two categories: local optima and global optima. A local optimum can be any point that is the optimum of all points within a limited range, while a global optimum is a point that is the optimum of all points in an unlimited range. Because deterministic optimization methods compare the current point with points in a limited range, they may be trapped in a local optimum. The stochastic feature of MOGA allows the algorithm to escape from local optima and achieve the global optimum.

Based on the discussion above, MOGA has two advantages: the programmer can control the execution time and the algorithm has the potential to achieve a global optimum point.

MOGA finds an optimum point according to the Pareto set; in other words, a point is optimum if it is not dominated by other points. Indeed, the Pareto principle allows a number of objectives to become optimum simultaneously. Each individual is checked for its domination in the population. Individual i is allocated a rank equal to one plus the number of individuals, n_i , dominating individual i . Once ranking has been completed, a raw fitness is assigned to each individual based on its rank using a linear mapping function.

$$F_i = N - \sum_{k=1}^{r_i-1} \mu(k) - 0.5(\mu(r_i) - 1) \quad (6)$$

where μ denotes the numbers of individuals in the rank. MOGA incorporates niching among individuals in each rank. The niche count with σ_share is found first. The distance metric is computed with the objective function values. Thus, the normalized distance between any two

individuals i and j in a particular rank is calculated as:

$$d_{ij} = \sqrt{\sum_{k=1}^M \left(\frac{f_k^{(i)} - f_k^{(j)}}{f_k^{\max} - f_k^{\min}} \right)^2} \quad (7)$$

The distance is computed for each pair of individuals. Therefore, the niche count is calculated by summing the shared function values:

$$SH(d_{ij}) = \begin{cases} 1 - \frac{d_{ij}}{\sigma_share}, & \text{if } d_{ij} < \sigma_share \\ 0, & \text{otherwise} \end{cases} \quad nc_i = \sum d_{ij}. \quad (8)$$

The shared fitness is calculated as $F'_i = F_i / nc_i$. Shared fitness is used as a basis for stochastically selecting individuals for the next generation.

The above process continues until the stopping condition is satisfied. When the algorithm terminates, the remaining individuals represent the optimum.

C. Multi-objective Bee Colony (MOBC)

The foraging behavior of bees is characterized by various steps that are used in optimization. The first step is called the Waggle Dance, which is used by bees to convey information to other bees about the direction, distance, and quality of a food source. Upon finding a food source, a bee begins to dance in a figure of eight pattern. The second step in the foraging behavior is following. In this step, follower bees that were waiting inside the hive, follow the dancer bee. The number of follower bees assigned to a path is directly proportional to the quality of the path. In the third step these bees return to the hive. More bees are recruited to the source of the food if the path is still good enough. Bees stop collecting poor-quality food and adjust their strategy for finding food based on information about the location of good-quality food.

Foraging behavior can be used for optimization when it is divided into two phases. The first phase consists of path construction. In this phase, a bee explores the entire food source, but with the exploration limited by constraints. When a bee does a tour (which includes all possible variables), it performs the Waggle Dance. Other bees use this information, expressed as:

$$Pf_i = \frac{1}{L_i} \quad (9)$$

where Pf_i is the profitability of a bee i and L_i is its tour. If a colony has n bees, the bee colony average profitability is given by:

$$Pf_{\text{colony}} = \frac{1}{n} \sum_{i=1}^n Pf_i = \frac{1}{n} \sum_{i=1}^n \frac{1}{L_i} \quad (10)$$

The dance duration of any bee is given by:

$$D_i = K * \frac{Pf_i}{Pf_{\text{colony}}}, \quad (11)$$

where K is the profitability rating and is adjusted according to the lookup table given in Table 1.

Table 1: Lookup table for adjusting profitability

Profitability Rating	K_i
$Pf_i < 0.9Pf_{\text{colony}}$	0.60
$0.9Pf_{\text{colony}} < Pf_i < 0.95Pf_{\text{colony}}$	0.20
$0.95Pf_{\text{colony}} < Pf_i < 1.15Pf_{\text{colony}}$	0.02
$1.15Pf_{\text{colony}} < Pf_i$	0.00

The second phase of the bee algorithm consists of path reconstruction. In this phase, bees in the hive, having received information from the explorer bee, utilize the path. Bees use a transition rule for choosing the appropriate path with the probability denoted by $P_{ij}(t)$, which measures the possibility of moving from step _{i} to step _{j} at time t . In a multi-objective sense, the discussed path must be examined for dominance over other paths. Formula (12) takes into consideration the fitness of all paths:

$$\rho_{ij}(t) = \begin{cases} \lambda & j \in F_i(t) \\ \frac{1 - \lambda |F_i(t) \cap A_i(t)|}{|A_i(t)| - |F_i(t) \cap A_i(t)|} & j \notin F_i(t) \end{cases} \quad (12)$$

where λ is the value (less than one) assigned to the preferred path, $|A_i(t)|$ is the number of allowed next steps, and $|F_i(t) \cap A_i(t)|$ is the number of preferred next steps [1, 14, 22, 28].

Now, we can examine the dominance of all paths according to Section 3.2.1, after which each path is classified as conforming to one of three situations:

- 1) Dominates another path(s),
- 2) is dominated by another path, and
- 3) is not dominated by any other path.

In the first situation, the path is stored in the archive. In the second situation, the path is destroyed, and in the third situation, the path is stored in the archive with the following probability:

$$P_{ij}(t) = \frac{[\rho_{ij}(t)]^\alpha * [\frac{1}{d_{ij}}]^\beta}{\sum_{j \in A_i(t)} [\rho_{ij}(t)]^\alpha * [\frac{1}{d_{ij}}]^\beta} \quad (13)$$

where d_{ij} is the distance between step _{i} and step _{j} , α is a variable that influences the fitness, and β is a variable that influences the distance. A is a collection of all steps that can be reached from the previous step.

4 Proposed Algorithm

First, we give an overview of the system. We set up a system with three assets in the network environment. Here, security implies creating confidentiality, integrity, and availability of these assets.

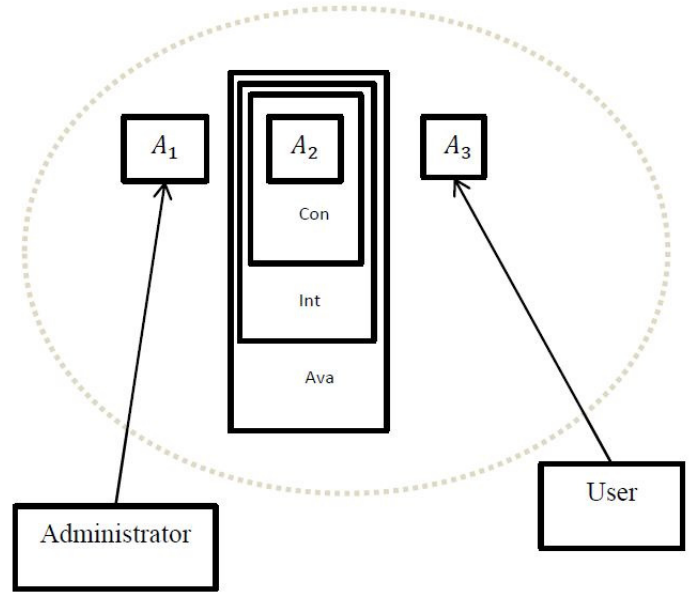


Figure 2: Overview of proposed algorithm

In Figure 2, A represents the assets and *Con*, *Int* and *Ava* denote confidentiality, integrity, and availability. Second, there is a need to create a model of the system. According to the above hits, we use the following optimization model to represent the security of the network model:

Optimize

Security (A_1, A_2, \dots, A_n), User Productivity (A_1, A_2, \dots, A_n)

Subject to: $\text{Con}(A_1) \leq M_1, \text{Con}(A_2) \leq M_2, \text{Con}(A_3) \leq M_3$

$\text{Int}(A_1) \leq N_1, \text{Int}(A_2) \leq N_2, \text{Int}(A_3) \leq N_3$

$\text{Ava}(A_1) \leq K_1, \text{Ava}(A_2) \leq K_2, \text{Ava}(A_3) \leq K_3$ (14)

where A_1, A_2, A_3 are assets in the system, *Int*, *Ava* and *Con* denote the integrity, availability, and confidentiality of the assets, and M, N, K are economic issues applied to each security concept. Security is denoted by the cost function and Optimize means simultaneously maximizing the confidentiality, integrity, and availability of the assets as well as user productivity. Let $M_1 = 5, M_2 = 6, M_3 = 4, N_1 = 4, N_2 = 5, N_3 = 7, K_1 = 5, K_2 = 4, K_3 = 5$ in the range $\{0, 5\}$. These assumptions do not limit the generalization of our modelling. We solve Equation (14) using the three algorithms described in Section 2.2.1, namely, AMOSA, MOGA, and MOBC. The desired levels for confidentiality, integrity, and availability of the assets and user productivity ('user productivity' is defined in Section 1) are in the range $\{0, 5\}$. The final results are listed in Table 2.

Table 2: Final results

	<i>Confidentiality(A₁)</i>	<i>Confidentiality(A₂)</i>	<i>Confidentiality(A₃)</i>
AMOSA	5	6	4
MOGA	5	5	4
MOBC	4	5	3
	<i>Integrity(A₁)</i>	<i>Integrity(A₂)</i>	<i>Integrity(A₃)</i>
AMOSA	4	5	7
MOGA	4	4	7
MOBC	4	4	6
	<i>Availability(A₁)</i>	<i>Availability(A₂)</i>	<i>Availability(A₃)</i>
AMOSA	5	4	5
MOGA	4	4	4
MOBC	4	4	5
	<i>user Productivity(A₁)</i>	<i>user Productivity(A₂)</i>	<i>user Productivity(A₃)</i>
AMOSA	9	8	7
MOGA	8	6	7
MOBC	6	7	6

5 Conclusion

In this paper, we presented an approach for modelling network security. The proposed approach is based on EMO. The application of security has two goals (security aspects and user productivity); therefore, we use a multi-objective optimization. In the model, we consider economic limitations applied to the various security aspects. We use an evolutionary method in the proposed approach, because the nature of networks is dynamic.

The model uses three EMO algorithms, all of which are stochastic. This means that different runs may produce different results, but some results are worth highlighting. AMOSA produces the best result, where best means greater maximization of all goals. In future works, we intend to consider a proper unifier for each goal (for example, a fuzzy set).

Acknowledgments

The work in this paper has been supported by National Natural Science Foundation of China (61272500), National High-tech R&D Program (863 Program) (2015AA017204) and Beijing Natural Science Foundation (4142008).

References

- [1] P. Agrawal, H. Kaur, and D. Bhardwaj, "Analysis and synthesis of enhanced bee colony optimization with the traditional bee colony optimization to solve traveling sales person problem," *International Journal of Computer & Technology*, vol. 2, no. 2, pp. 93–97, 2012.
- [2] A. Ameljaricz, "Multicriteria optimization in engineering design," in *Computing in Civil Engineering*, pp. 318–325, 1994.
- [3] A. Badreddine, T. B. Romdhane, and N. B. Amor, "A multi-objective risk management approach to implement an integrated management system: Quality, security, environment," in *Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics*, pp. 4728–4733, 2009.
- [4] A. Badreddine, T. B. Romdhane, and N. B. Amor, "A new process-based approach for implementing an integrated management system: Quality, security, environment," in *Proceedings of the 2009 International Conference on Industrial Engineering*, vol. 2, pp. 18–20, 2009.
- [5] S. Bandyopadhyay, S. Saha, U. Maulik, and K. Deb, "A simulated annealing-based multi-objective optimization algorithm: AMOSA," *IEEE Transactions on Evolutionary Computation*, vol. 12, no. 3, pp. 269–283, 2008.
- [6] A. Behnia, R. A. Rashid, and J. A. Chaudhry, "A survey of information security risk analysis methods," *Smart Computing Review*, vol. 2, no. 1, pp. 79–94, Feb. 2012.
- [7] M. Bishop, *Computer Security: Art and Science*, Tsinghua Press, pp. 3–10, 2004.
- [8] S. Bistarelli, F. Fioravanti, and P. Peretti, "Defense trees for economic evaluation of security investments," in *The First International Conference on Availability, Reliability and Security*, pp. 8, 2006.
- [9] C. A. Coello, D. A. Van Veldhuizen, and G. B. Lamont, *Evolutionary Algorithms for Solving Multi-objective Problems*, vol. 242, New York: Kluwer Academic, 2002.
- [10] G. C. Dalton, R. F. Mills, J. M. Colombi, and R. A. Raines, "Analyzing attack trees using generalized

- stochastic petri nets,” in *IEEE Information Assurance Workshop*, pp. 116–123, 2006.
- [11] J. B. Dugan, S. J. Bavuso, and M. A. Boyd, “Dynamic fault-tree models for fault-tolerant computer systems,” *IEEE Transactions on Reliability*, vol. 41, no. 3, pp. 363–377, 1992.
- [12] C. M. Fonseca and P. J. Fleming, “Genetic algorithm for multiobjective optimization: Formulation, discussion and generalization,” in *Proceeding of 5th International Conference on Genetic Algorithms*, pp. 416–423, 1993.
- [13] C. Fung, Y. L. Chen, X. Wang, J. Lee, R. Tarquini, and M. Anderson, “Survivability analysis of distributed systems using attack tree methodology,” in *IEEE Military Communications Conference (MILCOM’05)*, pp. 583–589, 2005.
- [14] M. Gupta and G. Sharma, “An efficient modified artificial bee colony algorithm for job scheduling problem,” *International Journal of Soft Computing and Engineering*, vol. 1, no. 6, pp. 291–296, 2012.
- [15] A. Haidine and R. Lehnert, “Multi-case multi-objective simulated annealing (mc-mosa): New approach to adopt simulated annealing to multi-objective optimization,” *World Academy of Science*, vol. 4, no. 3, pp. 9, 2008.
- [16] M. V. Higuero, J. J. Unzilla, E. Jacob, P. Saiz, M. Aguado, and D. Luengo, “Application of attack trees in security analysis of digital contents e-commerce protocols with copyright protection,” in *39th Annual 2005 International Carnahan Conference on Security Technology*, pp. 57–60, 2005.
- [17] E. Kiesling, C. Strau, and C. Stummer, “A multi-objective decision support framework for simulation-based security control selection,” in *IEEE Seventh International Conference on Availability, Reliability and Security*, pp.454–462, 2012.
- [18] A. Konak and A. E. Smith, “Multi-objective optimization using genetic algorithms: A tutorial,” *Reliability Engineering & System Safety*, vol. 91, no. 9, pp. 992–1007, 2006.
- [19] D. Kumar, D. Kashyap, K. K. Mishra, and A. K. Misra, “Security vs cost: An issue of multi-objective optimization for choosing PGP algorithms,” in *IEEE International Conference on Computer and Communication Technology*, pp. 532–535, 2010.
- [20] B. B. Madan, K. Gogeva-Popstojanova, K. Vaidyanathan, and K. S. Trivedi, “Modeling and quantification of security attributes of software systems,” in *International Conference on Dependable Systems and Networks*, pp. 505–514, 2002.
- [21] D. Micheal and Y. H. Yacov, “Influence diagrams with multiple objectives and tradeoff analysis,” *IEEE Transactions on Systems, Man and Cybernetics - Part A: Systems and Humans*, vol. 34, no. 3, pp. 293–304, 2004.
- [22] R. Murugan and M. R. Mohan, “Artificial bee colony optimization for the combined heat and power economic dispatch problem,” *ARPJN Journal of Engineering and Applied Sciences*, vol. 5, no. 7, 2012.
- [23] T. Neubauer, C. Stummer, and E. Weippl, “Workshop-based multiobjective security safeguard selection,” in *Proceedings of IEEE First International Conference on Availability, Reliability and Security*, pp. 8, 2006.
- [24] T. Okimoto, N. Ikegai, T. Ribeiro, K. Inoue, H. Okada, and H. Maruyama, “Cyber security problem based on multi-objective distributed constraint optimization technique,” in *43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop*, pp. 1–7, 2013.
- [25] J. Raissi, “Performance impact of imitation in multi-objective security service provisioning,” in *Proceedings of IEEE*, pp. 1–6, 2013.
- [26] K. Sallhammar, B. E. Helvik, and S. J. Knapskog, “Towards a stochastic model for integrated security and dependability,” in *IEEE First International Conference on Availability, Reliability and Security (ARES’06)*, pp. 8, 2006.
- [27] W. Stallings, *Cryptography and Network Security Principles and Practices*, Pearson Education, India, 2004.
- [28] S. Suriya, R. Deepalakshmi, S. S. Kannan, and S. P. Shantharajah, “Enhanced bee colony algorithm for complex optimization problems,” *International Journal on Computer Science and Engineering*, vol. 4, no. 1, pp. 72, 2012.
- [29] V. Viduto, W. Huang, and C. Maple, “Toward optimal multi-objective models of network security: Survey,” in *Proceedings of IEEE the 17th International Conference on Automation & Computing*, pp. 6–11, 2011.
- [30] V. Viduto, C. Maple, W. Huang, and A. Bochenkov, “A multi-objective genetic algorithm for minimizing network security risk and cost,” in *IEEE International Conference on High Performance Computing and Simulation*, pp. 462–467, 2012.
- [31] L. Wang, T. Islam, T. Long, A. Singhal, and S. Jajodia, “An attack graph-based probabilistic security metrics,” in *IFIP Annual Conference on Data and Applications Security and Privacy*, pp. 283–296, 2008.

Biography

Seyed Mahmood Hashemi received his bachelor from Islamic Azad University (Qazvin Branch) in software engineering at 2001 his master from Islamic Azad University (Science and Research Branch) in artificial intelligence at 2003. He is currently PhD candidate in Beijing University of Technology (BJUT). His research interests are Internet of Things (IoT), network security and Artificial Intelligence (AI).

Jingsha He received his Master and doctoral degrees in computer engineering from the University of Maryland

at College Park in the US. He is currently a professor in the School of Software Engineering at Beijing University of Technology (BJUT) in Beijing, China. Prior to joining BJUT in 2003, Prof. He worked for several multi-national companies such as IBM Corp., MCI Communications Corp. and Fujitsu Labs in the US. where he published more than 10 papers and received 12 U.S. patents. Since joining BJUT in 2003, Prof. He has published nearly 240 papers in journals and international conferences, received nearly 40 patents and 30 software copyrights in China and co-authored 7 books. He has been the principal investigators of more than 20 research projects. Prof. Hes research interests include information security, wireless networks and digital forensics.

A New Trusted Routing Protocol for Vehicular Ad Hoc Networks Using Trusted Metrics

Thangakumar Jeyaprakash¹, Rajeswari Mukesh²

(Corresponding author: Thangakumar Jeyaprakash)

School of Computing Sciences & Hindustan University¹

RajivGandhi Salai, Padur, Chennai, India

School of Computing Sciences & Hindustan University²

RajivGandhi Salai, Padur, Chennai, India

(Email: tkumar@hindustanuniv.ac.in, rajeswarim@hindustanuniv.ac.in)

(Received Nov. 20, 2015; revised and accepted Mar. 30 & May 31, 2016)

Abstract

Trusted routing in VANET is a challenging task due to highly dynamic network topologies and openness of wireless architecture. To provide secure routing among the Vehicular Ad-hoc Networks (VANET) and to avoid selfish nodes, an Optimized Node Selection Routing Protocol (Trusted-ONSRP) of VANET has been designed based on trusted metrics using a Trusted Computing Algorithm. The results stated that the T-ONSRP routing shows higher performance in security measures than the existing routing protocols.

Keywords: Routing protocol, trust, VANET, vehicular ad-hoc networks

1 Introduction

Vehicle to Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) are two distinguished models for real-time application. The past assertions for a centralized control object are committed to data handling and decision making. Given the self-motivated environment of the complicated communications nodes, the ubiquity along the road becomes a compulsory constraint. This might suggest a high- reasonable work, due to the claimed organization of stretched communication infrastructure road-sided [7]. To provide trust and reputation models [4, 5, 12], the following features such as Low Complexity [8], Scalability, Sparseness, Security [19], Performance and sustainability and Confidentiality have been considered in this proposed paper.

In the upcoming chapter, we will see a brief literature survey about the existing trusted routing protocols protocols for the usability of VANET. Section 3 describes the proposed work and the architecture of Trusted-ONSRP. Section 4 describes the T-ONSRP simulation experiments with various scenarios to find the reputation of vehicles

and the last section represents the results of the proposed routing protocol which has been compared with the existing routing protocol.

2 Related Works

Pophali et al. [9] proposed a trusted opportunistic routing protocol for VANET to improve the communication security and to safeguard the network from mischievous nodes. The author derives the minimum cost opportunistic routing to calculate the node cost to forward the packet from the source node to the destination. The malicious node has been strictly restricted from joining the network. Here, there is a chance of selfish nodes can be present in the network which restricts the transmission from the source to the destination vehicle.

In Yang [18] framework, the author describes a correspondence mining technique which is used for classifying similar information or same vehicles. The author proposed a reputation evaluation algorithm based on similarity theory. The reputation of each vehicle has been derived from the recommendation of other vehicles based on the weights calculations are made on which the selfish nodes are and other malicious nodes create a confusion instead of a reference given to a particular vehicle waiting for the reputation values.

Goudarzi et al. [1] presents a methodical literature review to provide complete and balanced material about various present trust conceptions in VANETs to upsurge excellence of data in transportation. The authors proposed a Trust model using the fuzzy logic to detect the misbehavior nodes. The authors also stated that there is no lightweight intelligence trust model available for VANETs that satisfies all the desired properties of a trust model.

Tan et al. [13] proposed a Novel trust management system. In this system, they use fuzzy logic and Graph the-

ory to evaluate the node trust value and it is integrated with the Optimized Link State Routing Protocol (OLSR). These algorithms are proposed to prevent malicious and victim nodes from participating in the networks [3] as much as possible. It does not include the selfish behavior nodes.

Rabayah et al. [2] proposed a routing protocol for VANET which associates the features of location based and topology based routing protocol. They integrate the protocol in such a way that if the location information is degraded, it automatically uses the reactive routing protocol to transmit the packet from the source to the destination. The author states the protocol is accessible and scalable and has an overhead over the new scalable Hybrid Routing does not include any Trust model to reduce the selfish nodes.

Wu et al. [11] proposed a new trusted routing protocol in VANET based on GeoDTN+Nav by using a greedy model which is associated with the four steps for initializing the routes, trusted routing establishment and the deletion of routes. As the greedy model [6] has more communication overhead, this model larger number of route discovery to establish the trusted route.

3 Proposed Work

3.1 Trusted Routing

There are two different types of trust models: 1) Infrastructure Based; 2) Self-organizing based.

The Infra-structure based trust models are Certificate based and RSS based. The Self Organizing models are entity oriented, data oriented and combined trust models. The reputation of the vehicle can be identified by data oriented Trust Model. The decentralized and self-controlled characteristics of Vehicular Adhoc Network are the widely recognized models, given the wireless-oriented nodes. To provide secured communication, a new trusted routing protocol of VANET has been proposed to avoid the selfish node behavior of the Vehicular Adhoc Networks which includes trust properties such as distance, direction, velocity and Trust value etc.

Figure 1 shows the architecture of ONSRP. Many attacks can be identified to compromise them, if the security requirements have been established for VANETs. Here we described the types of attacks of VANET with the activity of these attacks and their potential consequences. From these attacks, the selfish node behavior, characteristics and issues have been analyzed. The attacks are classified as attacks on identification and Authentication. (Impersonation and Sybil), attacks on Privacy. (Identity revealing and Location Tracking), attacks on non-repudiation (Sharing the same Credentials by two or more), attacks on confidentiality (Eavesdropping), attack on Availability (DoS, Selfish Node Behavior), availability in VANETs is very important in both communication channel and the participating nodes in the network. Network Denial of service leads to non-availability of the network for the

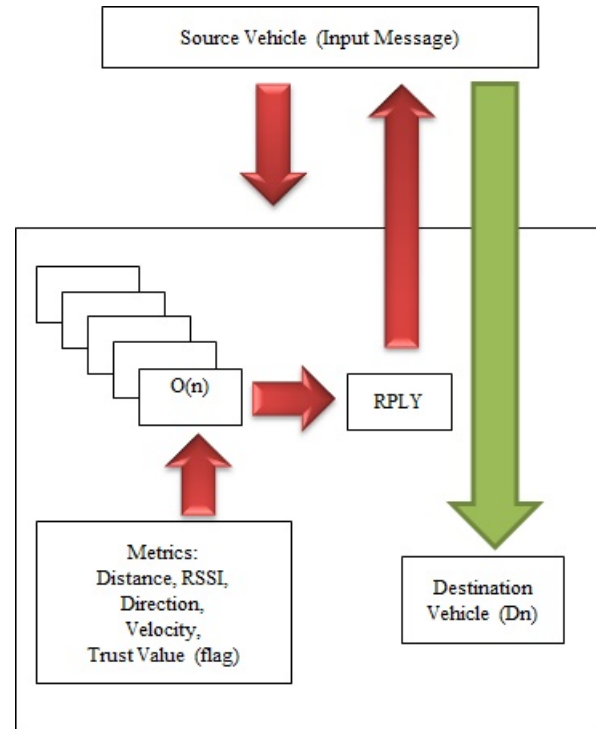


Figure 1: Architecture of ONSRP

participating vehicles which ends in dropping all messages or just a few according to self-interests known as Selfish Behavior.

The communication link failure due to high mobility can be identified by calculating the communication range depends upon the received signal strength. The Received signal strength index (RSSI) at a time period of transmission of packets from one node to another as shown with the following formulae using the distance between the two nodes. The Received signal strength index is directly proportional to the transmitted power and inversely proportional to the power loss. Each node communicates the data to the disseminating side of the next hop in the shortest route destination. The distance between the each node which is optimal is the Received Signal Strength Threshold. When the received signal strength index during the time period of receiving information is lesser than the RSST (RSST), the transmitting vehicle informs the previous node regarding the weaker signal strength which leads to communication link failure and discards the RREQ received from the precedent vehicle. Now the precedent node detects the weaker strength before transmitting the packet and broadcast the RREQ to other nodes.

3.2 Trust Metrics

The optimized node $O(n)$ selection routing protocol works on a hybrid reactive protocol and not on a proactive ba-

sis. The routing information will be shared together on demand using the trusted metrics such as distance, RSSI, direction etc. Otherwise, the route discovery process communication overhead increases, if the proactive routing has been followed. By discarding the broadcasting of RREQs, T-ONSRP is predictable considerably to avoid the communication overhead and reduce the communication delay. In addition to that, the ONSRP does not rely on any HELLO messages or ACK messages to check the status of the links to avoid unnecessary overheads. For the route maintenance or when the route break occurs, ONSRP used the RERR, Route error message to initiate a new route discovery process.

3.3 Distance

In order to determine this direction [14, 15], a node calculates the distance of the neighbor node as follows. At Time T1,

$$Distance(Do) = \Pi Minimum(D1||D2|| \dots ||Dn), \quad (1)$$

where $D1$ = Distance between the Last node of path 1 routing table and the Destination node; $D2$ = Distance between the Last node of path 2 routing table and the Destination node; DN = Distance between the Last node of path N routing table and the Destination node.

The communication link failure due to high mobility can be identified by calculating the communication range depends upon the received signal strength. The Received signal strength index (RSSI) at a time period of transmission of packets from one node to another as shown with the following formulae using the distance between the two nodes.

$$RSSIPr[do] = \frac{CtPt}{d^4Pl} \quad (2)$$

$$RSST = Dn = \sqrt{(X1 - X2)^2 + (Y1 - Y2)^2} \quad (3)$$

3.4 Direction

In order to determine this direction, a node calculates the direction of the neighbor node as follows.

At time T1, Direction in degrees

$$(Ao) = \Pi D(RWP(i, j)) || Min(D1||D2|| \dots ||Dn)(i, j), \quad (4)$$

where $D1$ = Distance between the Last node of path 1 routing table and the Destination node; $D2$ = Distance between the Last node of path 2 routing table and the Destination node; DN = Distance between the Last node of path N routing table and the Destination node; D = Destination; RWP = Random way points in the network are; i, j = two successive random way points.

3.5 Velocity

In the following, we utilize the velocity [16, 17] of nodes parameter from viewpoint to develop our Flag Trust

model. We consider the velocity distribution over simulation of network to determine the network connectivity status. The velocity of nodes is the main parameter that determines the network topology dynamics. It also plays a significant role in determining the estimated communication time between two vehicles. At Time T1,

$$Velocity(Vo) = \Pi V(Dn) || V(N1||N2|| \dots ||Nn), \quad (5)$$

where Dn = Destination node; $N1$ = Velocity of Neighbor Node 1 of Dn ; $N2$ = Velocity of Neighbor Node 1 of Dn ; Nn = Velocity of Neighbor Node 1 of Dn ; Vo = Optimized Velocity.

From Equations (3), (4) and (5):

$$Trustvalue = \Pi Do.Ao.Vo.FlagTrustCount. \quad (6)$$

3.6 The Algorithm

When the source node has the information to send at time T1, the trustworthiness of each node has been calculated using the trusted computing algorithm for each node available between the source and the destination vehicle. At this time T1, the algorithm finds the optimized node to transmit the packet from the source node to the destination node for the most reliable transmission of data. The source node creates a RREQ, Route request message and broadcasts to the neighbor nodes to find the possible route to the destination (See Algorithm 1).

Each node transmits the RREQ to the neighbor nodes to find the destination node for the packet transmission. The intermediate vehicles those received the RREQ are allowed to forward the route REPLY, when its trusted value has been calculated by the trusted routing protocol algorithm. Otherwise, the RREQ will be discarded. When the RREQ arrives at the neighbor node to the destination, and it is assumed to be a trusted vehicle, a route reply will be sent back to the source vehicle to start the transmission of data without link failure due high mobility and selfish node behavior in the Vehicular Adhoc Network.

4 Simulation Experiments

4.1 General Assumptions

Some assumptions have to be made about the ONSRP model [18] to make complexity lesser:

- At most one or two selfish node vehicles are available in the network.
- No hurdles and infrastructures such as buildings etc. in the road topology.
- The type of communication is bidirectional between the two vehicles, if available in the coverage area of the network.

Algorithm 1 Trusted Node Identification

```

1: Input: A source vehicle(S) and the destination (D)
   vehicle.
2: Output: Transmission of data with less no of link
   failure.
3: Get intermediate nodes trusted values using trusted
   computing algorithm.
4: Calculate the trusted values for all the intermediate
   nodes present between S and D.
5: Trust Threshold (TTH)= Total no of Nodes (Initial-
   ized Value)
6:  $O(n) = \alpha\Pi(D_o, A_o, V_o)$ 
7:  $T(\beta(O(n))) = \text{initial\_connect\_value} +$ 
    $\text{Total No of Nodes}$ 
8: Compare  $T(\beta(O(n)))$  with Trust Threshold(TTH)
9: if  $T(\beta(O(n))) >> \text{TrustThreshold}(TTH)$  then
10:   $T(\beta(O(n)))$  to send an RREP to the source vehicle(S)
11:  Discard RREQ Go to Line no 4
12: end if
13: Start data transfer
14: End

```

- Each vehicle is connected to the other in the Vehicular network and follows the car following model. Stand by vehicles are also available in the network.
- Each vehicle is equipped with global positioning system (GPS) to show its own location which helps to provide the absolute information to other vehicles.
- All the vehicles transmits and receive the data using Optimized Node selection routing protocol with the calculated trusted node to avoid the selfish node behavior which leads to communication link failure.
- The energy back up of each vehicle is always sufficient for the requirement of application to transmit the data from one vehicle to another.

4.2 Scenario I: All Vehicles Moving in the Same Direction (Towards East)

When a source vehicle A wants to transmit a packet to the Destination vehicle, it has to obtain the RSSI value of the neighbor node of the destination vehicle to send back the RRPLY for the efficient data transfer. In Figures 2, 3, 4, 5 each vehicle is labelled with a vehicle id presented in the vehicular Adhoc network. Note the A,B,C,D,E,F,G,H,I,J,N are representing the source vehicle, intermediate nodes and the destination vehicle respectively. The nodes K[RSSI(i)], L[RSSI(i+1)], M[RSSI (n-1)] are the set of intermediate nodes which has been received the RREQ from the source vehicle A. Thus the RREQ is broadcasted for the nodes B,E,G,J,L,N and D,F,H,M,N and C,I,K,L,N respectively. According to the formulae, the RSSI value has been calculated for the standard distance to reduce the complexity of the routing protocol. In Scenario I, as all the vehicles are moving in the

same direction, trusted routing algorithm has been implemented to the minimum distance RSSI value node.

The trusted routing algorithm has been implemented to the minimum distance RSSI value node [10].

$$\begin{aligned}
 RSSI[(i)] &= 52.45dBm \text{ where } i = 1m \\
 RSSI[(i+1)] &= 53.47dBm \text{ where } i = 2m \\
 RSSI[(i+3)] &= 58.23dBm \text{ where } i = 4m \\
 RSSI[(i+5)] &= 62.34dBm \text{ where } i = 6m \\
 RSSI[(i+8)] &= 64.45dBm \text{ where } i = 9m \\
 RSSI[(i+10)] &= 66.32dBm \text{ where } i = 11m \\
 RSSI[(i+14)] &= 75.43dBm \text{ where } i = 15m \\
 RSSI[(i+19)] &= 80.71dBm \text{ where } i = 20m.
 \end{aligned}$$

Trusted Node Calculation: Scenario I

Node M = 52.45 DBm;

If Data Transfer initiated via Node M:

$$\begin{aligned}
 InitialConnectValue &= 1; \\
 InitialReputationValue(Rn) &= 1; \\
 TotalnumberofNodespresent &= 250; \\
 TrustThreshold(TTH) &= InitializedValue \\
 &= 250; \\
 O(n) &= \alpha\beta(D_o, A_o, V_o); \\
 Rn(O(n)) &= Rn + initial_connect_value \\
 &\quad + InitializedValue = 252; \\
 Rn(Node(M)) &= 252; \\
 Rn(Node(M)) &> TrustThreshold(TTH); \\
 setVehicletrustedflag &= 1.
 \end{aligned}$$

else

$$\begin{aligned}
 InitializeReputationValue(Rn) &= 0; \\
 InitialConnectValue &= 0; \\
 Rn(O(n)) &= Rn + initial_connect_value \\
 &\quad + InitializedValue = 250.
 \end{aligned}$$

4.3 Scenario II: All Vehicles Moving Bidirectional (Towards East and West)

In the scenario II, the vehicles are moving bidirectionally. In Figure 6, When a source vehicle A wants to transmit a packet to the Destination vehicle, Even though it has to obtain the RSSI value of the neighbor node of the destination vehicle to send back the RRPLY for efficient data transfer, as the vehicles are moving in different lanes with opposite directions. In Scenario II, as all the vehicles are moving in the opposite direction, trusted routing algorithm has been implemented to the nodes moving in the same direction along with the destination node with the minimum distance RSSI value node.

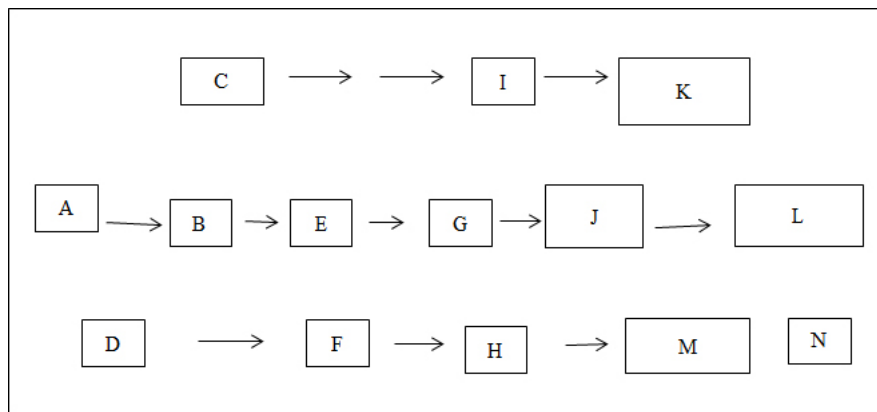


Figure 2: Set of vehicles A, B, C, D, E, F, G, H, I, J, N

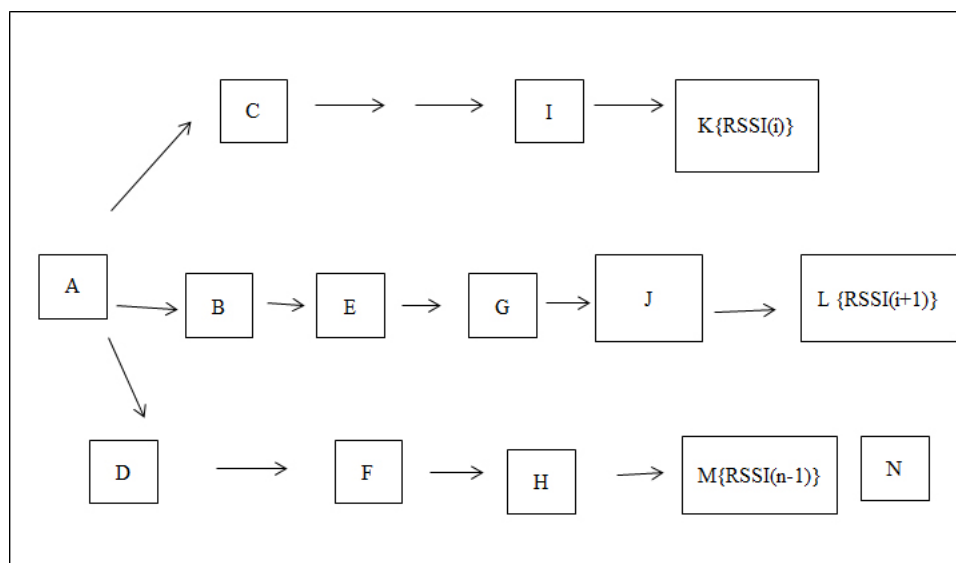


Figure 3: RSSI calculation

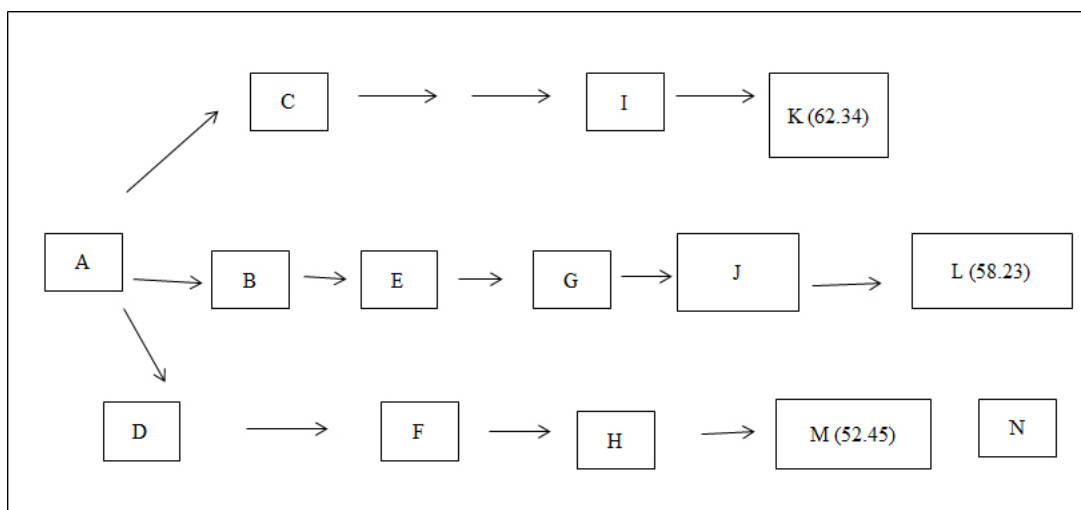


Figure 4: Node with RSSI values (Minimum distance)

Trusted Node Calculation: (Scenario II)

Node M = 58.45 DBm.

If Data Transfer initiated via Node M:

```

InitialConnectValue = 1;
InitialReputationValue(Rn) = 1;
TotalnumberofNodespresent = 250;
TrustThreshold(TTH) = InitializedValue
                        = 250;
O(n) = αΠ(Do, Ao, Vo);
Rn(Node(M)) = 252fromScenarioI;
Rn(O(n))) = Rn + initial_connect_value
            + Initialized Value
            = 252 + 1 + 250 = 503;
Rn(Node(M)) = 503;
Rn(Node(M)) > Trust Threshold (TTH);
set Vehicle trusted flag = 1.

```

else

```

InitializeReputationValue(Rn) = 0;
InitialConnectValue = 0;
Rn(O(n))) = Rn + initial_connect_value
            + Initialized Value = 250;
Rn(Node(M)) == Trust Threshold (TTH);
set Vehicle trusted flag = 0.

```

4.4 Scenario III: Selfish node Behavior (Node M)

In the selfish node attack situation, there is at most one Selfish node vehicle present in the network. In Figure 7, Assume the vehicle M. Vehicle M could be either a mischievous or a reputed vehicle. According to the formulae, the RSSI value has been calculated for the standard distance to reduce the complexity of the routing protocol. In Scenario III, as all the vehicles are moving in the same and opposite direction with the available of malicious node (selfish node), trusted routing algorithm has been implemented to the find the reputed node or a selfish node for the efficient data transfer to avoid the non-availability of the network.

Trusted Node Calculation: (Scenario III)

Node M = 52.45 DBm;

If Data Transfer initiated via Node M fails due to the

Selfish Node Attack:

```

InitialConnectValue = 1;
InitialReputationValue(Rn) = 1;
TotalnumberofNodespresent = 250;
TrustThreshold(TTH) = InitializedValue
                        = 250;
O(n) = αΠ(Do, Ao, Vo);
Rn(O(n))) = Rn + initial_connect_value
            + Initialized Value = 252;
Rn(Node(M)) = 252;
Rn(Node(M)) > TrustThreshold(TTH);
setVehicletrustedflag = 1.

```

else

```

InitializeReputationValue(Rn) = 0;
InitialConnectValue = 0;
Rn(O(n))) = Rn + initial_connect_value
            + Initialized Value = 250;
Rn(Node(M)) == TrustThreshold(TTH);
setVehicletrustedflag = 0.

```

5 Results and Comparisons

In Figures 8 and 9, the results shows the performance of ONSRP eventually exceeds the performance of Scalable Hybrid Routing Protocol, Modified Ad-hoc On demand distance vector Routing protocol and Greedy Perimeter coordinator Routing Protocol with the aspects of the packet delivery ratio, End-End Delay and total number of link failures.

In Figure 10, the total number of link failures has been reduced by ignoring the selfish nodes available on the network. The number of link failures has been reduced in a more gradual manner when compared to the existing routing protocol using the Optimized Node selection Routing Protocol. The graph shows the performance of ONSRP against the existing routing protocols in the presence of various mobility models and the Drivers realistic mobility model. From the results of various simulations, we have proved the performance of the proposed ONSRP against the various existing routing protocols.

6 Conclusions and Scope of Work

An Optimized node selection routing protocol of VANET has been implemented using Trusted Computing Algorithms with the features of extended light weight routing and routing messages with trust information which can be updated directly through optimized node selection Routing protocol Algorithm. When performing trusted routing discovery, communication overhead can be reduced

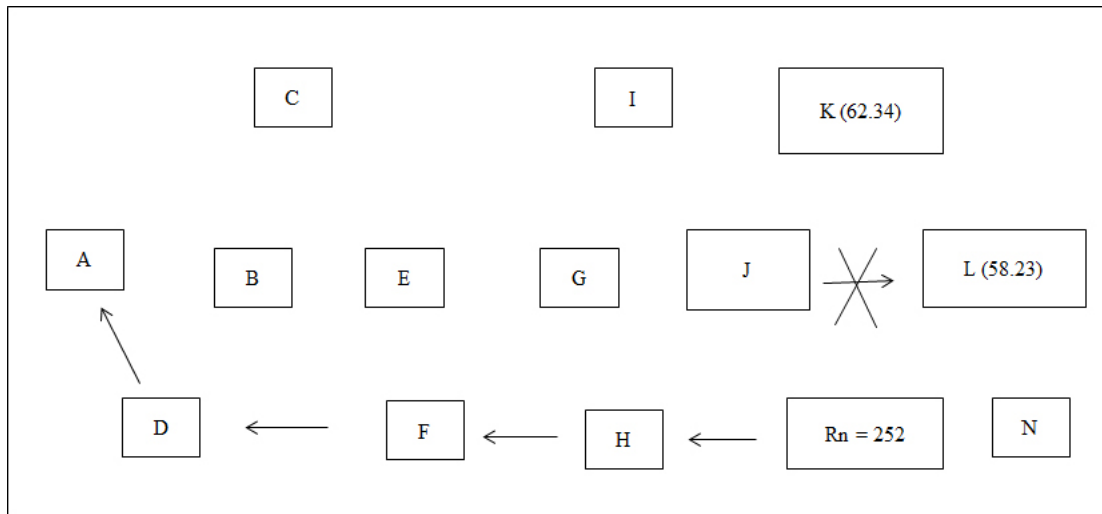


Figure 5: RRPLY sent to source node from node M

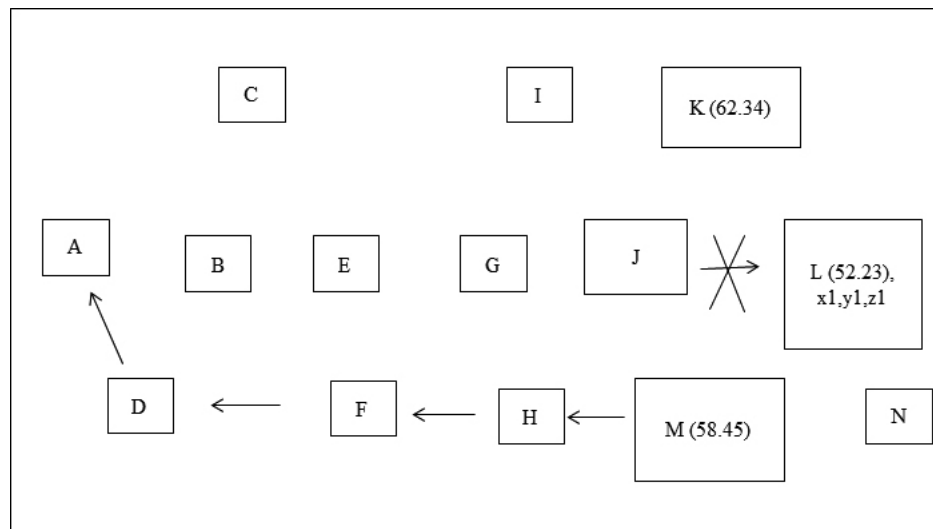


Figure 6: RPLY sent to source node via M (same direction)

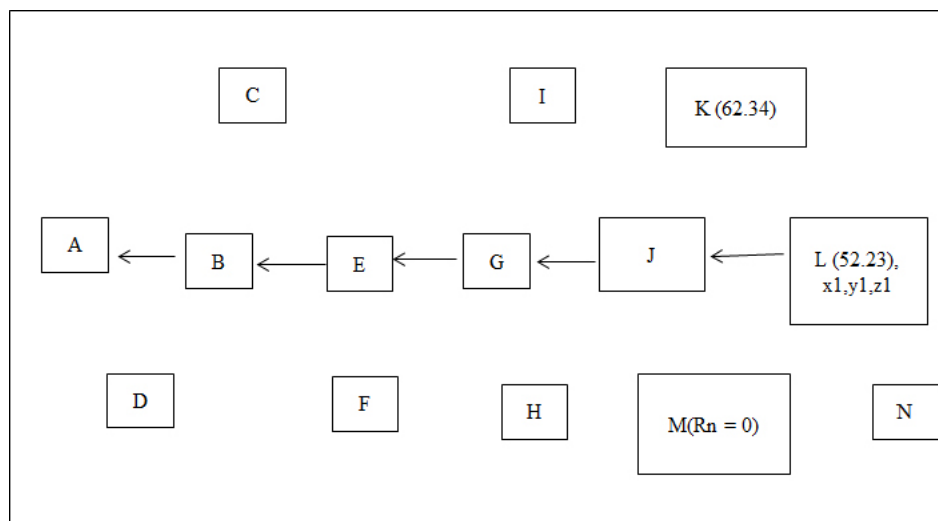


Figure 7: RRPLY sent to source node from node L as M behaves as selfish node (Rn = 0)

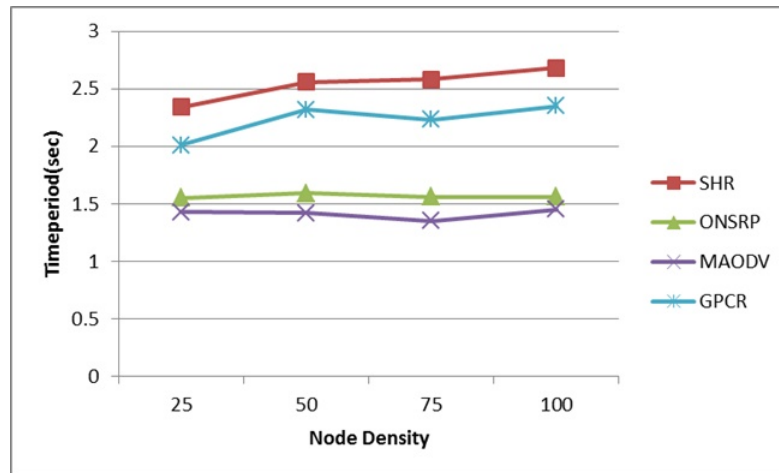


Figure 8: End-End delay analysis

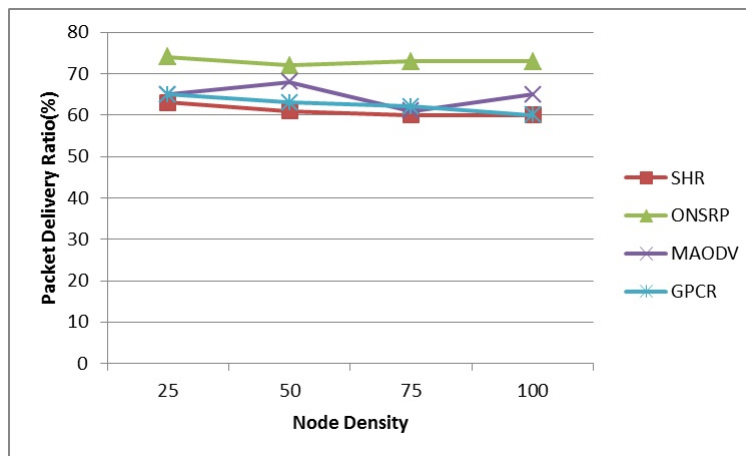


Figure 9: Packet delivery ratio

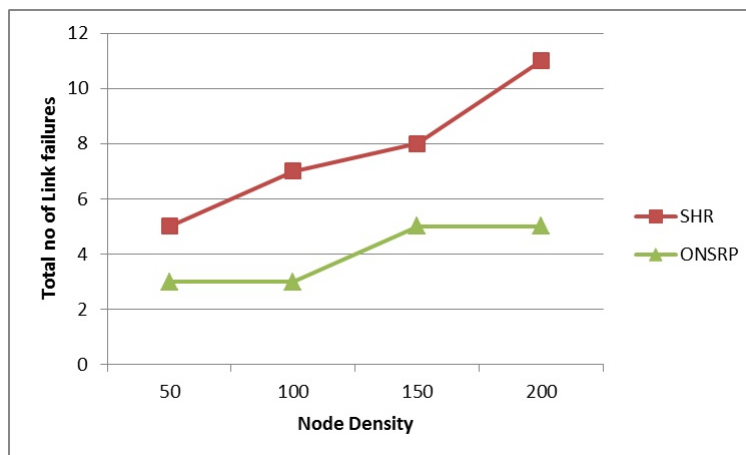


Figure 10: Link failures vs. node density

and packet delivery ratio can be increased by avoiding the frequent route discovery process. This performance has been proved, but can perhaps be shown to be valid for other existing shortest-path protocols. The scope of the work can move towards the comparison of T-ONSRRP against other routing protocols in an attempt to further support this performance analysis.

References

- [1] S. A. Soleymani, A. H. Abdullah, W. H. Hassan, M. H. Anisi, S. Goudarzi, M. A. R. Baee and S. Mandala, "Trust management in vehicular ad hoc network: A systematic review", *EURASIP Journal on Wireless Communications and Networking*, DOI: 10.1186/s13638-015-0353-y, Dec. 2015.
- [2] M. Al-Rabayah and R. Malaney, "A new hybrid location-based ad-hoc routing protocol," *IEEE Global Telecommunications Conference (GLOBECOM'10)*, vol. 1, no. 6, pp. 6–10, Dec. 2010.
- [3] C. Bhalodia, A. M. Lathigaraet, "Modified route maintenance in AODV routing protocol," *International Journal of Advance Engineering and Research Development*, vol. 1, no. 5, pp. 1–9, May 2014.
- [4] M. Gerlach and F. Friederici, "Implementing trusted vehicular communications," *69th IEEE Vehicular Technology Conference (VTC'09)*, pp. 1–2, Apr. 2009.
- [5] F. G. Mármol and G. M. Pérez, "Trip, A trust and reputation infrastructure-based proposal for vehicular ad hoc networks," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 934–941, May 2012.
- [6] B. Karp and H. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks," in *Proceedings of ACM MobiCom*, pp. 243–254, 2000.
- [7] M. Mejia and R. Chaparro-Vargas, "Distributed trust and reputation mechanisms for vehicular ad-hoc networks," *Vehicular Technologies - Deployment and Applications*, vol. 1, no. 6, pp. 6–10, Dec. 2013.
- [8] P. Papadimitratos, L. Buttyan, J. P. Hubaux, F. Kargla, A. Kung, and M. Raya., "Architecture for secure and private vehicular communications," in *7th IEEE International Conference on ITS Telecommunications*, pp. 1–6, 2007.
- [9] M. Pophali, S. Mohod, T. S. Yengantiwar, "Trust based opportunistic routing protocol for VANET communication," *International Journal Of Engineering And Computer Science*, vol. 3, no. 8, pp. 7408–7414, Aug. 2014.
- [10] R. C. Poonia and V. Singh, "Performance evaluation of radio propagation model for vehicular ad hoc networks using vanetmobisim and NS-2," *International Journal of Distributed and Parallel Systems*, vol. 3, no. 4, July 2012.
- [11] W. Qiwu, Q. Liu, L. Zhang, Z. Zhang, "A trusted routing protocol based on GeoDTN+Nav in VANET," *China Communications*, vol. 11, no. 14, pp. 166–174, 2014.
- [12] M. Raya, P. Papadimitratos, and J. P. Hubaux, "Securing vehicular communications", *IEEE Wireless Communications*, vol. 13, no. 5, pp. 8–15, Oct. 2006.
- [13] S. Tan, X. Li, and Q. Dong, "A trust management system for securing data plane of ad hoc networks," *IEEE Transactions on Vehicular Technology*, DOI: 10.1109/TVT.2015.2495325, 2015.
- [14] J. Thangakumar, R. Mukesh, "Simulation of vehicular adhoc network routing protocols with the performance analysis," *Journal of Communication Software and Systems*, vol. 11, no. 2. pp. 86–93, June 2015.
- [15] J. Thangakumar, R. Mukesh, "An optimized node selection routing protocol of vehicular adhoc networks - A hybrid model," *Journal of Communication Software and Systems*, vol. 11, no. 2. pp. 80–85, June 2015.
- [16] J. Thangakumar, R. Mukesh, "An enhanced routing protocol of VANET using trust computing algorithms," *International Journal of Soft Computing*, vol. 11, no. 2. pp. 45–51, Jan. 2016.
- [17] J. Thangakumar, R. Mukesh, "Mathematical analysis of trust routing algorithms," *Elsevier Procedia Computer Science Journal*, vol. 58, pp. 105–112, 2015.
- [18] N. Yang, "A similarity based trust and reputation management framework for VANETs," *International Journal of Future Generation Communication and Networking*, vol. 6, no. 2, Apr. 2013.
- [19] J. Zhang, "A survey on trust management for vanets," in *IEEE Advanced Information Networking and Applications (AINA'11)*, pp. 105–112, 2011.

Thangakumar Jeyaprakash has received his B.E Degree in Electrical and Electronics Engineering from Dr.Sivanthi Aditanar College of Engineering, Tamilnadu in 2003. He obtained his M.Tech in Computer Science and Engineering, SRM University, Chennai. He is presently pursuing his Ph.D in Hindustan Institute of Technology and Science, Chennai, Tamilnadu, India. He has Eleven years of industrial, academic and research Experience. He is a member of IEEE, IET. His area of Interests is Mobile Ad hoc Networks, Vehicular Ad hoc Networks, Cryptography and Network Security, Data mining and software Engineering.

Rajeswari Mukesh has received her Ph.D. degree in Computer Science and Engineering from Jawaharlal Nehru University. Hyderabad. At present, she is a Professor and Head of Computer science and Engineering department at Hindustan University. She is guiding 8 PhD candidates. She has published more than 10 international journals and attended more than 15 international and National Conferences. Her area of specialization is Big Data, Biometrics, Adhoc Networks, Cyber Security. She is a Member of IEEE and IET. She has won the Women Engineer award recently from IET.

New Constructions of Binary Interleaved Sequences with Low Autocorrelation

Ruifang Meng, Tongjiang Yan

(Corresponding author: Tongjiang Yan)

College of Science, China University of Petroleum, Qingdao, Shandong 266580, China

Key Laboratory of Network Security and Cryptology, Fujian Normal University, Fuzhou, Fujian 350117, China

(Email: yantoji@163.com)

(Received Apr. 24, 2016; revised and accepted June 29 & July 19, 2016)

Abstract

The autocorrelation of a key stream sequence in a stream cipher is an important cryptographic property. This paper proposes two constructions of binary interleaved sequences of period $4N$ by selecting appropriate shift sequences, subsequences and complement sequences. And the autocorrelation functions of new sequences are given. The results show that these sequences have low autocorrelation under certain conditions.

Keywords: *Interleaved sequences, low autocorrelation, stream cipher, subsequences*

1 Introduction

Pseudorandom sequences with low autocorrelation have wide applications in code-division multi-access system, spread spectrum communication and many other engineering fields [4].

Given two binary sequences $a = a(t)$ and $b = b(t)$ of period N , the periodic correlation between them is defined by

$$R_{a,b}(\tau) = \sum_{t=0}^{N-1} (-1)^{a(t)+b(t+\tau)}, 0 \leq \tau < N, \quad (1)$$

where the addition $t + \tau$ is performed modulo N . $R_{a,b}(\tau)$ is called the (periodic) cross correlation function of a and b . If $a = b$, $R_{a,b}(\tau)$ is called the (period) autocorrelation function of a , denoted by $R_a(\tau)$ for short [11].

According to the remainder of N modulo 4, the optimal values of out-of-phase autocorrelations of binary sequences are classified into four types as follows:

- 1) $R_a(\tau) = -1$ if $N \equiv 3 \pmod{4}$;
- 2) $R_a(\tau) \in \{-2, 2\}$ if $N \equiv 2 \pmod{4}$;
- 3) $R_a(\tau) \in \{1, -3\}$ if $N \equiv 1 \pmod{4}$;
- 4) $R_a(\tau) \in \{0, -4, 4\}$ if $N \equiv 0 \pmod{4}$, where $0 < \tau < N$.

In the first case, $R_a(\tau)$ is often called ideal autocorrelation. In the last case, $R_a(\tau)$ is three level, then it can also be called optimal autocorrelation magnitude [11]. Specially, except one point, the out-of-phase autocorrelation values of sequence a are all included in the set $\{0, -4, 4\}$, we call $R_a(\tau)$ almost optimal autocorrelation magnitude [12]. For more details about optimal autocorrelation, the reader is referred to [1, 2, 10].

The interleaved structure of sequences for constructing sequences with low out-of-phase autocorrelation and crosscorrelation was firstly introduced by Gong [5]. There are some known constructions of binary interleaved sequences with low autocorrelation.

In 2010, Tang and Gong gave three new interleaved constructions of binary sequences with low autocorrelation value or magnitude [8]. Subsequently, Yan showed a more general construction and searched for a new construction of binary interleaved sequences with optimal autocorrelation [11].

In 2011, based on an arbitrary ideal autocorrelation sequence, generalized GMW sequence and its modified version, two types of Legendre sequences, twin-prime sequence and its modified version respectively, Zhang, Wen and Qin found five constructions of binary interleaved sequences of period $2N \times 2$ with almost optimal autocorrelation magnitude [12]. Furthermore, Ke and Lin also obtained several binary sequences with optimal autocorrelation value by using decimated sequences [6]. In this paper, we propose two new constructions of binary sequences with low autocorrelation based on interleaving technology.

This paper is organized as follows. Section 2 introduces some related definitions and lemmas which would be used later. In Section 3, we present two new constructions of binary sequences with low autocorrelation magnitude, and give the complete autocorrelation distributions of these sequences. Conclusions are given in Section 4.

2 Preliminaries

2.1 Interleaved Sequence

Definition 1. [7] Let $\{a_0, a_1, \dots, a_{T-1}\}$ be a set of T sequences of period N . An $N \times T$ matrix U is formed by placing the sequence a_i on the i th column, where $0 \leq i \leq T-1$. Then one can obtain an interleaved sequence u of period NT by concatenating the successive rows of the matrix U . For simplicity, the interleaved sequence u can be written as

$$u = \mathbf{I}(a_0, a_1, \dots, a_{T-1}),$$

where \mathbf{I} denotes the interleaved operator.

Lemma 1. [11] Let the binary sequence $s = \mathbf{I}(a_0(k), a_1(k), \dots, a_{T-1}(k))$, be a binary interleaved sequence of period KT , where $0 \leq k \leq K-1$, and $T = \tau_1 T + \tau_2$, where $0 \leq \tau_2 \leq T-1$. Its left shifted version is shown as:

$$L^\tau(s) = \mathbf{I}(a_{\tau_2}(k + \tau_1), a_{1+\tau_2}(k + \tau_1), \dots, a_{T-1}(k + \tau_1), a_0(k + \tau_1 + 1), \dots, a_{\tau_2-1}(k + \tau_1 + 1)),$$

where L denotes the left cyclic shift operator.

2.2 Subsequence

Lemma 2. Let N be an odd number, $s = (s(0), s(1), \dots, s(N-1))$ be a binary sequence of period N . Take two subsequences of sequence s : $s_1 = (s(0), s(2), \dots, s(2t), \dots)$ and $s_2 = (s(1), s(3), \dots, s(2t+1), \dots)$, where $t = 0, 1, 2, \dots, N-1$, $2t$ and $2t+1$ are performed modulo N respectively. Then we have some results as follows:

- 1) $R_{s_1}(\tau) = R_s(2\tau)$;
- 2) $R_{s_2}(\tau) = R_s(2\tau)$;
- 3) $R_{s_1, s_2}(\tau) = R_s(2\tau + 1)$;
- 4) $R_{s_2, s_1}(\tau) = R_s(2\tau - 1)$.

Proof By Equation (1), we have

$$\begin{aligned} R_{s_1}(\tau) &= \sum_{t=0}^{N-1} (-1)^{s_1(t) + s_1(t+\tau)} \\ &= \sum_{t=0}^{N-1} (-1)^{s(2t) + s(2t+2\tau)} \\ &= \sum_{t=0}^{N-1} (-1)^{s(t') + s(t'+2\tau)} \\ &= R_s(2\tau), \end{aligned}$$

where $t' = 2t$. So 1) is proved. Similarly, the other three results can be proved obviously.

3 Two New Constructions

In this section, we introduce two new constructions of binary sequences of period $4N$ with low autocorrelation.

3.1 Construction A

Let $N \equiv 3 \pmod{4}$, $s = (s(0), s(1), \dots, s(N-1))$ be a binary ideal autocorrelation sequence of period N . Define a new binary interleaved sequence of period $4N$ as the following:

$$a = I(s_1, L^d(\overline{s_1}), s_2, L^d(\overline{s_2})), \quad (2)$$

where $\overline{s_1}$ is the complement sequence of s_1 , $\overline{s_2}$ is the complement sequence of s_2 , $d \neq \frac{N+1}{4}$ is an integer. Obviously, the sequence a possesses the balance property with the symbols "1" and "0" [9]. Next we consider the autocorrelation of the new sequence a .

Let $\tau = 4\tau_1 + \tau_2$, $\tau_2 = 0, 1, 2, 3$. By Lemmas 1 and 2, the autocorrelation of sequence a due to four different values of τ_2 can be given by the following.

Case 1. $\tau_2 = 0$, $0 < \tau_1 < N$.

$$\begin{aligned} R_a(\tau) &= R_a(4\tau_1) \\ &= R_{s_1}(\tau_1) + R_{L^d(\overline{s_1})}(\tau_1) + R_{s_2}(\tau_1) + R_{L^d(\overline{s_2})}(\tau_1) \\ &= 4R_s(2\tau_1). \end{aligned}$$

Since $0 < \tau_1 < N$, $2\tau_1 \neq 0 \pmod{N}$, $R_s(2\tau_1) = -1$. Then $R_a(\tau) = -4$, and it turns up $N-1$ times altogether.

Case 2. $\tau_2 = 1$, $0 \leq \tau_1 < N$.

$$\begin{aligned} R_a(\tau) &= R_a(4\tau_1 + 1) \\ &= R_{s_1, \overline{s_1}}(\tau_1 + d) + R_{\overline{s_1}, s_2}(\tau_1 - d) \\ &\quad + R_{s_2, \overline{s_2}}(\tau_1 + d) + R_{\overline{s_2}, s_1}(\tau_1 + 1 - d) \\ &= -R_{s_1}(\tau_1 + d) - R_{s_1, s_2}(\tau_1 - d) \\ &\quad - R_{s_2}(\tau_1 + d) - R_{s_2, s_1}(\tau_1 + 1 - d) \\ &= -R_s(2(\tau_1 + d)) - R_s(2(\tau_1 - d) + 1) \\ &\quad - R_s(2(\tau_1 + d)) - R_s(2(\tau_1 + 1 - d) - 1) \\ &= -2R_s(2\tau_1 + 2d) - 2R_s(2\tau_1 - 2d + 1). \end{aligned}$$

- 1) If $\tau_1 = N - d$, $(2\tau_1 + 2d) = 0 \pmod{N}$, $2\tau_1 - 2d + 1 \neq 0 \pmod{N}$. Then $R_s(2\tau_1 + 2d) = N$, $R_s(2\tau_1 - 2d + 1) = -1$. So $R_a(\tau) = -2N + 2$;
- 2) If $\tau_1 = \frac{N+2d-1}{2}$, $2\tau_1 + 2d \neq 0 \pmod{N}$, $2\tau_1 - 2d + 1 = 0 \pmod{N}$. Then $R_s(2\tau_1 + 2d) = -1$, $R_s(2\tau_1 - 2d + 1) = N$. So $R_a(\tau) = 2 - 2N$;
- 3) If $\tau_1 \neq N - d$ and $\tau_1 \neq \frac{N+2d-1}{2}$, $2\tau_1 + 2d \neq 0 \pmod{N}$ and $2\tau_1 - 2d + 1 \neq 0 \pmod{N}$. Then $R_s(2\tau_1 + 2d) = R_s(2\tau_1 - 2d + 1) = -1$. So $R_a(\tau) = 4$.

In this case, $R_a(\tau) = -2N + 2$ turns up 2 times, and $R_a(\tau) = 4$ turns up $N - 2$ times.

Case 3. $\tau_2 = 2, 0 \leq \tau_1 < N$.

$$\begin{aligned}
 & R_a(\tau) \\
 = & R_a(4\tau_1 + 2) \\
 = & R_{s_1, s_2}(\tau_1) + R_{\overline{s_1}, \overline{s_2}}(\tau_1) \\
 & + R_{s_2, s_1}(\tau_1 + 1) + R_{\overline{s_2}, \overline{s_1}}(\tau_1 + 1) \\
 = & R_s(2\tau_1 + 1) + R_s(2\tau_1 + 1) \\
 & + R_s(2(\tau_1 + 1) - 1) + R_s(2(\tau_1 + 1) - 1) \\
 = & 4R_s(2\tau_1 + 1).
 \end{aligned}$$

- 1) If $\tau_1 = \frac{N-1}{2}, 2\tau_1 + 1 = 0 \pmod{N}$. Then $R_s(2\tau_1 + 1) = N$. So $R_a(\tau) = 4N$, and it turns up only 1 time;
- 2) If $\tau_1 \neq \frac{N-1}{2}, 2\tau_1 + 1 \neq 0 \pmod{N}$. Then $R_s(2\tau_1 + 1) = -1$. So $R_a(\tau) = -4$, and it turns up $N - 1$ times.

Case 4. $\tau_2 = 3, 0 \leq \tau_1 < N$.

$$\begin{aligned}
 & R_a(\tau) \\
 = & R_a(4\tau_1 + 3) \\
 = & R_{s_1, \overline{s_2}}(\tau_1 + d) + R_{\overline{s_1}, s_1}(\tau_1 + 1 - d) \\
 & + R_{s_2, \overline{s_1}}(\tau_1 + 1 + d) + R_{\overline{s_2}, s_2}(\tau_1 + 1 - d) \\
 = & -R_s(2(\tau_1 + d) + 1) - R_s(2(\tau_1 + 1 - d)) \\
 & - R_s(2(\tau_1 + 1 + d) - 1) - R_s(2(\tau_1 + 1 - d)) \\
 = & -2R_s(2\tau_1 + 2d + 1) - 2R_s(2\tau_1 - 2d + 2).
 \end{aligned}$$

- 1) If $\tau_1 = \frac{N-2d+1}{2}, 2\tau_1 + 2d + 1 = 0 \pmod{N}, 2\tau_1 - 2d + 2 \neq 0 \pmod{N}$. Then $R_s(2\tau_1 + 2d + 1) = N, R_s(2\tau_1 - 2d + 2) = -1$. So $R_a(\tau) = -2N + 2$;
- 2) If $\tau_1 = \frac{N+2d-2}{2}, 2\tau_1 + 2d + 1 \neq 0 \pmod{N}, 2\tau_1 - 2d + 2 = 0 \pmod{N}$. Then $R_s(2\tau_1 + 2d + 1) = -1, R_s(2\tau_1 - 2d + 2) = N$. So $R_a(\tau) = 2 - 2N$;
- 3) If $\tau_1 \neq \frac{N-2d+1}{2}$ and $\tau_1 \neq \frac{N+2d-2}{2}, 2\tau_1 + 2d + 1 \neq 0 \pmod{N}$, and $2\tau_1 - 2d + 2 \neq 0 \pmod{N}$. Then $R_s(2\tau_1 + 2d + 1) = R_s(2\tau_1 - 2d + 2) = -1$. So $R_a(\tau) = 4$.

In this case, $R_a(\tau) = -2N + 2$ turns up 2 times, and $R_a(\tau) = 4$ turns up $N - 2$ times altogether.

According to the above discussion about $R_a(\tau)$, we obtain the following theorem.

Theorem 1. Let $0 \leq \tau < 4N$, and $d \neq \frac{N+1}{4}$. The autocorrelation function of the new sequence a defined by Equation (2) is:

$$R_a(\tau) = \begin{cases} 4N & 2 \text{ times,} \\ 2 - 2N & 4 \text{ times,} \\ 4 & 2N - 4 \text{ times,} \\ -4 & 2N - 2 \text{ times.} \end{cases}$$

Specially, let $d = \frac{N+1}{4}$. Then $2\tau_1 + 2d = 2\tau_1 - 2d + 1 \pmod{N}$ and $2\tau_1 + 2d + 1 = 2\tau_1 - 2d + 2 \pmod{N}$. So in Case 2, the autocorrelation of the sequence a can be reduced to $R_a(\tau) = -4R_s(2\tau_1 + 2d)$. If $\tau_1 = \frac{3N-1}{4}$, then

$2\tau_1 + 2d = 0 \pmod{N}, R_s(2\tau_1 + 2d) = N$. So $R_a(\tau) = -4N$ and it turns up 1 time. Otherwise, together with the facts that s has ideal autocorrelation, $R_a(\tau) = 4$. Similarly, in Case 4, $R_a(\tau) = -4R_s(2\tau_1 + 2d + 1)$. If $\tau_1 = \frac{N-3}{4}$, then $2\tau_1 + 2d + 1 = 0 \pmod{N}, R_s(2\tau_1 + 2d + 1) = N$. So $R_a(\tau) = -4N$ and it turns up 1 time. Otherwise, $R_a(\tau) = 4$. Naturally, based on Theorem 1, we can get the following corollary.

Corollary 1. Let $0 \leq \tau < 4N$, and $d = \frac{N+1}{4}$. The autocorrelation function of the new sequence a defined by Equation (2) is:

$$R_a(\tau) = \begin{cases} 4N & 2 \text{ times,} \\ -4N & 2 \text{ times,} \\ 4 & 2N - 2 \text{ times,} \\ -4 & 2N - 2 \text{ times.} \end{cases}$$

3.2 Construction B

Let $N \equiv 3 \pmod{4}$, $s = (s(0), s(1), \dots, s(N-1))$ be a binary ideal autocorrelation sequence of period N . Define a new binary interleaved sequence of period $4N$ as the following:

$$a = I(s_1, L^d(\overline{s_1}), \overline{s_2}, L^d(s_2)), \quad (3)$$

where $\overline{s_1}$ is the complement sequence of s_1 , $\overline{s_2}$ is the complement sequence of s_2 , d is an arbitrary integer and $d \neq \frac{(N+1)}{4}$.

Similarly to the Construction A, the new sequence a constructed as above is also balanced, and we can gain the autocorrelation of the new sequence a by calculation.

Let $\tau = 4\tau_1 + \tau_2, \tau_2 = 0, 1, 2, 3$. By Lemmas 1 and 2, the autocorrelation of sequence a given by Construction B due to four different values of τ_2 can be given by the following.

Case 1. $\tau_2 = 0, 0 < \tau_1 < N$.

$$\begin{aligned}
 & R_a(\tau) \\
 = & R_a(4\tau_1) \\
 = & R_{s_1}(\tau_1) + R_{L^d(\overline{s_1})}(\tau_1) + R_{\overline{s_2}}(\tau_1) + R_{L^d(s_2)}(\tau_1) \\
 = & 4R_s(2\tau_1).
 \end{aligned}$$

Since $0 < \tau_1 < N, 2\tau_1 \neq 0 \pmod{N}, R_s(2\tau_1) = -1$. Then $R_a(\tau) = -4$, and it turns up $N - 1$ times altogether.

Case 2. $\tau_2 = 1, 0 \leq \tau_1 < N$.

$$\begin{aligned}
 & R_a(\tau) \\
 = & R_a(4\tau_1 + 1) \\
 = & R_{s_1, \overline{s_1}}(\tau_1 + d) + R_{\overline{s_1}, \overline{s_2}}(\tau_1 - d) \\
 & + R_{\overline{s_2}, s_2}(\tau_1 + d) + R_{s_2, s_1}(\tau_1 + 1 - d) \\
 = & -R_{s_1}(\tau_1 + d) + R_{s_1, s_2}(\tau_1 - d) \\
 & - R_{s_2}(\tau_1 + d) + R_{s_2, s_1}(\tau_1 + 1 - d) \\
 = & -R_s(2(\tau_1 + d)) + R_s(2(\tau_1 - d) + 1) \\
 & - R_s(2(\tau_1 + d)) + R_s(2(\tau_1 + 1 - d) - 1) \\
 = & -2R_s(2\tau_1 + 2d) + 2R_s(2\tau_1 - 2d + 1).
 \end{aligned}$$

- 1) If $\tau_1 = N - d$, $2\tau_1 + 2d = 0 \pmod{N}$, $2\tau_1 - 2d + 1 \neq 0 \pmod{N}$. Then $R_s(2\tau_1 + 2d) = N$, $R_s(2\tau_1 - 2d + 1) = -1$. So $R_a(\tau) = -2N - 2$;
- 2) If $\tau_1 = \frac{N+2d-1}{2}$, $2\tau_1 + 2d \neq 0 \pmod{N}$, $2\tau_1 - 2d + 1 = 0 \pmod{N}$. Then $R_s(2\tau_1 + 2d) = -1$, $R_s(2\tau_1 - 2d + 1) = N$. So $R_a(\tau) = 2 + 2N$;
- 3) If $\tau_1 \neq N - d$ and $\tau_1 \neq \frac{N+2d-1}{2}$, $2\tau_1 + 2d \neq 0 \pmod{N}$ and $2\tau_1 - 2d + 1 \neq 0 \pmod{N}$. Then $R_s(2\tau_1 + 2d) = R_s(2\tau_1 - 2d + 1) = -1$. So $R_a(\tau) = 0$.

In this case, $R_a(\tau) = -2N - 2$ turns up 1 time, $R_a(\tau) = 2N + 2$ turns up 1 time, and $R_a(\tau) = 0$ turns up $N - 2$ times.

Case 3. $\tau_2 = 2$, $0 \leq \tau_1 < N$.

$$\begin{aligned}
 R_a(\tau) &= R_a(4\tau_1 + 2) \\
 &= R_{s_1, \overline{s_2}}(\tau_1) + R_{\overline{s_1}, s_2}(\tau_1) \\
 &\quad + R_{\overline{s_2}, s_1}(\tau_1 + 1) + R_{s_2, \overline{s_1}}(\tau_1 + 1) \\
 &= -R_s(2\tau_1 + 1) - R_s(2\tau_1 + 1) \\
 &\quad - R_s(2(\tau_1 + 1) - 1) - R_s(2(\tau_1 + 1) - 1) \\
 &= -4R_s(2\tau_1 + 1).
 \end{aligned}$$

- 1) If $\tau_1 = \frac{N-1}{2}$, $2\tau_1 + 1 = 0 \pmod{N}$. Then $R_s(2\tau_1 + 1) = N$. So $R_a(\tau) = -4N$, and it turns up only 1 time;
- 2) If $\tau_1 \neq \frac{N-1}{2}$, $2\tau_1 + 1 \neq 0 \pmod{N}$. Then $R_s(2\tau_1 + 1) = -1$. So $R_a(\tau) = 4$, and it turns up $N - 1$ times.

Case 4. $\tau_2 = 3$, $0 \leq \tau_1 < N$.

$$\begin{aligned}
 R_a(\tau) &= R_a(4\tau_1 + 3) \\
 &= R_{s_1, s_2}(\tau_1 + d) + R_{\overline{s_1}, s_1}(\tau_1 + 1 - d) \\
 &\quad + R_{\overline{s_2}, \overline{s_1}}(\tau_1 + 1 + d) + R_{s_2, \overline{s_2}}(\tau_1 + 1 - d) \\
 &= R_s(2(\tau_1 + d) + 1) - R_s(2(\tau_1 + 1 - d)) \\
 &\quad + R_s(2(\tau_1 + 1 + d) - 1) - R_s(2(\tau_1 + 1 - d)) \\
 &= 2R_s(2\tau_1 + 2d + 1) - 2R_s(2\tau_1 - 2d + 2).
 \end{aligned}$$

- 1) If $\tau_1 = \frac{N-2d+1}{2}$, $2\tau_1 + 2d + 1 = 0 \pmod{N}$, $2\tau_1 - 2d + 2 \neq 0 \pmod{N}$. Then $R_s(2\tau_1 + 2d + 1) = N$, $R_s(2\tau_1 - 2d + 2) = -1$. So $R_a(\tau) = 2N + 2$;
- 2) If $\tau_1 = \frac{N+2d-2}{2}$, $2\tau_1 + 2d + 1 \neq 0 \pmod{N}$, $2\tau_1 - 2d + 2 = 0 \pmod{N}$. Then $R_s(2\tau_1 + 2d + 1) = -1$, $R_s(2\tau_1 - 2d + 2) = N$. So $R_a(\tau) = -2 - 2N$;
- 3) If $\tau_1 \neq \frac{N-2d+1}{2}$ and $\tau_1 \neq \frac{N+2d-2}{2}$. Then $2\tau_1 + 2d + 1 \neq 0 \pmod{N}$, $2\tau_1 - 2d + 2 \neq 0 \pmod{N}$. So $R_s(2\tau_1 + 2d + 1) = R_s(2\tau_1 - 2d + 2) = -1$, $R_a(\tau) = 0$.

In this case, $R_a(\tau) = 2N + 2$ turns up 1 time, $R_a(\tau) = -2N - 2$ turns up 1 time, and $R_a(\tau) = 0$ turns up $N - 2$ times altogether.

According to the above discussion about $R_a(\tau)$, we prove the following theorem.

Theorem 2. Let $0 \leq \tau < 4N$, and $d \neq \frac{N+1}{4}$. The autocorrelation function of the new sequence a defined by Equation (3) is:

$$R_a(\tau) = \begin{cases} 4N & 1 \text{ time,} \\ -4N & 1 \text{ time,} \\ -4 & N - 1 \text{ times,} \\ 4 & N - 1 \text{ times,} \\ 0 & 2N - 4 \text{ times,} \\ -2 - 2N & 2 \text{ times,} \\ 2 + 2N & 2 \text{ times.} \end{cases}$$

In a special case: $d = \frac{N+1}{4}$, similarly to Corollary 1, we can conclude the following corollary.

Corollary 2. Let $0 \leq \tau < 4N$, and $d = \frac{N+1}{4}$. The autocorrelation function of the new sequence a defined by Equation (3) is:

$$R_a(\tau) = \begin{cases} 4N & 1 \text{ time,} \\ -4N & 1 \text{ time,} \\ 4 & N - 1 \text{ times,} \\ -4 & N - 1 \text{ times,} \\ 0 & 2N \text{ times.} \end{cases}$$

Obviously, except for $-4N$, the values of out-of-phase autocorrelation of the sequence a are all contained in the set $\{0, -4, 4\}$. Therefore, the sequence a in Corollary 2 is a binary sequence with almost optimal autocorrelation magnitude.

Example 1. Let $N = 7$, $d = \frac{N+1}{4}$, and $s = (1, 1, 1, 0, 0, 1, 0)$, a m -sequence of period 7. The new sequence a of period $4N = 28$ defined by Construction A is

$$\begin{aligned}
 t &= (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, \\
 &\quad 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1).
 \end{aligned}$$

By calculation, the autocorrelation of a is

$$R_a(\tau) = \{28, 4, -4, 4, -4, 4, -4, -28, -4, 4, -4, 4, -4, 4, 28, 4, -4, 4, -4, 4, -4, -28, -4, 4, -4, 4, -4, 4\},$$

which is compatible with the result given by Corollary 1.

Example 2. Let $N = 7$, $d = \frac{N+1}{4}$, and $s = (1, 1, 1, 0, 0, 1, 0)$, a m -sequence of period 7. The new sequence a of period $4N = 28$ defined by Construction B is

$$\begin{aligned}
 t &= (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, \\
 &\quad 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0).
 \end{aligned}$$

By calculation, the autocorrelation of a is

$$R_a(\tau) = \{28, 0, 4, 0, -4, 0, 4, 0, -4, 0, 4, 0, -4, 0, -28, 0, -4, 0, 4, 0, -4, 0, 4, 0, -4, 0, 4, 0\},$$

which is compatible with the result given by Corollary 2.

4 Conclusion

In this paper, two new constructions of binary interleaved sequences of period $4N$ with low autocorrelation and balance property are proposed. From the autocorrelation distributions given by Corollaries 1 and 2, we can conclude that two new binary sequences defined in this paper have good autocorrelation properties. Especially, when $d = \frac{N+1}{4}$, the sequence a in Construction B is a binary sequence with almost optimal autocorrelation magnitude.

Ideally, good sequences combine the low autocorrelation properties with high linear complexity [3]. Furthermore, apart from balance property and autocorrelation property, the linear complexity of these sequences constructed in this paper remains to be solved.

Acknowledgments

The project is supported by the open fund of Fujian Provincial Key Laboratory of Network Security and Cryptology Research Fund (Fujian Normal University) (No.15002), the Natural Science Fund of Shandong Province (No.ZR2014FQ005), the National Natural Science Foundations of China (No.61170319) and the Fundamental Research Funds for the Central Universities (No.11CX04056A, 15CX08011A, 15CX05060A).

References

- [1] K. T. Arasu, C. Ding, T. Hellesteth, P. V. Kumar, and H. M. Martinsen, "Almost difference sets and their sequences with optimal autocorrelation," *IEEE Transactions on Information Theory*, vol. 47, no. 7, pp. 2934–2943, 2001.
- [2] C. Ding, T. Hellesteth, and K. Y. Lam, "Several classes of binary sequences with three-level autocorrelation," *IEEE Transactions on Information Theory*, vol. 45, no. 7, pp. 2606–2612, 1999.
- [3] V. Edemskiy and A. Ivanov, "Linear complexity of quaternary sequences of length with low autocorrelation," *Journal of Computational and Applied Mathematics*, vol. 259, Part B, pp. 555–560, 2014.
- [4] A. D. Elbayoumy and S. J. Shepherd, "Stream or block cipher for securing voip?," *International Journal of Network Security*, vol. 5, no. 2, pp. 128–133, 2007.
- [5] G. Gong, "Theory and applications of q-ary interleaved sequences," *IEEE Transactions on Information Theory*, vol. 41, no. 20, pp. 400–411, 1995.
- [6] P. Ke and F. Lin, "Constructions of binary sequences with optimal autocorrelation value," *IEEE Transactions on Information Theory*, vol. 46, no. 20, pp. 1381–1382, 2010.
- [7] X. Ma, T. Yan, D. Zhang, and Y. Liu, "Linear complexity of some binary interleaved sequences of period $4N$," *International Journal of Network Security*, vol. 18, no. 2, pp. 244–249, 2016.

- [8] X. Tang and G. Gong, "New constructions of binary sequences with optimal autocorrelation value/magnitude," *IEEE Transactions on Information Theory*, vol. 56, no. 3, pp. 1278–1286, 2010.
- [9] H. Xiong, L. Qu, and C. Li, "2-adic complexity of binary sequences with interleaved structure," *Finite Fields and Their Applications*, vol. 33, pp. 14–28, 2015.
- [10] T. Yan, "New binary sequences of period pq with low values of correlation and large linear complexity," *International Journal of Network Security*, vol. 10, no. 3, pp. 185–189, 2008.
- [11] T. Yan and G. Gong, "Some notes on constructions of binary sequences with optimal autocorrelation," 2014. (<http://arxiv.org/abs/1411.4340>)
- [12] X. Zhang, Q. Wen, and J. Qin, "Constructions of sequences with almost optimal autocorrelation magnitude," *Journal of Electronics and Information Technology*, vol. 33, no. 8, pp. 1908–1912, 2011.

Biography

Ruifang Meng was born in 1991 in Shandong Province of China. She was graduated from China University of Petroleum. She will study for a postgraduate degree at China University of Petroleum in 2015. And her tutor is Tongjiang YAN. Email:mmrrfang@163.com

Tongjiang Yan was born in 1973 in Shandong Province of China. He was graduated from the Department of Mathematics, Huaibei Coal-industry Teachers College, China, in 1996. In 1999, he received the M.S. degree in mathematics from the Northeast Normal University, Lanzhou, China. In 2007, he received the Ph.D. degree in Xidian University. He is now a professor of China University of Petroleum. His research interests include cryptography and algebra. Email:yantoji@163.com

A New Level 3 Trust Hierarchal Certificateless Public Key Cryptography Scheme in the Random Oracle Model

Mohammed Hassouna¹, Bazara Barry² and Eihab Bashier²

(Corresponding author: Eihab Bashier)

Faculty of Computer Studies, National Ribat University, P.O. Box: 55, Khartoum, Sudan¹

Faculty of Mathematical Sciences, University of Khartoum, P.O. Box: 321, Khartoum, Sudan²

(Email: eihabbashier@gmail.com)

(Received Feb. 21, 2016; revised and accepted May 6 & July 19, 2016)

Abstract

Despite the fact that the traditional public key infrastructure provides Level 3 trusted authority, but its two major problems of scalability and certificate management raised the need to an alternative security infrastructure. That motivated the appearance of new technologies to replace the traditional PKI, such as the Identity based encryption, the certificateless encryption, etc. But all those new technologies are yet immature and could not introduce a trust level more than Level 2, except few trials at the level of the authority. This paper aims at introducing an integrated hierarchal certificateless scheme with a Level 3 trust authority. This is done through merging the traditional PKI hierarchy and the certificateless technology in one scheme. The new scheme employs the X509 certificate format and is free of the scalability and certificate management problems of the PKI. We also describe how our new hierarchal certificateless PKC, can be integrated with a traditional PKI through a bridge model.

Keywords: Certificateless cryptography, public key infrastructure, random oracle model, security services, trust levels

1 Introduction

Public Key Infrastructure (PKI) is a complete system to manage the public keys in any public key cryptography-based application using the concept of digital certificates. The PKI provides authentication of system users by allowing some trusted third-party to sign the public key of any entity in the system. In the context of PKI, any entity in the system can verify the authentication of any other entity by verifying its signed certificate using the trusted third-party's public key. In this way, any other cryptographic services (like confidentiality and non-repudiation) can be achieved and implemented.

Furthermore, PKI has some well established trust models that meet the organization flowchart and requirements. Examples of these trust models are hierarchal and bridge models. When the system scale gets large, the number of signed digital certificates also gets large. Therefore the overhead of the management of these certificate increases. Moreover, other issues like public key revocation and its related notification methods are raised. However, in spite of the maturity of the PKI and its wide applications and usage, the PKI has main two challenges. These challenges are scalability and certificate management [1, 10].

Some other paradigms of public key cryptography are introduced to overcome the PKI challenges and simplifying the key management. Identity-based Public Key Cryptography (ID-PKC) (which was invented by Boneh and Franklin [2]) and Certificateless Public Key Cryptography (CL-PKC) (invented in 2003 by Al-Ryami and Paterson [1]) are such examples to these paradigms. The CL-PKC addressed the key-escrow problem of the ID-PKC [1] and provided a lightweight infrastructure for managing the public keys of the users in the system without using the digital certificates. Since the original Al-Ryami and Paterson scheme [1], many certificateless encryption schemes [3, 11, 13], certificateless digital signature schemes [14, 15, 17, 18] and certificateless key agreement protocols [5, 12, 16] were appeared in the literature.

However, the existence of a trusted third party (or trusted authorities) is a common feature among all the public key infrastructure models. These trusted authorities are the certificate authority (CA) in the traditional PKI, the Key Generation Center (KGC) in the ID-PKC and CL-PKC in the certificateless infrastructure. The trusted third party in a public key infrastructure schemes is the heart of the whole security system. It controls the system components and parameters, publishes the system parameters and the users public keys, and in addition to that it might play a partial or a full role in generating

the pairs of public and private keys of the users. If this third party is malicious, then the security of the whole infrastructure could be compromised. For this, Girualt [6] defined three levels of trust: At Level 1 trust, the authority knows (or can easily compute) users' secret keys and therefore, can impersonate any user at any time without being detected (the KGC of the ID-PKC). At Level 2 trust, the authority does not know users' secret keys, but it can still impersonate a user by generating false guarantees (CL-PKC). At Level 3 the authority cannot compute users' secret keys, and if it does so, it can be proven that it generates false guarantees (The CA in the traditional PKI).

In 2013 Hassouna et al. [7] proposed an integrated Certificateless public key infrastructure model (CL-PKI). In their model, a different method for generating entity key pair has been introduced. Furthermore, Hassouna et al. [7] incorporated a different binding technique to link the entity's identity with its corresponding keys to ensure the uniqueness of the key pair. The direct security and management advantages of using this method of key generation are two-factor private key authentication, private key portability, private key recovery and private key archiving [7]. Moreover, Hassouna et al. extended their CL-PKI model by proposing a new security model for certificateless digital signature schemes. Then, they proposed a strong and efficient provable secure certificateless digital signature scheme [8] in the Random Oracle Model (ROM) without stating its security proof. Recently, Hassouna et al. [9] stated the complete security proof of the digital signature scheme in the random oracle model [8].

In this paper, we propose a Hierarchal Certificateless Public Key Cryptography Scheme (HCL-PKC) and then use it to construct a Hybrid PKI/CL-PKI scheme. These two schemes are introduced in the context of Hassouna et al.'s CL-PKI model, hence they enjoy the security properties and key management features of Hassouna et al.'s [7] model.

The rest of this paper is organized as follows. We state Hassouna et al.'s [7] CL-PKI model in Section 2. Hassouna et al.'s [8] digital signature scheme is given in Section 3. In Section 4, we introduce the proposed Hierarchal Certificateless Public Key Cryptography Scheme (HCL-PKC). In Section 5, we give the Hybrid PKI/CL-PKI scheme. Finally, Section 6 concludes the paper.

2 Hassouna et al.'s Certificateless Public Key Infrastructure Model (CL-PKI)

As stated in [7]: to make the CL-PKC schemes suitable for practical applications, there is a need for some sort of infrastructure as the traditional PKI. Therefore, Hassouna et al. [7] proposed a CL-PKI model with three components: Registration Authority (RA), Key Generation Center (KGC) and Public Directory (PD).

The components of the proposed CL-PKI and their functions are as follows:

- 1) **The Registration Authority (RA):** The registration authority plays the same role as the registration authority of the traditional PKI. The user might interact with this authority and provides proofs of his personal information like names, address, national ID number and email address. After the RA verifies the information of the user, it gives the user a unique random generated password for latter authentication purposes, in addition to the system parameters, generated by the KGC server in a token or any electronic media.
- 2) **The Key Generation Center (KGC):** The KGC is responsible of generating its master secret and the system parameters. It has to keep its master secret in a secure storage and publish the system parameters in a public directory. The KGC also has a database that holds the user identities with their password hashed by any strong cryptographic hash function like MD5 or SHA-1.
- 3) **The KGC's Public Directory (PD):** The public directory is responsible of storing the KGCs' public parameters, users identities, users partial private keys, users public key and other user parameters. It is controlled and updated by the KGC. The contents of the PD are available for only the authenticated users, who do not have the right to write in it. The typical format of the public directory records are given in Figure 1 and Figure 2, respectively.

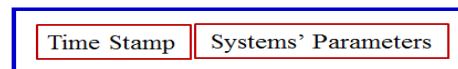


Figure 1: Systems' parameters record

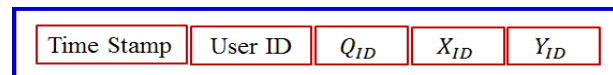


Figure 2: Contents of the public directory of a user

Typically the RA has an offline connection with the KGC. When the KGC generates the user's password at the registration time, the RA passes it to the user without knowing it.

In [7], Hassouna et al. introduced several methods of authentication between the user and the KGC/PD. The complete description of the model is as following:

- **Setup (running by the KGC):** The KGC chooses a secret parameter k to generate G_1, G_2, P, e ; where G_1 and G_2 are two groups of a prime order q , P is

a generator of G_1 and $e : G_1 \times G_1 \rightarrow G_2$ is a bilinear map. The KGC generates a random system's master key $s \in \mathbb{Z}_q^*$ and computes the system public key $P_{pub} = sP$. Then, the KGC chooses a cryptographic hash functions H_1 and H_2 , where $H_1 : \{0,1\}^* \times G_1 \rightarrow G_1$ and $H_2 : \{0,1\}^* \rightarrow \{0,1\}^n$. Finally, the KGC publishes the system parameters $params = \langle G_1, G_2, e, P, P_{pub}, H_1, H_2, n \rangle$, and keeps the secret master-key safe.

- **Set-Secret-Value (running by the user):** A user m with an identity ID_m downloads the system parameters. He/She then generates two random secret values $x_m, x'_m \in \mathbb{Z}_q^*$. Then, it computes $X_m = x'_m P$ and sends X_m to the KGC. To provide two factor of authentication and protection for the user's private key against the device theft or compromise, the proposed scheme enforces the user to choose a strong password $pass$. The client device uses the hash function H_2 to generate $z_m = H_2(pass)$ and multiplies the base point P by the hashed password to get $z_m P$. The hash function H_2 must be capable to preserve the large size of the hashed value z_m to prevent the brute-force attack on the point $z_m P$. It then uses the hashed value z_m as key along with the MAC function to encrypt the secret value x_m as $MAC_{z_m}(x_m)$ and sends a copy to the KGC's public directory to be stored together with the point $z_m P$ locally. It is worthy to notice that there is no need to store the password $pass$ or its hash value z_m .
- **Partial-Private-Key-Extract (running by the KGC):** When the KGC receives X_m from a user m with an identity ID_m , the KGC first computes $Q_m = H_1(ID_m || X_m)$, then it generates the partial private key of user m as $D_m = sQ_m$. User m can verify the correctness of his/her partial private key D_m , through testing whether $e(D_m, P) = e(Q_m, P_0)$.
- **Set-Public-Key (running by the user):** The user m whose identity is ID_m computes $Q_m = H_1(ID_m || X_m)$, $Y_m = x'_m Q_m$ and sets $\langle X_m, Y_m \rangle$ as his/her long-term public key P_m . Finally, user m sends Y_m to the KGC.
- **Set-Private-Key (running by the user):** Every time a user wants to calculate and use his/her full private key, he/she enters his/her password, the system hashes it as z'_m , calculates $z'_m P$ and compares it with the stored point $z_m P$. If the comparison results in a match, then the password is correct and the user is authenticated. Then, the user uses (z_m) as a key to decrypt the stored $MAC_{z_m}(x_m)$, and uses the extracted value x_m to calculate the full private key by $(x_m + z_m)D_m$. In case of mismatch, the system aborts the process. We must note here that the private key is never stored on the client and it will be deleted after every usage.

Further issues such as the users' authentication at the first time, updates of system's parameters and users' passwords, generation of public and private key pairs, private key recovery; portability; archiving and public key revocation are discussed in details in [7].

3 Hassouna et al.'s Certificateless Digital Signature Scheme

In this section, we provide details on the certificateless digital signature scheme that was proposed by Hassouna et al. and its functionality [8].

- **Setup (running by the KGC):** The KGC chooses a secret parameter k to generate G_1, G_2, P, e where G_1 and G_2 are two groups of a prime order q , P is a generator of G_1 and $e : G_1 \times G_1 \rightarrow G_2$ is a bilinear map. The KGC randomly generates the system's master key $s \in \mathbb{Z}_q^*$ and computes the system public key $P_{pub} = sP$. Then, the KGC chooses cryptographic hash functions H_1 and H_2 , where $H_1 : \{0,1\}^* \rightarrow G_1$ (Map-to-Point hash function), and $H_2 : \{0,1\}^n \rightarrow \mathbb{Z}_q^*$ (any cryptographic hash function like MD5 or SHA family). Finally, the KGC publishes the system parameters $params = \langle G_1, G_2, e, P, P_{pub}, H_1, H_2, n \rangle$, while the secret master-key is saved and secured by the KGC.
- **Set-Secret-Value (running by the user):** A user m with an identity ID_m downloads the system parameters, generates two random secret values $x_m, x'_m \in \mathbb{Z}_q^*$. Then, user m computes $X_m = x'_m P$ and sends X_m to the KGC. The proposed scheme enforces the user to choose a strong password $pass$, the system at the client side hashes the password to be $z_m = H_2(pass)$, multiplies the base point P by the hashed password to be $z_m P$, uses the hashed value z_m as key to encrypt the secret value x_m and generates the Password-based Encryption Code (PEC) as $PEC_{z_m}(x_m)$, sends a copy of it to the KGC's public directory and stores it along with the point $z_m P$ locally.
- **Partial-Private-Key-Extract (running by the KGC):** On receiving X_m computed by user m with identity ID_m , the KGC first computes $Q_m = H_1(ID_m)$, then it generates the partial private key of user m as $D_m = sQ_m$.
- **Set-Public-Key (running by the user):** The user m with identity ID_m computes $Q_m = H_1(ID_m)$, $Y_m = x'_m Q_m$ and sets $\langle X_m, Y_m \rangle$ as his/her long-term public key P_m . Finally, user m sends Y_m to the KGC.
- **Set-Private-Key:** User m 's private key is $S_m = (x_m + z_m)D_m = (x_m + z_m)sQ_m = (x_m + z_m)sH_1(ID_m)$. Also, the user generates the secret term $Z_m = x_m P$.

- **Sign:** The user generates the signature of the message M using his secret terms $\{x_m, Z_m\}$ as follows:

- 1) The signer generates a big random integer $a \in G_2^*$.
- 2) The signer calculates $MP_m = H_1(m) \in G_1^*$.
- 3) The signer calculates $MP_{1m} = ax_m MP_m \in G_1^*$.
- 4) The signer calculates $s_m = e(MP_m, Z_m)^{ax'_m} = e(MP_m, P)^{ax_m x'_m}$.
- 5) The signer sends $\sigma = (m, MP_{1m}, s_m)$ as the signature.

- **Verify:** After receiving the signature $\sigma = (m, MP_{1m}, s_m)$, the verifier uses the public key $\langle X_m, Y_m \rangle$ of user m to verify the signature as follows:

- 1) The verifier checks whether $e(X_m, Q_m) = e(Y_m, P)$. If it holds then user m 's public key is authenticated, otherwise the signature is rejected.
- 2) The verifier calculates $MP'_m = H_1(m) \in G_1^*$.
- 3) If $MP_{1m} = MP'_m$ or $s_m = e(H_1(m), X_m)$ then the verifier rejects the signature. Otherwise, the verifier calculates $r_m = e(MP_{1m}, X_m)$.
- 4) The verifier accepts the signature iff $r_m = s_m$, otherwise he/she rejects the signature.

3.1 Hassouna et al.'s Security Model

In Hassouna et al. [8] two types of adversaries were considered: Type I and Type II adversaries according to the term Z_m as follows:

- 1) **Type I Adversary A_I :** This adversary is allowed to replace the term Z_m by a valid value of his choice, but is not allowed to replace users' public keys and has not access to the master secret key s .
- 2) **Type II Adversary A_{II} :** This adversary has an access to the master secret key s , and is allowed to replace users public keys with valid values of his choice, but is not allowed to replace the term Z_m .

Type I adversary represents an outsider attacker and type II attacker is a malicious KGC. Two games are defined as follows.

- **Game I.** The first game is performed between a challenger C and a Type I adversary A_I as follows.

- 1) Setup. The challenger C runs Setup algorithm and generates a master secret key msk and public system parameters $params$. C gives $params$ to A_I , while keeping msk secret.
- 2) Queries. A_I may adaptively issue the following queries to C .

- Partial private key queries: Upon receiving a partial private key query for an identity ID , C returns the partial private key with respect to identity ID to A_I .
- Public key queries: Given an identity ID , C returns the corresponding public key terms $\langle X_A, Y_A \rangle$ to A_I .
- Replace public key: Given an identity ID with a pair of values (x_{ID}^1, pk_{ID}^1) which are chosen by A_I , C updates the user ID original secret/public key (x'_{ID}, pk_{ID}) to the new (x_{ID}^1, pk_{ID}^1) .
- Z – key Extraction queries: This is a new oracle in this security model, given an identity ID , C returns the corresponding Z – key value Z_{ID} .
- Replace Z – key: This is a new oracle in this security model which on input (ID, x_{ID}^1, Z_{ID}^1) , C replaces the user ID original term (x_{ID}, Z_{ID}) by (x_{ID}^1, Z_{ID}^1) .
- Private key queries. Upon receiving a private key query for an identity ID , C returns the corresponding private key sk_{ID} to A_I .
- Sign queries: Proceeding adaptively, A_I can request signatures on any messages m with respect to an identity ID . C computes signature, and returns to A_I .

- 3) Forgery. Eventually, A_I outputs a certificateless signature σ^* on message m^* corresponding to public key pk_{ID^*} for an identity ID^* . A_I wins the game if $\text{Verify}(params, ID^*, pk_{ID^*}, m^*, \sigma^*) = 1$ and the following conditions hold:

- A_I has never been queried Partial private key oracle on ID^* .
- A_I never replaced the user ID^* 's public key.
- A_I has never been queried Private key oracle on ID^* .
- A_I has never been queried Sign oracle on (ID^*, m^*) .

The success probability of A_I is defined as the probability that it wins in game I.

- **Game II.** This game is performed between a challenger C and a Type II adversary A_{II} as follows.

- 1) Setup. The challenger C runs A_{II} on k and a special Setup, and returns a master secret key msk and public system parameters $params$ to A_{II} .
- 2) Queries. In this phase, A_{II} can adaptively access the Private key oracle, Public key oracle, Replace public key oracle, Z – key oracle, Replace Z – key oracle and Sign oracle, which are the same as that in Game I.

- 3) Forgery. A_{II} outputs a certificateless signature σ^* on message m^* corresponding to public key pk_{ID^*} for an identity ID^* . A_{II} wins the game if $\text{Verify}(params, ID^*, pk_{ID^*}, m^*, \sigma^*) = 1$ and the following conditions hold:
- A_{II} has never been queried Private key oracle on ID^* .
 - A_{II} has never been queried Replace Z – key oracle on ID^* .
 - A_{II} has never been queried Signature oracle on (ID^*, m^*) .

The success probability of A_{II} is defined as the probability that it wins in Game II.

Accordingly, the security definitions of any certificateless digital signature scheme in the Random Oracle Model (ROM) can be given as follows.

Definition 1. A certificateless signature scheme is $(t, q_H, q_e, q_z, q_{sk}, q_{pk}, q_s, \epsilon)$ -existentially unforgeable against Type I adversary under adaptively chosen message attacks if no t -time adversary A_I , making at most q_H to the random oracles, q_e partial private key queries, q_z to the Z – key queries, q_{sk} private key queries, q_{pk} public key queries and q_s signature queries, have a success probability at least ϵ in Game I.

Definition 2. A certificateless signature scheme is $(t, q_H, q_z, q_{sk}, q_{pk}, q_s, \epsilon)$ -existentially unforgeable against Type II adversary under adaptively chosen message attacks if no t -time adversary A_{II} , making at most q_H to the random oracles, q_z to the Z – key queries, q_{sk} private key queries, q_{pk} public key queries and q_s signature queries, have a success probability at least ϵ in Game II.

Definition 3. A certificateless signature scheme is existentially unforgeable under adaptively chosen message attack (EUF-CMA), if the success probability of any polynomially bounded adversary in the above two games is negligible.

Theorem 1. Hassouna et al.'s [8] digital signature scheme is secure against existential forgery under adaptively chosen message attacks in the random oracle model with the assumptions that CDHP (Computation Diffie-Hellman Problem) and BDHP (Bilinear Diffie-Hellman Problem) in G_1 are intractable.

The full proof of Theorem 1 in the random oracle model is stated in [9].

4 The Proposed Hierarchal Certificateless Public Key Cryptography Scheme (HCL-PKC)

Al-Ryami and Paterson introduced a Hierarchal Certificateless Encryption scheme (HCL-PKE) in their original

paper [1]. Their HCL-PKE did not provide a trust Level 3 at the sense of Girault's definition [6]. Therefore, it was not acceptable as alternative to the traditional hierarchal PKI. In this section, we use Hassouna et al.'s [8] signature scheme as assistant technique to propose a new Hierarchal Certificateless Cryptography scheme (HCL-PKC) which is based on Hassouna et al.'s [7] CL-PKI model. The proposed HCL-PKC (See Figure 3) is straightforward and could provide a trust Level 3.

- **Root KGC Setup.** The KGC chooses a secret parameter k to generate G_1, G_2, P, e , where G_1 (additive group) and G_2 (multiplicative group) are two groups of a large prime order q , P is a generator of G_1 and $e : G_1 \times G_1 \rightarrow G_2$ is a bilinear map. The KGC randomly generates the system's master keys $x_0, x'_0 \in \mathbb{Z}_q^*$ and computes the system public key $X_0 = x'_0 P$ and the private key term $Z_0 = x_0 P$. Then, the KGC chooses cryptographic hash functions H_1 and H_2 , where $H_1 : \{0, 1\}^* \times G_1 \rightarrow G_1$ and $H_2 : \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$. Finally, the KGC publishes the system parameters $params = \langle G_1, G_2, e, P, X_0, H_1, H_2, n \rangle$, while the secret master-keys are saved and secured by the KGC.

- **Set-Secret-Value.** The user at level t with identity ID_t , where ID_0 is the identity of the root KGC downloads the system parameters $params$, generates two random secret numbers $x_t, x'_t \in G_2^*$. As in the signature scheme, we enforce the user to choose a strong password $pass$, the system at the client side hashes the password to be $z_m = H_2(pass)$, multiplies the base point P by the hashed password to be $z_m P$, uses the hashed value z_m as a key to encrypt the secret value x_m and generates the Password-based Encryption Code (PEC) as $PEC_{z_m}(x_m)$, sends copy of it to the KGC's public directory and stores copy of it along with the point $z_m P$ locally.

- **Set-Public-Key.** The user at level t calculates its public key (X_t, Y_t) as $X_t = x'_t P$ and $Y_t = x'_t Q_t$ where $Q_t = H_1(ID_t, X_t)$. Then, the user sends X_t to the previous user in the hierarchy ID_{t-1} .

- **Extract-Partial-Private-Key.** The user at level $t - 1$ accepts the request of the users at level t (the request contains the terms Q_t and X_t) and calculates their partial private key D_t as $D_t = x_{t-1} Q_t$. Furthermore, the user at level $t - 1$ signs the public term X_t of the user at level t using the proposed CL-SS scheme with the terms Z_{t-1} and the per-signature random number a_{t-1} and creates the signature as (X_t, MP_{1t}, s_t) and puts this signature along with the rest of user's public terms into the public directory $\{ID_t, Q_t, X_t, Y_t, MP_{1t}, s_t\}$.

- **Set-Private-Key.** Every time the user at level t needs to calculate and use his/her full private key, he/she enters his/her password, the system hashes it as z'_m , calculates $z'_m P$ and compares it with stored

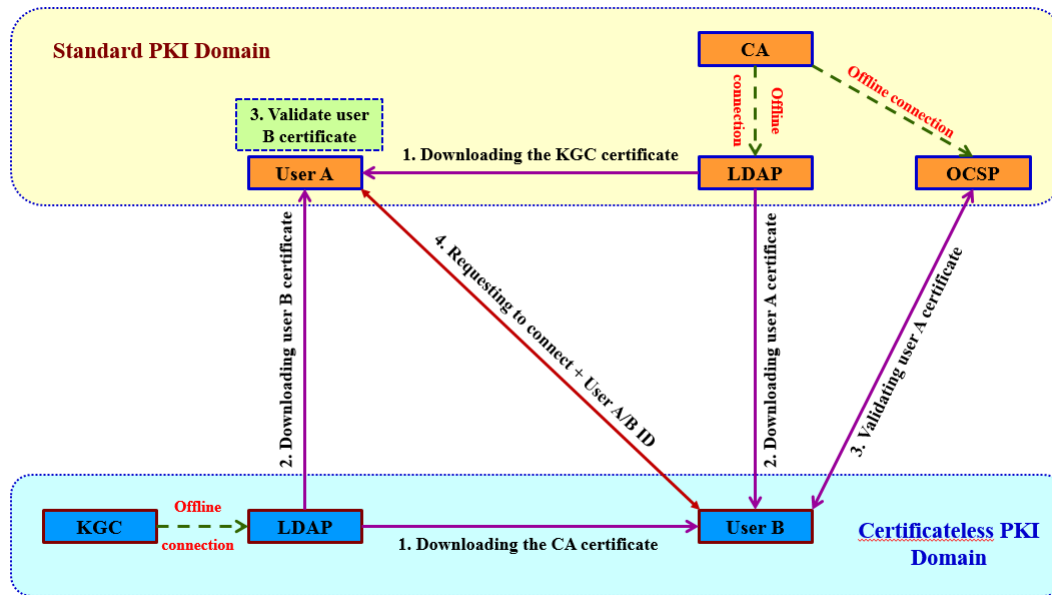


Figure 3: The proposed HCL-PKC model

point $z_m P$. If the comparison result in a match, then the password is correct and the user is authenticated. The user then uses (z_t) as a key to decrypt the stored encrypted value x_t , and after that uses the extracted value x_t to calculate the full private key by $(x_t + z_t)D_t$ and the term $Z_t = x_t P$. In case of a mismatch, the system aborts the process.

Every user in the system has a unique record in the Public Directory (PD) which contains the information $\{ID_t, Q_t, X_t, Y_t, PEC_{z_t}(x_t), MP_{1t}, s_t\}$. We can think about the user's record as X.509 certificate. Hence, the interoperability between the traditional PKI system and this proposed HCL-PKC scheme will be easy because the two systems will be compatible.

Furthermore, the proposed HCL-PKC scheme provides a new mechanism to authenticate the user's public key and provides a trust Level 3 as same as the hierarchical PKI does. That means if the user's public key has been replaced, then no one excepts the user's intermediate KGC can do that. This because no one can replace the signature term by a valid one except the user's intermediate KGC. Therefore, the user can detect and determine the entity that has replaced his/her public key.

Moreover, the proposed HCL-PKC scheme inherits an attractive feature from CL-PKI model that is introduced by Hassouna et al. [7], which is stated as: Even if the KGC or the intermediate KGC replaces (temporarily) the public key (as in the traditional PKI system) in order to compromise that user for decryption or signature forgery, this attack will fail because the user's private key is calculated from another different secret value. So, replacing the user's public key is not enough for compromising that user. Therefore, the separation of public/private key generation provides strong security feature.

5 Hybrid PKI/CL-PKI Scheme

Suppose we have organization with two domains, the first domain utilizes the traditional PKI with one CA and one LDAP server for trust distribution. The other domain has the Hassouna et al.'s [7] CL-PKI which has the same structure as the traditional PKI, i.e it uses X.509 certificate format to load the certificateless user's information with the signature as Hassouna et al.'s [8] one. Then, the two domains can operate smoothly as follows:

- **Bridge Model:** Bridge trust model can be used between the CA of the PKI and the KGC of the CL-PKI. Then, the CA generates and signs the X.509 certificate (using a standard PKI and ECC-based signature scheme like ECDSA) to the KGC that includes the KGC's public parameters. Also, the KGC generates and signs the X.509 certificate (using the Hassouna et al.'s signature scheme) to the CA that includes the CA's public key. The CA stores the KGC's certificate into its local LDAP server and also the KGC stores the CA's certificate into its local LDAP server. Since the recent versions of the PKI-enabled protocols like TLS v1.2 protocol [4] have become supportive to the Elliptic Curve Cryptosystems like ECDSA signature scheme and ECDH key exchange protocol as Hassouna et al.'s CL-PKI-enabled protocols did, then it is possible to agree on using the ECDH for key exchange protocol to generate the symmetric key. The other parameters can be agreed on at the handshake phase of the transaction. Note that the users at the PKI domain needs to be equipped with the pairing algorithm in order to do the signature generation/verification.

- **PKI Domain's User:** User A in the PKI domain when encrypting/signing a message to user B in the CL-PKI domain, he/she needs to do as follows:

- 1) User A first request B's certificate either directly from user B or from the CL-PKI's LDAP server.
- 2) After the user A gets user B's certificate, downloads the KGC's certificate from his/her local LDAP server. Then, he/she uses CA's public key to validate the KGC's certificate. If it is not valid, then user A rejects and aborts the transaction.
- 3) If the KGC's certificate is valid, then user A extracts KGC's public key and uses it to verify B's certificate by verifying the signature on the user B's certificate using the Hassouna et al. signature scheme.
- 4) User A also can verify the expiry/revocation of the user B's certificate using either the CRL mechanism or the OSCP protocol.
- 5) After user A authenticates user B, then users A and B can start the handshake protocol to agree on the key size, generate per-session symmetric encryption key using ECDH protocol, agree on the encryption algorithm, hash function and the signature algorithm (ECDSA for PKI users and the Hassouna et al.'s one for CL-PKI users).

- **CL-PKI Domain's User:** User B in the CL-PKI domain when encrypting/signing a message to user A in the PKI domain, he/she does the following:

- 1) User B first requests A's certificate either directly from user A or from the PKI's LDAP server.
- 2) After user B gets user A's certificate, downloads the CA's certificate from his/her local LDAP server, then he/she uses KGC's certificate to authenticate the CA's certificate (using Hassouna et al.'s signature scheme). If it is not valid, then user B rejects and aborts the transaction.
- 3) If the CA's certificate is valid, then user B extracts CA's public key and uses it to verify B's certificate (prefer to use ECDSA algorithm).
- 4) User B also can verify the expiry/revocation of the user A's certificate using either the CRL mechanism or the OSCP protocol as in the traditional PKI system.
- 5) After user B authenticates user A, then users A and B can start the handshake protocol to agree on the encryption key size, generate per-session symmetric encryption key using ECDH protocol, agree on the encryption algorithm, hash function and the signature scheme (ECDSA for PKI users and Hassouna et al.'s one for CL-PKI users).

6 Conclusions and Remarks

This paper used the Hassouna et al.[8] signature scheme and proposed a trust Level 3 hierarchal certificateless public key cryptography scheme. The proposed hierarchal scheme is based on Hassouna et al.'s [7] CL-PKI model. Therefore, it enjoys the same security features that CL-PKI has, along with the interesting trust Level 3 satisfaction property. The paper also proposed a new Hybrid PKI/CL-PKI scheme that provides interoperability model between traditional PKI and CL-PKI systems in one organization under the X.509 certificate format.

References

- [1] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 452–473, 2003.
- [2] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology (CRYPTO'01)*, LNCS 2139, pp. 213–229, Springer-Verlag, 2001.
- [3] A. W. Dent, B. Libert, and K. G. Paterson, "Certificateless encryption schemes strongly secure in the standard model," in *Public Key Cryptography*, pp. 344–359, 2008.
- [4] T. Dierks and E. Rescorla, *The Transport Layer Security (TLS) Protocol*, IETF RFC 4346, 2006.
- [5] N. A. Farah, M. Hassouna, M. Hashim, E. B. M. Bashier, "A secure and efficient key agreement protocol based on certificateless cryptography," *University of Khartoum*, 2016. <http://khartoumspace.uofk.edu/handle/123456789/21502>
- [6] M. Girault, "Self-certified public keys," in *Advances in Cryptology (EUROCRYPT'91)*, LNCS 547, pp. 490–497, Springer, 1992.
- [7] M. Hassouna, B. Barri, N. Mohamed, and E. Bashier, "An integrated public key infrastructure model based on certificateless cryptography," *International Journal of Computer Science and Information Security*, vol. 11, no. 11, pp. 1–10, 2013.
- [8] M. Hassouna, E. Bashier, and B. Barry, "A short certificateless digital signature scheme," in *International Conference of Digital Information Processing, Data Mining and Wireless Communications*, pp. 120–127, 2015.
- [9] M. Hassouna, E. Bashier, and B. Barry, "A strongly secure certificateless digital signature scheme in the random oracle model," *International Journal of Network Security*, vol. 18, no. 5, pp. 938–945, 2016.
- [10] A. V. N. Krishna, A. H. Narayana, K. M. Vani, "Window method based cubic spline curve public key cryptography," *International Journal of Electronics and Information Engineering*, vol. 4, no. 2, pp. 94–102, 2016.

- [11] J. K. Liu, M. H. Au, and W. Susilo, "Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model," in *Proceedings of the 2nd ACM symposium on Information, computer and communications security*, pp. 273–283, 2007.
- [12] R. Mokhtarnameh, S. Ho, and N. Muthuvelu, "An enhanced certificateless authenticated key agreement protocol," in *Proceedings of the 13th International Conference on Advanced Communication Technology*, pp. 802–806, 2011.
- [13] S. S. Vivek, S. S. D. Selvi, C. P. Rangan, "CCA2 secure certificateless encryption schemes based on RSA," in *Proceedings of the International Conference on Security and Cryptography (SECRYPT'10)*, pp. 208–217, 2011.
- [14] C. Wang, D Long, and Y. Tang, "An efficient certificateless signature from pairing," *International Journal of Network Security*, vol. 8, no. 1, pp. 96–100, 2009.
- [15] H. Xiong, Z. Qin, and F. Li, "An improved certificateless signature scheme secure in the standard model," *Fundamenta Informaticae*, vol. 88, no. 1-2, pp. 193–206, 2008.
- [16] H. Yang, Y. Zhang, and Y. Zhou, "An improved certificateless authenticated key agreement protocol," in *IEEE 14th International Conference on Communication Technology (ICCT'12)*, pp. 26–30, 2012.
- [17] Y. Yuan and C. Wang, "A secure certificateless signature scheme in the standard model," *Journal of Computational Information Systems*, vol. 9, no. 11, pp. 4353–4362, 2013.
- [18] L. Zhang and F Zhang, "A new provably secure certificateless signature scheme," in *IEEE International Conference on Communications*, pp. 1685–1689, 2008.

Biography

Mohammed Alfateh Hassouna is Assistant Professor at Department of Computer Science - Faculty of Computer Studies - The National Ribat University - Sudan. He was gain his PhD in cryptography from the University of Khartoum - Sudan. Currently he is working as ICT Manger at the National Ribat University. He has many published papers in several international journals and conferences related to the information security and cryptography. (Email: m.fateh@ribat.edu.sd)

Bazara Barry is an associate professor at the department of Computer Science - University of Khartoum and formerly the head of the same department. He was director of research at the Faculty of Mathematical Sciences. Bazara is a reviewer and TPC head/member of many international journals/conferences and a member of the IEEE. He has won several best paper and research awards at the international level. (Email: baazobarry@hotmail.com)

Eihab Bashier obtained his PhD in 2009 from the University of the Western Cape in South Africa. He is an associate professor of applied mathematics at University of Khartoum, since 2013 and recently, he joined the department of Mathematics, Physics and Statistics of Qatar University. The research interests of Dr. Bashier are mainly in numerical methods for differential equations with applications to biology and in information and computer security. In 2011, Dr. Bashier won the African Union and the Third World Academy of Science (AU-TWAS) young scientists national award in basic sciences, technology and Innovation. Dr. Bashier is a reviewer for many international journals and an IEEE member. (Email: eihabbashier@gmail.com)

A Secured Access Control Technique for Cloud Computing Environment Using Attribute Based Hierarchical Structure and Token Granting System

Balamurugan Balusamy¹, P. Venkata Krishna², G. S. Tamizh Arasi³, and Victor Chang⁴

(Corresponding author: Balamurugan Balusamy)

School of Information Technology and Engineering & VIT University¹
Vellore, Tamil Nadu, India.

(Email: balamuruganb@vit.ac.in)

Department of Computer Science & Sri Padmavathi Mahila Visvavidyalayam, University²
Tirupati, Andhra Pradesh, India

School of Computer Science and Engineering & VIT University³
Vellore, Tamil Nadu, India

Leeds Beckett University, UK⁴

(Received Mar. 01, 2016; revised and accepted June 10 & July 12, 2016)

Abstract

Cloud computing has drastically condensed the computational and storage costs of outsourced data. The existing access control techniques offer users access provisions centered on the common user attributes like Roles, which reduces the fine-grained access measure. The paper defines a Storage Correctness and Fine-grained Access Provision (SCFAP) scheme, that provides the user an exclusive access through the use of a hierarchical structure which is a combination of users unique and common attributes. Also, we deploy the concept of Token Granting system that allows the users to verify the correctness of outsourced data without the retrieval of the respective files. The tokens are derived from the metadata containing file location that helps in the process of storage correctness verification and improvises the storage efficiency. The experimental results show SCFAP has improved storage efficiency and error recovery measures than existing techniques.

Keywords: Access control, access structure, barrier limits, storage efficiency, token granting system

1 Introduction

Cloud computing is one of the widely used emerging technique that offers various methods to acquire and manage IT resources on a large-scale [19, 22]. Cloud computing, in turn, provides different types of services such as

Infrastructure-as-a-service (IaaS) also sometimes called as hardware as a service (HaaS) [1, 7], Platform-as-a-service (PaaS) and Software-as-a-service (SaaS). Cloud computing planning promotes the resource sharing in a pure plug and provides a model that dramatically simplifies its infrastructure. The major advantage of cloud computing includes ease-of-use and cost-effectiveness in accessing the resources over the Internet. Employing the resources in the cloud provides greater expediency to the user because of its systematic manner. Cloud helps us to make use of the existing technologies such as virtualization, service-orientation and grid computing in large-scale distributed environment [4, 5]. To assure the cloud data integrity and availability, efficient approaches that enable storage correctness assurance on behalf of cloud users have to be premeditated. Hence, cloud operations should also imperatively support the dynamic features that make the system design even more challenging.

As Cloud computing is a new emergent technology despite having many beneficial factors, it faces many threats in various ways. It has spread very fast due to its flexibility over ease of access as it eliminates the need for extra hard drives and memory space allocation. As the cloud is a distributed system, the data stored in it is widespread in distinct locations, and it is accessed anywhere. The distributed nature of the data creates the requirement for high security over outsourced data as there exists a probability that anyone can exploit the outsourced data. The hackers [1, 2, 16], can also access the outsourced data by hacking any server virtually, and the statistical results

showed that one-third of the breaches happened from stolen or lost laptops exposing the data unintentionally from the users or the employee of the organization over the Internet. Further, nearly 16 percent of this data exposure is due to the insider theft. The cloud security providers were even trying to provide a solution to security problems such as security, privacy, reliability, legal issues, open standards, compliance, freedom and long-term viability.

Cloud affords three major types of deployment models, which comprises of Public, Private, and Hybrid Cloud. Most-common level people and some organizations make use of the public cloud model in a majority for data storage purposes because it consumes less cost and correspondingly provides utmost security over the outsourced data, but there is also a probability of data leakage in a public cloud environment. The private cloud model [9, 13], depends upon a particular firm but found to be comparatively costlier than the public cloud. The combination of either private- public or public-public or private-private infrastructure forms the Hybrid cloud environment [12, 15], providing the combined advantage of both the private and the public cloud. The significant benefit of the use of the hybrid cloud involves improvised security with lesser management costs.

The possession of fine-grained data access control and storage correctness verification remains to be a mandatory feature in any system, which shares the data contents among multiple users with different level of trust. To ensure the property of cloud data security, highly trusted cloud users might be allowed with full access rights while the other users were assigned partial access rights over the outsourced data. Efficient management of the fine-grained access provision in a system with users having different access privileges remains to be a challenging issue in cloud computing.

To provide better security features in cloud computing environment, a novel Storage Correctness and Fine-grained Access Provision Scheme (SCFAP) is given. It comprises of two parts, where the first part designates the access structures to the users and the second presents a storage correctness scheme through the use of the access structure defined at the preliminaries. A combination of public key, private key, and access structures is assigned to all the users of the system that is derived from the appropriate user attributes. Through the distributed keys and access structures, every single user of the system establishes the secure cloud connection and performs accesses to the cloud data. For every successful cloud data upload, the user is provided with a token, which is used to verify and validate the storage correctness associated with the outsourced data thereby improving the storage efficiency.

The paper is organized in the following manner. The section next to introduction details the literature survey, the next part, deals with the summary of limitations followed by preliminary concepts and algorithms, system design, the proposed SCFAP scheme, case study, Implementation Details, Results, and Discussion. The paper is

ended with the conclusion and future work.

2 Related Works

This section describes and analyzes other approaches towards facing the challenge of fine-grained access provision to cloud users. Multiple solutions are examined, after which an overview of their works was given. This section also describes the comparison of two major approaches that is related to the fine-grained access provision techniques.

2.1 Overview

This section presents an overview of the works, which is related to the proposed SCFAP scheme.

2.1.1 Cloud based Access Control Techniques

[24] presents a data access control scheme called DAC-MAC for the multi authority cloud storage system. It provides a multi-authority CP-ABE scheme with efficient data decryption and user revocation functions. This work further offers an Extensive Data Access Control Scheme (EDAC-MACS) that provides secured user data access even at weaker security assumptions. The security analysis results of this scheme prove that this scheme is collusion resistance but lacks at the property of fine-grained access provision to the individual users of the system. In work done by [25, 10], integration of cryptographic techniques with RBAC techniques was made and it uses role keys for data decryption. Further this work presents a hybrid cloud architecture, where the public cloud contains the basic level details and most sensitive information over the private cloud. This work separates the property of user delegation to active and passive types and establishes effective role management through the use of delegation servers and protocols. The Cipher text-Policy Attribute-Based Encryption was given by; it realizes the complex access control mechanisms over the encrypted data [23, 14]. Here the attributes expressed solitarily the user credentials and the person who encrypts the data could fix the access limit to the users for data decryption. Through the use of this scheme, the data stored could be kept confidential even though it resides on the untrusted server. The ID-based cryptographic scheme [8], makes use of the user attributes such as user id for encryption and decryption process of the outsourced data. The development of ID-based cryptographic scheme provides the secured data storage over the public cloud and improved client authorization for other users to access the data content.

2.1.2 Hierarchical Based Access Control Schemes

In HASBE [17, 21], the user access rights were provided by the hierarchical access structure framed for each user of

the system. This scheme ensures the property of scalability through the extension of ASBE (Attribute-Set Based Encryption) technique [6]. It defines a hierarchical structure that delegates the operation of trusted authority and private key generation to the domain authorities of the lower level. Here the user attributes were converted into the stable structure of the recursive type that permits the users to define constraints dynamically by representing a different combination of attributes, which satisfies the user access policy. That ensures the property of flexibility and fine-grained access control over HASBE systems. The concept of Hierarchical Based Access Structure is extended to form the Hierarchical Structure used in this paper.

2.1.3 Token Based Access Verification Systems

[20] proposed a flexible distributed storage integrity auditing mechanism that consists of homomorphic tokens and erasure-coded data. Tokens are provided to the users from randomly chosen block indices from each data vector space analogous to the memory location of the user requested file in the cloud. The use of erasure coded data technique protects the user data and eliminates the system errors such as data redundancy, fault tolerance and server crashes. In Privacy-Preserving Public Auditing for Secure Cloud Storage by [18, 11] comprises a third-party auditor (TPA) for auditing the integrity of outsourced data; this eradicates the new threats and realizes the data privacy. This scheme uses random masking technique integrated with a homomorphic authenticator that ensures the privacy of public auditing. Flexible distributed storage integrity checking mechanism is proposed by [3] using homomorphic tokens and it avoids security problems like identifying unknown users. Through the use of homomorphic tokens and distributed erasure coded data, users were permitted to audit the outsourced data. This auditing allows the users to identify both the improper data access and cloud server misbehaviors. This scheme even ensures the cloud data security, which allows the users to perform dynamic operations efficiently over the outsourced data. Experimental analysis of their proposed scheme proves that it provides high efficiency against Byzantine failure, unknown user attacks and attacks on cloud data modification. Access control schemes based on the token system were developed to provide greater security over the cloud storage systems.

2.2 Comparison of Related Works

This section presents a brief summary about two major approaches relating to the proposed SCFAP scheme. The HASBE scheme given by [17], and the flexible integrity auditing mechanism provided by Wang Cong et al, were taken into comparison, and it is described as follows:

2.2.1 Work by Wan Zhiguo et al.

To ensure the property of scalability and flexibility over outsourced data, a solution is presented in work done by [17]. This work shows a Hierarchical Attribute-Set-Based Encryption (HASBE) scheme to cloud users, which extends the property of Cipher-text attribute-set-based encryption technique. This scheme not only aims in the achievement of scalability, it even inherits the property of flexibility and fine-grained access provision through the management of compound attributes. The HASBE scheme makes use of multiple value access expiration time to deal with user revocation problems. The first part of this work describes the extension of HASBE from ASBE technique using the hierarchical structure. Whereas the second part provides a clear demonstration of the implementation of access control scheme based on HASBE for cloud computing.

The cloud computing system considered in this work consists of five major entities. The cloud service provider provides services to users. The data owners share their data contents through the cloud in an encrypted manner. Data consumers decrypt the shared contents to perform their respective access operations. Each data owner and data consumer was assigned with a domain authority, where each domain authorities could be managed through parent domain authorities or trusted domain authorities. The major responsibility of every domain authority is to administer the domain authorities at next level or the data owner or consumer in its domain. In HASBE scheme the data users were only assumed to possess read access. All the entities associated with this scheme were organized in a hierarchical manner to accomplish their tasks.

A recursive set based key structure is formed for every user, where each element of the set is either a set or an element corresponding to a user attribute. The depth of the key structure is found using the level of recursions in the recursive set, which is similar to the definition of depth tree. For a key structure of depth 2, members of the set can either be sets or attribute elements at depth 1. At depth 2 it is mandatory that all the members of the set should be of attribute elements. A unique label for the user attributes was formed using key structure. The access structure to the users in HASBE was formed in a similar way to the ASBE scheme given by [3]. In access tree structures the leaf nodes were considered to be the attributes, and non-leaf nodes represent the threshold gates. The non-leaf nodes were defined using its children and threshold values.

This work provides user access provision with the help of the hierarchical access structure, and it is formed using appropriate user key structure and access structures. It means that the user with private key corresponding to attributes in key structure would be able to access the data, only when their attributes satisfies the access policies defined by the access structure. System Setup, Top-Level Domain Authority Grant, New Domain Authority/User Grant, New File Creation, User Revocation, File Access,

and File Deletion are the seven major operations associated with Wan Zhiguo et al HASBE scheme. Each major system operations related to the HASBE scheme invokes the appropriate algorithms associated with it to accomplish their tasks, and it works by bilinear mapping concepts. Through the use of this operations, every user of the system shares and uses their data contents using HASBE scheme.

Though Wan Zhiguo et al system provides a better solution to scalability and flexibility issues, the complete support for compound values and multiple value assignments are measured and found to be lagging in efficiency. Which reduces the level of fine-grained data access. The proposed SCFAP scheme defines users with their role-based classification. Provides efficient support for compound attributes and multiple value assignments. The hierarchical structure described in SCFAP scheme improves the level of fine-grained access provision associated with individual users of the system. The HASBE scheme further does not allow write access to the data users of the system. This makes its application inappropriate to critical systems like financial sectors, where several users require write operations to be performed. SCFAP scheme allows the users to perform write operations in an effective manner, and it is achieved through the use of token granting system, which preserves the storage correctness of the outsourced data.

2.2.2 Work by Wang Cong et al.

An approach to form solution for security risks accompanying the correctness of physical possession over outsourced data were done by [17]. This work presents a flexible distributed storage integrity auditing mechanism, which ensures the correctness of outsourced data through the use of homomorphic token and distributed erasure-coded data. This scheme provides efficient user auditing of cloud data with very lightweight communication and computation cost. The auditing result provides both storage correctness guarantee as well as fast data error localization (identification of server misbehaviors). It even allows user access operations over outsourced data including block deletion, modification and appends functionalities. The overall contributions of this work is summarized as follows:

- 1) In comparison to many of its predecessors, this scheme achieves both the storage correctness insurance and data error localizations.
- 2) This scheme further supports secure and dynamic operation over data blocks including update, delete and append.
- 3) The work further makes an extensive security analysis that shows its resistance towards Byzantine failures and malicious data modification attack and server colluding attacks.

The flexible integrity auditing mechanism discussed in this section consists of four major entities, which includes User, Cloud Service Provider (CSP), Cloud Server (CS) and Third Party Auditor (TPA). Users share their data through cloud storage services, and a user can be either enterprise or an individual customer. Cloud Server (CS) is managed by the CSP to provide better computation and storage facilities to the users of the system. TPA is an optional entity with expertise qualities that user does not possess. TPA assesses and describes the risk of cloud storage services on behalf of users upon request. This work provides more focus towards file oriented data rather than non-file oriented applications like social networking systems. Block level operations over user data were considered as block update, block delete, block insert and append operations. The major focus of this work is to identify the key integrity issues like unauthorized data modifications and corruptions, caused due to server compromises and random Byzantine failures.

Users store their valid credential to cloud servers through CSPs. The problem of data redundancy could be employed through the technique of erasure correcting code. This scheme further tolerates faults and server crashes that happen due to increasing data users. The users interact with cloud servers for processing file retrieval request through CSPs. As it is not feasible for the users to possess their data locally, it is necessary to verify the correctness and maintenance of the cloud data. The users were provided with the pre-computed tokens that provide correctness assurance to the users of the system. Tokens are derived from the subset of file blocks in a random manner. The verification token helps the users to ensure correctness of data operation request processed by the CSP. Tokens are issued to the user based on randomly chosen block indices from each data vector space corresponding to memory position of the requested file in the cloud and erasure-coded data. In cases of inappropriate situations like insufficient resources and time the users can delegate their responsibilities to TPA. The system is designed in such a way that leakages of user? Outsourced data towards auditing protocol were prohibited. This work achieves secure data storage through five major steps, which includes file distribution preparation, challenge token pre-computation, correctness verification and error localization, file retrieving and auditing and finally, towards third party auditing. The algorithms associated with each stage helps in the management of activities accompanying data storage management and correctness verification processes. This scheme provides an approach methodology that prevents CSP to process data dynamics without knowing user secret key materials and ensures users that dynamic data operation request done by CSP were processed faithfully. In this manner the property of integrity assurance and storage correctness where done in [17] scheme.

Tokens were provided to the users, based upon randomly generated block indexes and memory position of the file. This makes the property of storage correctness

associated with integrity auditing scheme to be a probabilistic feature. The proposed SCFAP scheme solves this issue by granting tokens to the users in a deterministic manner. In SCFAP scheme tokens were derived from Metadata containing file locations and distributed to all the users of the system during appropriate phases. Here the major advantage is that as a result of the write operation done by the authorized system an updated token would be provided to all the users of the system, through which the property of storage correctness is achieved.

3 Construction of Storage Correctness and Fine-grained Access Provision Technique

3.1 System Design

This section presents a conceptual design of the novel scheme called Storage Correctness and Fine-grained Access Provision (SCFAP) scheme, which is described in Figure 1. The proposed SCFAP scheme consists of two parts. The first part deals with the construction of hierarchical based user access structures and the second part depicts the algorithmic phases associated with SCFAP scheme that helps in the achievement of fine-grained data access and improved storage efficiency across the outsourced cloud data storage. A set of appropriate cryptographic keys and access structures derived from the exact user attributes were distributed to all the users of the system. Through the use of the access structures and cryptographic keys every user of the system performs the cloud data access in a secure way. As a result of the encryption process, both the data owners and users were provided with a token, which assists in the process of integrity and security verification over the outsourced data.

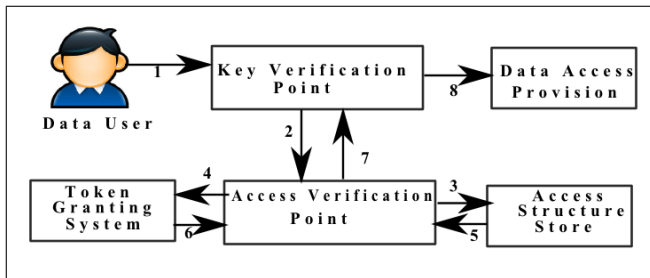


Figure 1: System design of SCFAP

The proposed system consists of five major entities and the description to the entities were given as follows, Attribute Authority (AA): The major responsibility of the Attribute Authority (AA) is to manage all the attribute related activities in specialization with the activities confining to the management of user roles. This includes maintenance of role revocation, delegation, key allocation to users and authentication of the user given credentials like the public key, private key, etc. Cloud server (CS):

Cloud server performs all the computation related activities. This includes the computation of user given inputs and producing corresponding computational results and acknowledgments to the users. Cloud Service Provider (CSP): The Cloud Service Provider (CSP) provides services to the users of the system and performs the validation of the user given inputs and outputs during the process of encryption and decryption. Service Consumers (Users): A Service consumer is also called as the user of the system, consumes the services provided by the cloud computing environment. Data Owner: Shares valid data contents over cloud computing environment and fixes data access limits across data users.

3.2 Assumptions

This work assumes an existing data access control model to build upon, and the proposed design makes use of the access control properties defined previously at related works. The hierarchical structure described in this paper is assumed to provide many-to-many data sharing in a secured manner through which the property of fine-grained access control, confidentiality, and non-repudiation of the outsourced data was achieved.

3.3 Key Terminologies

3.3.1 Access Assignment Structure

A summary on Access assignment structure is depicted in Figure 2.

3.3.2 Hierarchical Structure

The hierarchical structure defines the access policy associated with the individual users of the system. A hierarchy is framed from the combination of the user unique and common attributes. Each hierarchy represents the one to one relationship between the user and their access policies. The access policy defines the set of operations (read or write access) the user could perform over the outsourced data.

3.3.3 Key Structure

Key structures were designed to preserve the security of the outsourced data. Key structures are derivatives from the user common attributes like roles. The formation of key structure assigns the access privileges to the set of the common users over the outsourced data. This states that users beneath a particular role were assigned with a key structure such that they could gain access to a particular set of files.

3.3.4 Access Structure

Access structures were designed to achieve the property of fine-grained user access and it is derived from the user unique attributes like user id. It defines the extent to which an individual user could access the data.

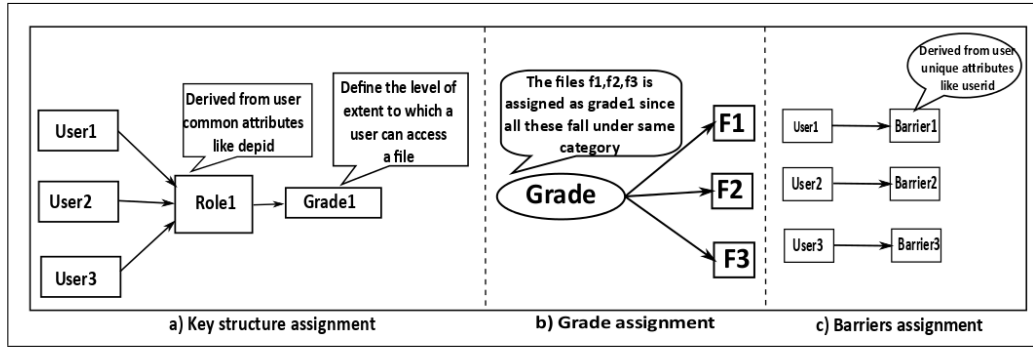


Figure 2: Access assignment structure

3.3.5 Grade

Grade denotes the level of the extent to which the set of common users could gain access to a particular set of files. Each grade formally represents a key structure, such that a user with certain grade could gain access to all the files that comes with the scope of a particular grade. Grades were derived from the user common attributes like dep id, such that it represents a set of files that belongs to the particular department. An example of the measure of a grade is described in Figure 3.

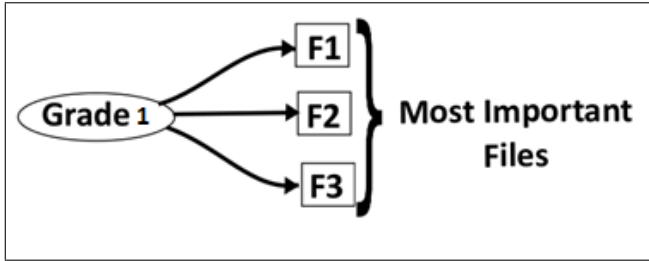


Figure 3: Access limits associated with a grade

3.3.6 Barriers

Barriers are restrictions imposed over the grades to achieve the fine-grained user access level. It has been found that it is not necessary for a user with a particular grade to access all the files that come under a particular grade. To solve this issue, barriers were designed and imposed over the user grades.

From Figure 4. It is understood that though the user belongs to grade1 which provides access rights to three files F1, F2, F3. The imposition of the barrier B1 over the particular user grade G denies the user file access request to the file F2; such that the user could only be able to access the files F1 and F2. It provides the appropriate access rights to the users through which the property of fine-grained access provision is achieved.

3.3.7 Tokens

Tokens were derived from the metadata containing the file location and it acts as a user authentication entity. To-

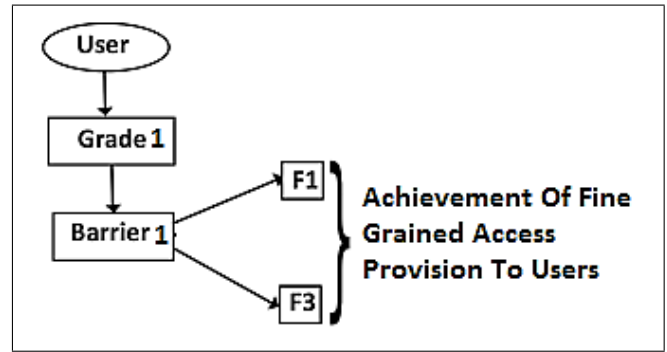


Figure 4: Barrier generations

kens were issued to the data users as a result of the data encryption process. Through the use of the tokens, the user could easily verify the existence of their corresponding files in a convenient manner. Since the token represents the Metadata about the file location, it assists in the process of easier file retrieval. This improves the storage efficiency of the proposed system. Further, clear descriptions about the working of the tokens were described in phase 6, 7 and 8 of the SCFAP scheme. A new method of mathematical modelling was used to identify the functions and variables of the proposed scheme.

4 Preliminary Concepts and Algorithms

4.1 KeyGen()

KeyGen() is a basic algorithm for key generation through which all the other keys associated with the data users were derived. This algorithm is invoked automatically whenever the process of key generation is required.

Let us consider the set of keys k such that it contains a set of integers up to n . Such that $K_n = \{k_1, k_2, \dots, k_n\}$.

$$k_n : \sum_{Z=0}^n K_Z \approx \sum_{m=0}^n d_m.$$

Where d is the set of derived keys. It could be of any other keylike master key, public key and private key. In

a simpler way the KeyGen algorithm generates random number of keys in accordance to the user given input parameters.

4.2 Formation of Hierarchical Access Structure

The proposed SCFAP scheme makes use of the hierarchical access structure to define the user access rights. The basic concept behind the hierarchical access structure was described in the previous section of the paper. In SCFAP scheme each user is assigned with a hierarchical structure, which is derived from their respective key and access structures.

Key structure is premeditated to preserve the security of the outsourced data and it represents the access rights to the group of users with a common identity. The basic concepts behind the formation of the key structure were given in the previous section. It is formed using the user common attributes like dep id. In an organization the most important or most secured files could be accessed only by the personals at the top-most designation order, least important files by the low-level personals and ordinary files could be accessed by the mid-level individuals. In correspondence to the user designation order grades for a group of members with common identity (users under a particular role) is calculated from “grade1.grade n”. For every user with a role, grades were allocated with respect to their access privilege that defines the level of extent to which the users could access the data.

4.2.1 Access Structure

The access structure represents the access rights to the individual user of the system. Even though a particular user is assigned with a grade representing the key structure, it is not mandatory that the user could access all the files that come under a particular grade. The access structures associated with the SCFAP scheme were designed in such a way that solves the problem of above mentioned issue. The access structure was framed from the user barrier limits, which are derived from the user unique attributes like user id. Barriers are restrictions that were imposed over the user access grades to achieve the fine-grained access control. The assignment of the access structure defines the individual access limits over the set of files. In addition to this, phase 3 of the storage correctness scheme provides a brief summary about the algorithmic implementation of the user access structure assignment.

Through the use of the key and access structure discussed above, a hierarchical access structure is formed in the proposed SCFAP scheme, and it is illustrated in Figure 2.

4.2.2 Token Granting System

The proposed SCFAP scheme makes use of the token granting system through which the property of storage

correctness is achieved. As it is described at the previous section tokens were derived from the Meta data containing the file location that assist in both ways, through which the process of storage correctness as well as the easier retrieval of the outsourced files could be made. The prime idea behind the use of token granting system in SCFAP scheme is that at the end of every successful data encryption process the data users were provided with the tokens, through which the data users verifies the existence of the outsourced data. The users could also be able to perform the decryption process only when the Meta data of the user given token points to the user requested file.

4.3 SCFAP Phases

The storage correctness phases and fine-grained access provision scheme consists of nine phases through which the property of fine-grained access provision and storage correctness verification is achieved. The SCFAP phases apply the concept of hierarchical access structure and token granting system described in preliminaries part.

4.3.1 Phase 1: SetUp()

It takes the user security parameter λ as an input and generates master key m_k as an output. This step is done by the cloud server through automatically invoking the KeyGen algorithm.

$$K : m_k = \lambda \bowtie k_n. \quad (1)$$

Equation 1 joins the user security parameter with the unique key generated by KeyGen() algorithm and distributes the master key to the corresponding users of the system.

4.3.2 Phase 2: GradeGen(m_k, R_{id})

This phase is performed by the Attribute Authority and it takes the master key m_k and Role id R_{id} as an input, produces public key p_k and grade g as an output. Public key is derived from the master key m_k by manually invoking the KeyGen() algorithm. Let us consider two sets, $R = \{R_1, R_2, R_3, \dots, R_n\}$ and $G = \{g_1, g_2, g_3, \dots, g_n\}$ be the set of roles and grades. Such that $R \approx G$ (means that the role R is isomorphic to grade G).

$$Z : \forall R_{id} \in R | R_{id} \subseteq R.$$

Any R_{id} that belongs to R is the subset of R.

$$Z : \forall R_{id} : P(R_{id}) | R_{id} < \bullet R. \quad (2)$$

At least for one value of R_{id} the value of R_{id} in R is true. Such that R_{id} is covered by r where $r \in R$.

$$\therefore Z : \exists R_{id} \rightarrow r | r \Leftrightarrow G.$$

There exists G and R_{id} that implies a role such that the role corresponds to a grade G.

4.3.3 Phase 3: BarrierGen(U_{id}, r_k, p_k)

It takes (U_{id}, r_k, p_k) use rid, role key, and public key as an input and as a result of computation the barrier limit b_l and the private key p_{rk} is returned to the users.

The private key is manually generated by role admin through the invocation of KeyGen() algorithm.

Let U be the universal set that contains all the users of the system and can be written as $U = \{U_1, U_2, \dots, U_n\}$ and B be the set of barriers such that can be written as $B = \{b_1, b_2, \dots, b_n\}$.

$$\begin{aligned} Z &: \forall U_{id} \in U_{id} \subseteq U. \\ \forall U_{id} &: P(U_{id})|U_{id} \prec \bullet U. \end{aligned}$$

Similarly from Equation 2 this step is derived.

$$\sum_{k=1}^n U_k \exists B | \sum_{k=1}^n U_k \in B | \sum_{k=1}^n U_k \subseteq B.$$

Means that for all the users there exists a barrier limit such that all the users in U belong to barriers in B . So that U is the subset of B . Such that there exists an $U_{id} \in B$. where

$$Z : b = \prod_{u \in U} bu : \prod_{u \in U} Ru \rightarrow G.$$

Since, all the users U is the subset of B there exists a b corresponding to the user u , where the barriers can be calculated as a co-product of user and barrier sets.

4.3.4 Phase 4: Encrypt(f, r_k, p_k)

This phase is done by the CSP and it takes the file f , role key r_k and Public key p_k as an input and the outputs cipher text c_p to the users of the system. Data encryption is done as a part of file upload.

$$\begin{aligned} Z &: f \times r_k \times p_k \Leftrightarrow f^{(r_k, P_k)} \\ Z &: f \times r_k \times p_k \Leftrightarrow c.t | c.t \approx f^{(r_k, P_k)}. \end{aligned}$$

Encryption is done as a combination of input parameters.

4.3.5 Phase 5: TokGen(f, r_k, p_k)

It takes file f , role key r_k and Public key p_k as an input. It is the most important part of the encryption process and it is done during the process of file upload. Since tokens were derived from the data containing file locations, here we use the concept of reduction to reduce a file to tokens. Let $F = \{f_1, f_2, \dots, f_n\}$ be the set of files such that by property of reduction

$$\begin{aligned} &\text{if} \\ &\exists f \in d_b \bullet \forall R \in F \Leftrightarrow f(R) \in t_i \\ &\text{then} \\ &F \leq_{db} t_i \end{aligned}$$

$F \leq_{db} t$ Denotes that a file set F can be reduced to token t_i and it is achieved through the data blocks. At the end of this phase tokens generated were distributed to the data users to verify the correctness of the outsourced data.

4.3.6 Phase 6: Token Computation

It is done by the CSP and cloud server as a part of the data decryption process. Let $F = \{f_1, f_2, \dots, f_n\}$ be the set of files and $T_i = \{t_{i1}, t_{i2}, \dots, t_{in}\}$ be the set of tokens associated with the files. Then,

$$\prod [t_{i1}, t_{i2}, \dots, t_{in}](F_i) = \{d_b[t_{i1}, t_{i2}, \dots, t_{in}]; d_b \in F\}.$$

Where, $F_i = \{1, 2, \dots, n\}$ (Only the tokens between $[t_{i1}, t_{i2}, \dots, t_{in}]$ can access the files in data blocks). Tokens out of this scope would be computed as corrupted and cannot be accessed. It is based on the projection property. Where,

$$d_b[t_{i1}, t_{i2}, \dots, t_{in}] = \{(t_i, v) \in d, t \in [t_{i1}, t_{i2}, \dots, t_{in}]\}.$$

Means the remaining set of data blocks corresponds to some other tokens.

The result of proportion $\prod [t_{i1}, t_{i2}, \dots, t_{in}](F)$ can be found only if $[t_{i1}, t_{i2}, \dots, t_{in}]$ is $\subseteq (F)$. It means a file would be accessed only when token matches with it.

4.3.7 Phase 7: Token Update

Whenever the data user performs the write operation the tokens associated with the users were updated and distributed to all the associated system entities. This is due to the reason that the process of write operation may extend or delete some part of the file that leads to the change of the Meta data containing the file location. The process of token update is described as follows:

$$newt_i = t_i \bowtie w_c.$$

Where w_c is the newly written content.

4.3.8 Step 8: Token Correctness

It is done as a part of data decryption during the process of file download. It takes (t_i, c_p) as an input. Let t_i, c_p be an algebraic function over F then $Z : t_i \in T_i; c_p \in C_p$; let us take an element $t_i \in f$. Such that,

$$\begin{aligned} Z &: (t_i, c_{p1}) + (t_i, c_{p1}) \sim (t_{i1} + t_{i2} + c_p) \\ Z &: (t_i, c_{p1}) + (t_i, c_{p1}) \sim (t_{i1}, c_{p1} + c_{p2}) \\ Z &: f(t_i, c_p) \sim (ft_i, c_p) \sim (t_i, fc_p) \Leftrightarrow t_i \otimes c_p. \end{aligned}$$

It matches the values in the token and cipher text and returns the mismatch thus the token correctness is verified.

4.3.9 Phase 9: Decryption($c_p, r_k, b_l, p_{rk}, t_i$)

Data decryption is done as a part of the file download process. It takes cipher text, role key, barrier limits, private key and token as input and returns the plain text to the users based on their respective access structures.

$$\begin{aligned} Z &: c_p \bowtie t_i = \prod b_1(c_p \bowtie t_i) \\ Z &: c_p \bowtie t_i = \prod b_1(c_p \bowtie t_i) | (c_p \bowtie t_i) = \prod b_1(c_p \bowtie t_i) \Leftrightarrow P_t. \end{aligned}$$

It combines the cipher text and token depending upon the user barrier levels and provides the plain text.

Table 1: Summary of SCFAP phases

Phase No	Phase Name	Input	Output	Doneby
1	SetUP()	λ	M_k	CS
2	GradeGen()	M_k, R_{id}	P_k, G	AA
3	BarrierGen()	U_{id}, R_k, P_k	B, P_r, k	RA
4	Encrypt()	F, R_k, P_k	C_t	CSP
5	TokGen()	F, R_k, P_k	T_i	CS, CSP
6	TokenComp()	F, T_i	C_t	CS, CSP
7	TokenUpdate()	T_i	$newT_i$	CS, CSP
8	TokenCorrectness()	T_i, C_t	File Validity	CS, CSP
9	Decrypt()	T_i, C_t, R_k, B, P_r, k	Plaintext	CSP

5 Advantages of Proposed SCFAP Scheme

- 1) Through the use of the barrier limits in user hierarchical access structure helps in the achievement of fine-grained access rights to the users of the system.
- 2) The algorithmic deployment of the token granting system helps in the achievement of the storage correctness verification of the outsourced data with improved storage efficiency.
- 3) The tokens were derived from the Meta data containing the file location. This reduces the file retrieval time associated with the user data access request.

6 Case Study

It has been found that government agencies adopt cloud services to meet their scaling industrial needs. Though social networking sites were found to be the major users of cloud usage, currently banking contributes to the most activities in the cloud, utilizing 64% of the overall cloud services. Factors like modernization, innovation in information technology, financial products, liberalization and consolidation of financial markets enforces the transformation of the ordinary banking system to the cloud-based one.

In cloud banking systems, the clients could access different types of banking services like balance enquiry, fund transformations, etc. The banking system taken in this scenario falls under the category of fully electronic based transaction systems, where the banking sites exhibit all the information like bank locations, bank products, loan enquiry, loan eligibility details, transaction details, statement of accounts and money transfer facilities.

The management of activities associated with this type of cloud banking system includes several entities like bank clients, cloud service providers, and entities related to the payment gateway. In such a case it is not necessary for the system management entities with common attributes like similar roles to access all the end user provided valid credentials. This creates the need for the application of fine-grained access control scheme over the cloud banking sys-

tem. To solve these issues, the proposed SCFAP scheme were applied to the Cloud banking system that solved the problem of fine-grained access level associated with the individual system entities. Let us consider the situation, where the bank client performs the money transaction across the cloud banking system. The process of money transfer requires the fulfillment of several essential details including the client's valid password. Once the client completes the form filling activity, the client details were transformed to their respective financial institution cloud servers. The client transaction request could be processed through various system management entities like bank account manager, fund transfer manager, cloud service provider, etc. Though all the associated entities possess the same authority of power, it is not necessary for them to process or access all the user given credentials. During fund transfer, it is necessary that the fund transfer manager could access only the required client details like user account balance and eligibility to perform the transaction. But the fund transfer manager is no way related to the user personal and account credentials. It is appropriate for the account manager to verify and validate client account detail apart from the other user given inputs. In order to implement this restriction, a hierarchical access structure is formed in a similar way to the SCFAP scheme. In this case, a hierarchy could be formed through the system entities, common attributes like organization ID along with their unique user ID. Further, the storage correctness phases depicted in this paper could be applied to the cases resembling the need for data integrity assurance. In cloud banking, during the process of user registration the user uses their valid credentials as an input and as a result of the user registration, a login id and password were given to them that act as a token. It could be used by the clients to verify the validity of the user registered details. Thus the storage correctness of the user given inputs such as bank details were verified.

The above scenario clearly explains the application of SCFAP scheme to cloud banking system and it is illustrated in Figure 5. This scheme can also be applied to similar scenarios ranging from the medium-sized to large-sized enterprises. Our system is highly efficient in cases, where a significant number of users with similar roles needs the fine-grained access provisions and frequent ver-

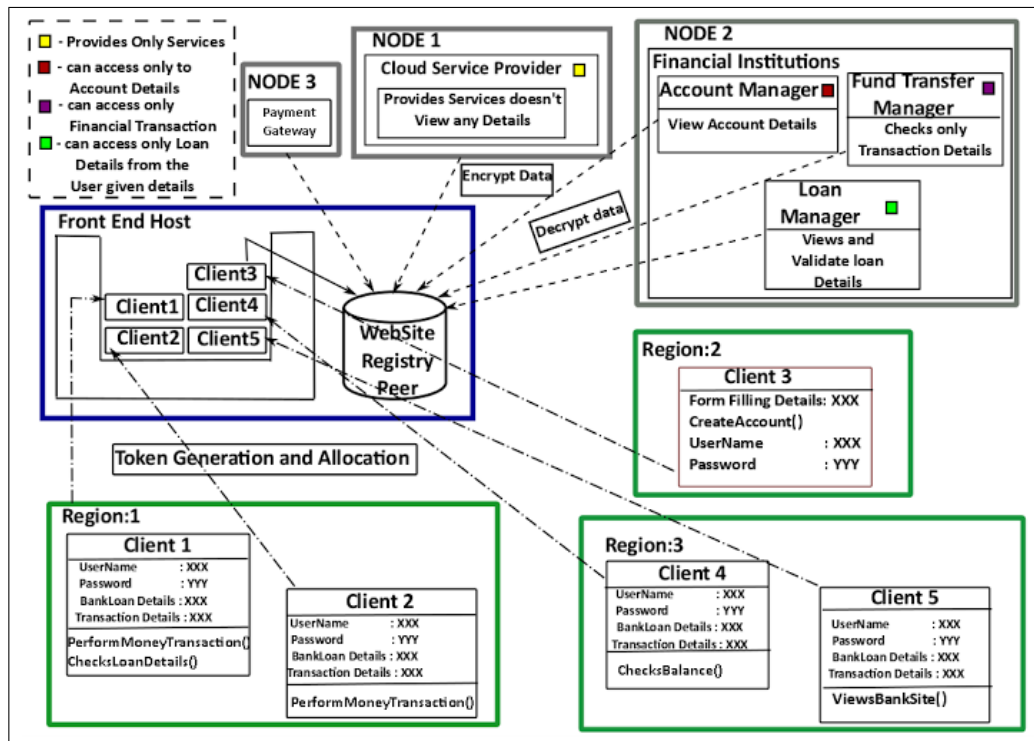


Figure 5: Cloud based financial system-A case study

ifications to the outsourced data.

7 Experimental Study

7.1 Deployment of SCFAP Over Eucalyptus Cloud

An application is created in Eucalyptus an open source cloud platform, which deploys the proposed SCFAP scheme. An interface is developed using JSP to enable users to authenticate and view the cloud storage. Eucalyptus consists of several other interfaces like cloud42, tAWSTanacasino, EC2 Dream, but it is not feasible for the proposed implementation. MySQL community server5.7 is used for storage purposes. The proposed SCFAP scheme runs at the infrastructure layer of the eucalyptus, and it works on a layered basis to accomplish its tasks. The SCFAP scheme consists of four layers such as user registration layer, authentication layer, access security management layer and instance management layer as it is described in Figure 6. The registration layer performs the user registration process. Authentication layer validates the cloudlet credentials, and the access security management layer allows or denies the user file access requests to the virtual machines with the aid of the functionalities present in the instance management layer. The application consists of the Command Line User Interface (CUI) using Euca2ools, which allows the users to interact with the system. Here the users of the system were considered to be the subjects and the files uploaded to the cloud were assumed to be the objects. Every subject creates the

newer objects and requests their corresponding object access through the proposed SCFAP scheme that preserves the storage correctness and fine-grained access provision of the user data. The security management layer controls and directs the access control schemes. The implementation consists of the web interface that possesses the property of ease of use through which the Cloud Service Providers (CSP) or Attribute Authorities (AA) creates the restriction over the cloud instances. The implemented SCFAP scheme allows the AA to manage access to cloud resources, instances, virtual machines and common user groups associated with the cloud computing environment.

The first step associated with the implementation of SCFAP scheme over eucalyptus cloud consists of the setup phase. Once the subject is registered with the system, the AA adds the subject to the common user groups. This states that all the subjects under the common user group contain the common access privileges with particular individual restrictions. These restrictions were imposed on the subjects through the assignment key structure and access structure to the subjects. Every subject can create new objects and gain access to existing objects based upon the following access restrictions:

- 1) Grades Defines the level of the extent to which a common user group can access.
- 2) Barriers Defines the level of extent through which an individual user can access.
- 3) Tokens Derived from Meta data containing file location.

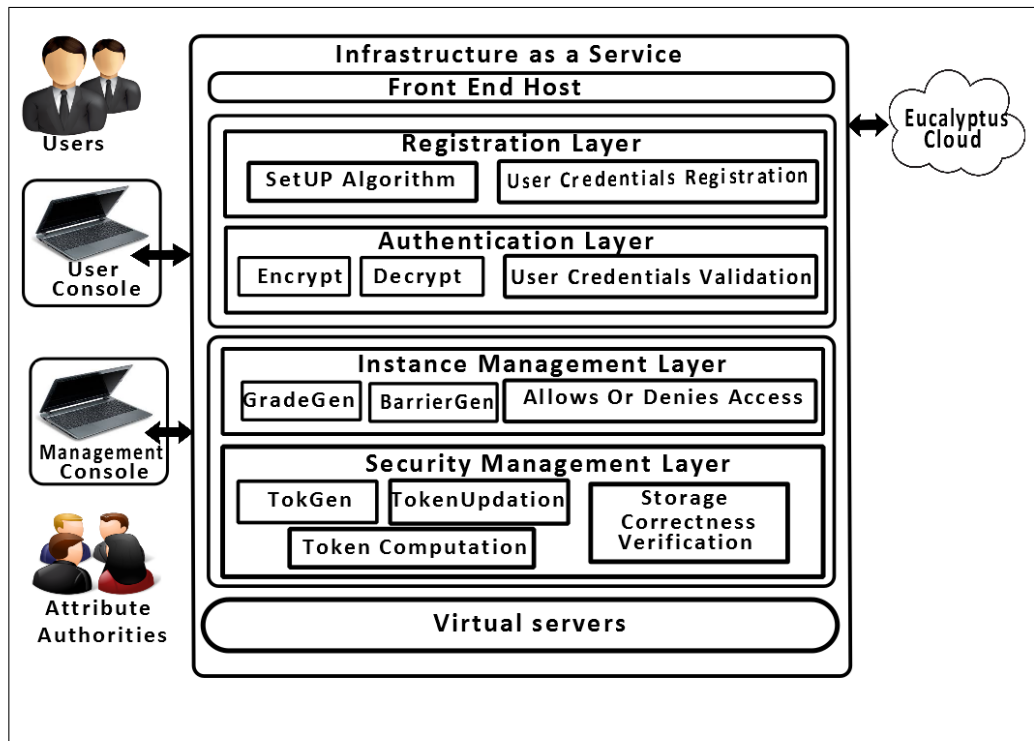


Figure 6: Architecture of SCFAP over eucalyptus cloud

Each subject shares their newly created objects to the other subjects of common user groups. The subject can also share their objects to other Common User groups which they were not a member. To gain access to the shared objects and instances the subject accessing the object could not violate the SCFAP access policy. Each subject could ensure the property of integrity over their respective subjects through the use of token granting systems. An updated token would be distributed to every subject associated with the shared object in case of modifications to the shared data objects. In this manner, the subject could gain access to the outsourced objects.

The implemented SCFAP consists of two distinct types of interfaces that include subject management and object management interfaces. The subject management interface assists in the management of all the subject related activities that include subject authentication, user common group assignments, subject key allocation, and management. The object management interface is responsible for the process of management of all the object-related activities that include object storage, object retrieval, token generation, token computation, and management.

7.2 Validation of Premises

Built on the open source cloud platform Eucalyptus the application of SCFAP scheme to the developed prototype could be validated through the verification of premises that happens in four steps, which are described as follows:

- 1) Each authenticated subject should be assigned to the common user group.
- 2) Each subject should be assigned with an appropriate hierarchical access structure.
- 3) Token computation results should match with the user given token and the user given file access request.
- 4) Encryption and decryption processes could be performed when the subject given inputs are valid.

7.3 Access Verification Tests

The first test comprises the access request to the object from the subject who is not the member of the any of the common user group associated with the developed system. The request would be denied by the setup algorithm present at the authentication layer. The next test comprises the file access request from the subject with inappropriate hierarchical access structure. This request is blocked by GradeGen and AccessGen algorithms functioning at the access security management layer. A subjects access request for an object with invalid user credentials like invalid tokens and the secret key is denied, and the subject is blocked from accessing the services if he repeats the same for three times. The request for encryption or decryption processes with inappropriate cryptographic keys or inputs by the subjects is blocked through the several algorithms like Setup, GradeGen, BarrierGen, Token computation and Encrypt or Decrypt algorithm present at the user registration layer, Authentication Layer Security management layer and instance management layer of the developed prototype. In this

manner the exception handling capabilities of the developed prototype where clearly described using the system access verification tests.

8 Results and Discussions

The major objective of the experimental implementation is to validate the level of an extent to which the proposed SCFAP scheme provides the property of fine-grained data access to the cloud users. To validate this objective prototypes using traditional access control, techniques like ABE and RBAC were implemented, and it is compared with the proposed SCFAP scheme. From the results of the implementation, a comparison is made regarding both system performance and fine-grained access provision, which is described in Figure 7 and 8. First, a comparison is made between the amount of data to be retrieved and file retrieval time to find the system performance. At client side, n numbers of client nodes were created, and a large number of files from different client node was uploaded to the cloud storage. Client file access requests were given from various nodes and the number of client requests per minute was calculated regarding size of the data files accompanying the client requests and it is kept as X limits. The time taken by the cloud server to respond to user file access requests was calculated in seconds, and this forms the Y limits. It has been observed that the time taken for file retrieval on the size of the data file for our SCFAP scheme remains constant up to a particular threshold. Even though there is a tremendous increase in file size that happens after a particular threshold, the time taken for file retrieval increases in a consistent manner. But the observation of traditional access control schemes like ABE and RBAC deviates highly and takes more time for file retrieval after a particular threshold. This is due to the inconsistent nature of their underlying access policies. The comparison between SCFAP with traditional ABE and RBAC techniques regarding file retrieval time proves that the proposed SCFAP scheme takes reduced file retrieval time than the existing schemes. This is due to the use of the token granting systems. Since the tokens were derived from the Meta data containing the file location, the time taken for file retrieval and storage correctness verification has been comparatively improved. The overall simulation results depict that the file retrieval has been reduced by 0.5 seconds in comparative to the existing access control techniques. This improves the overall performance measure of the system.

A measure to the level of fine-graininess associated with the SCFAP scheme in comparison to the traditional access control methods like ABE and RBAC were made, which is depicted in Figure 7.

The level of fine-grained access control is measured by the extent to which the appropriate access rights were provided to the users of the system. User access policies based upon SCFAP, ABE and RBAC models were designed for each client nodes associated with the system.

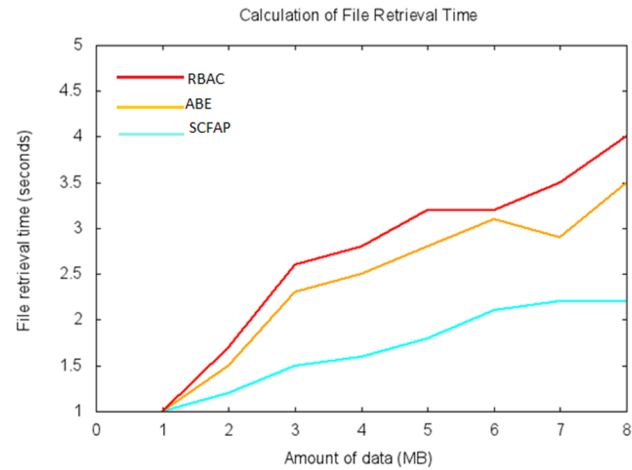


Figure 7: Comparison of file retrieval time in SCFAP scheme

Through the implementation of SCFAP scheme over the eucalyptus-cloud and the use of a vast number of the client nodes, a hierarchy is formed for every user accompanying the client node. A comparative measure of fine-grained access level has been made in association with the depth of access structure. The depth of the access structures was kept in X limits and fine-grained access level in percentage were fixed at Y limits. It has been found that our proposed SCFAP scheme provides better fine-grained access level to the data users even at lesser access structure depth. The other access control techniques taken into comparison were found to be lagging inefficiency at the lower level of access structure depth. Achieved through the derivation of appropriate hierarchical structures associated with SCFAP scheme, which provides better access provision even at the lower access structure depth. The existing technique lags at fine-grained access provision through the complex access structure formation. The tests were conducted using banking research dataset of the Federal Bank of New York.

9 Conclusion

The paper defines an SCFAP scheme that solves the problem of fine-grained access provision and storage correctness associated with the existing access control techniques. The first part of the SCFAP scheme involves the formation of hierarchical structures that fixes the appropriate access policies to the users; this improves the fine-grained ness associated with the access policy. The next part deals with the achievement of storage correctness related to the files, and it is made through the usage of the token granting system. In addition to this, the use of token granting system improves the storage efficiency, security, and performance of the proposed system. As this paper explains only on the key structure and Access Structure associated with the plain text but not about the Cipher Text Access Structure. In future, this work could

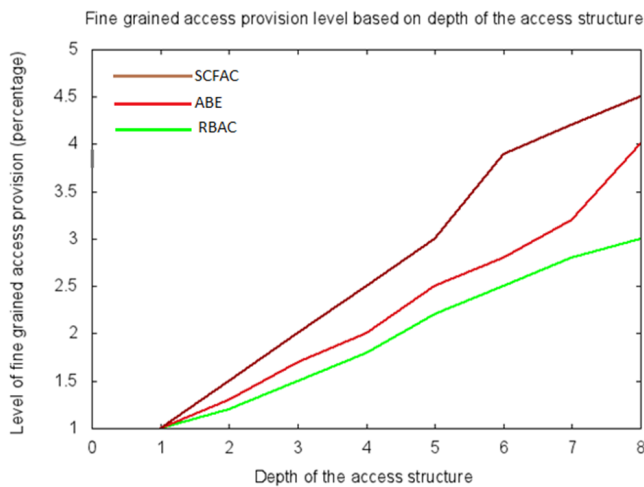


Figure 8: Comparison to fine-grained access provision measure in SCFAP scheme

be extended for outsourced data decryption techniques.

Acknowledgments

The author gratefully acknowledge the VIT University for providing us an wonderful work infrastructure.

References

- [1] P. Arora, R. C. Wadhawan, and E. S. P. Ahuja, "Cloud computing security issues in infrastructure as a service," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, no. 1, pp. 1–7, 2012.
- [2] V. Bhangotra and A. Puri, "Enhancing cloud security by using hybrid encryption scheme," *International Journal of Advanced Engineering Technology*, vol. 6, no. 4, pp. 34–40, 2015.
- [3] R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: A practically motivated enhancement to attribute-based encryption," in *Computer Security (ESORICS'09)*, pp. 587–604, Springer, 2009.
- [4] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Generation Computer Systems*, vol. 25, no. 6, pp. 599–616, 2009.
- [5] Z. Cao, C. Mao, L. Liu, "Analysis of one secure anti-collusion data sharing scheme for dynamic groups in the cloud," *International Journal of Electronics and Information Engineering*, vol. 5, no. 2, pp. 68–72, 2016.
- [6] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security*, pp. 89–98, 2006.
- [7] W. Huang, A. Ganjali, B. H. Kim, S. Oh, and D. Lie, "The state of public infrastructure-as-a-service cloud security," *ACM Computing Surveys*, vol. 47, no. 4, pp. 68, 2015.
- [8] N. Kaaniche, A. Boudguiga, and M. Laurent, "ID-based cryptography for secure cloud data storage," in *2013 IEEE Sixth International Conference on Cloud Computing*, 2013.
- [9] R. Ko and R. Choo, *The Cloud Security Ecosystem: Technical, Legal, Business and Management Issues*, Syngress, 2015.
- [10] J. Li, J. Li, X. Chen, C. Jia, and W. Lou, "Identity-based encryption with outsourced revocation in cloud computing," *IEEE Transactions on Computers*, vol. 64, no. 2, pp. 425–437, 2015.
- [11] J. Liu, X. Huang, and J. K. Liu, "Secure sharing of personal health records in cloud computing: ciphertext-policy attribute-based signcryption," *Future Generation Computer Systems*, vol. 52, pp. 67–76, 2015.
- [12] O. Mazhelis and P. Tyrväinen, "Role of data communications in hybrid cloud costs," in *2011 37th IEEE EUROMICRO Conference on Software Engineering and Advanced Applications*, pp. 138–145, 2011.
- [13] S. Ramgovind, M. M. Elof, and E. Smith, "The management of security in cloud computing," in *Proceeding of IEEE Information Security for South Africa (ISSA'10)*, pp. 1–7, 2010.
- [14] B. D. Revathy, M. P. Ravishankar, and C. I. T. Ponnampet, "Enabling secure and efficient keyword ranked search over encrypted data in the cloud," 2015.
- [15] P. Samarati and S. De C. di Vimercati, *Cloud security: Issues and concerns*, Wiley, New York, 2016.
- [16] J. Singh, "Cyber-attacks in cloud computing: A case study," *International Journal of Electronics and Information Engineering*, vol. 1, no. 2, pp. 78–87, 2014.
- [17] Z. Wan, J. Liu, and R. H. Deng, "Hasbe: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 743–754, 2012.
- [18] C. Wang, S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," *IEEE Transactions on Computers*, vol. 62, no. 2, pp. 362–375, 2013.
- [19] C. Wang, K. Ren, W. Lou, and J. Li, "Toward publicly auditable secure cloud data storage services," *IEEE Network*, vol. 24, no. 4, pp. 19–24, 2010.
- [20] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing," *IEEE Transactions on Services Computing*, vol. 5, no. 2, pp. 220–232, 2012.
- [21] S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen, and W. Xie, "An efficient file hierarchy attribute-based encryption scheme in cloud computing," *IEEE*

Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1265–1277, 2016.

- [22] H. Wittl, C. Ghedira, E. Disson, and K. Boukadi, “Security governance in multi-cloud environment: A systematic mapping study,” in *12th World Congress on Services (SERVICES’16)*, 2016.
- [23] Y. Wu, Z. Wei, and R. Deng, “Attribute-based access to scalable media in cloud-assisted content sharing networks,” *IEEE Transactions on Multimedia*, vol. 15, no. 4, pp. 778–788, 2013.
- [24] K. Yang and X. Jia, “Dac-macs: Effective data access control for multi-authority cloud storage systems,” in *Security for Cloud Storage Systems*, pp. 59–83, Springer, 2014.
- [25] L. Zhou, V. Varadharajan, and M. Hitchens, “Achieving secure role-based access control on encrypted data in cloud storage,” *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 1947–1960, 2013.

Biography

Balamurugan Balusamy is with VIT University as Associate Professor in School of Information Technology and Engineering. His research interests have evolved from cloud computing, cloud security to Big data and Ph.D thesis is on Cloud Access Control.

P. Venkata Krishna is a Professor at Sri Padmavati Mahila Visvavidyalayam, Tirupati, India. He received his BTech in Electronics and Communication Engineering from Sri Venkateswara University, Tirupathi, India, MTech in Computer Science and Engineering from REC, Calicut, India, and he received his PhD from VIT University, Vellore, India. Dr. Krishna has several years of experience working in academia, research, consultancy, academic administration, and project management roles. His current research interests include mobile and wireless systems, QoS, and Cloud computing. He has been the recipient of several academic and research awards, such as the Cognizant Best Faculty Award for the year 2009-2010 and VIT Researcher Award for the year 2009-2010. He has authored over 150 research papers in various reputed journals and conferences. He has delivered several keynote addresses in reputed conferences. He is currently serving as Editor-in-Chief for IJSGGC, Inderscience Publishers.

G. S. Tamizh Arasi is a PG scholar in VIT University and her research interests are Cloud Computing security and Cloud access control.

Victor Chang is a Senior Lecturer in Computing at Leeds Beckett University. He has been a technical lead in web applications, web services, database, grid, cloud, storage/backup, bioinformatics, financial computing which subsequently have become his research interests. Victor has also successfully delivered many IT projects in Taiwan, Singapore, Australia, and the UK since 1998. Victor is experienced in a number of different IT subjects and has 27 certifications with 97% on average. He completed PGCert (Higher Education, University Greenwich, 2012) and PhD (C.S, University of Southampton, 2013) within four years while working full-time, whereby the distance between his work and research is about hundreds of miles away. He has over 70 published peer-reviewed papers, including several high-quality journals up-to-date. Victor won G20,000 funding in 2001 (Singapore-Cambridge Trust) and G81,000 funding in 2009 (Department of Health). He was involved in part of the G6.5 million project in 2004, part of the G5.6 million project in 2006 and part of a G300,000 project in 2013. He is a PI and Co-PI in some projects. Victor is a winner in 2011 European Identity Award in “On Premise to Cloud Migration”. He was selected to present his research in the House of Commons, UK, in 2011. He won the best student paper in CLOSER 2012. Dr Victor Chang has taught numerous undergraduate and postgraduate modules. In some modules he taught, students like his teaching and enjoy his labs and lectures.

A Certificateless Strong Designated Verifier Signature Scheme with Non-delegatability

Yang Chen^{1*}, Yang Zhao^{2*}, Hu Xiong^{2,3}, and Feng Yue²

(Corresponding author: Feng Yue)

Sichuan Aerospace Vocational College¹

No.155, Tiansheng Road, Longquanyi District, Chengdu City, Sichuan Province, China

School of Computer Science and Engineering & University of Electronic Science and Technology of China²

No. 4, North Jianshe Road, Chenghua District, Chengdu, Sichuan, 610054, China

State Key Laboratory of Information Security, Institute of Software & Chinese Academy of Sciences³

No. 19, Yuquan Road, Shijingshan District, Beijing, 100190, China

(Email: yf1513875@163.com)

(Received Nov. 6, 2015; revised and accepted Mar. 6 & Apr. 9, 2016)

Abstract

The designated verifier signature only enables the designated verifier to check the correctness of the signature, while any third party can not verify whether this signature is valid or not. Most of the previous designated verifier signature schemes depend on certificate-based cryptography or identity-based cryptography, while little attention has been paid to the certificateless designated verifier signature scheme which has much more advantages than the previous constructions. In this paper, we propose the first certificateless strong designated verifier signature scheme with non-delegatability. We show that our scheme satisfies the basic properties of a designated verifier signature scheme and resists the two types of adversaries in certificateless cryptography. In addition, the comparison with other existing certificateless SDVS schemes demonstrates the proposed scheme is provided with a good level of security and performance.

Keywords: Certificateless cryptography, designated verifier signature, non-delegatability, strong designated verifier signature

1 Introduction

As we all know, the correctness of the conventional digital signature can be checked by anyone using the signer's public key. However, in some situations such as e-voting [14], e-bidding and software licensing, the signer do not desire the receiver to convince the third party of the signature's authenticity. To settle this problem, Jakobsson et al. [9] proposed the notion of designated verifier signature which can be abbreviated to DVS. The most obvious

difference between the conventional digital signature and the DVS is that the designated verifier can not persuade the third party to trust the correctness of the signature in DVS scheme, because the designated verifier is able to construct the signature designated to himself which is indistinguishable from the real signer's signature. Meanwhile, Jakobsson et al. [9] also introduced the conception of the strong designated verifier signature (SDVS) in which the designated verifier's secret key must be used in the verifying phase. Most of existing (S)DVS schemes are based on certificate-based cryptography or identity-based cryptography. Since the public key certificate is involved, the certificate-based (S)DVS schemes bring in massive consumption of certificate management. As to the identity-based (S)DVS schemes, the key escrow problem also causes fatal threats to the users in the scheme. In order to avoid the two inherent flaws mentioned above, the concept of certificateless designated verifier signature scheme is proposed by Huang et al. [6]. Certificateless cryptography is able to avert the utility of public key certificate. Meanwhile, certificateless cryptography ensures the security of user's private key, because the KGC (Key Generation Center) just can get user's partial private key instead of full private key. In this paper, we focus on constructing a certificateless SDVS scheme with non-delegatability.

1.1 Related Works

The notions of DVS and SDVS were firstly proposed by Jakobsson et al. [9] in 1996 and more and more attention was paid to this special signature scheme. In 2003, Saeednia et al. [19] firstly made the formal definition of SDVS and proposed an efficient SDVS scheme without the layer of encryption. In 2004, Susilo et al. [21] introduced the

*These authors contribute equally to this work.

concept of identity-based strong designated verifier signature (IBSDVS) which was built on identity-based cryptography and provided a concrete construction. Because of abandoning the public key certificate, this construction was much more efficient than the certificate-based schemes. As the definition of DVS and SDVS became formalized, some other (S)DVS schemes with new construction methods emerged [7, 10, 18]. Until 2005, Lipmaa et al. [15] figured out a type of attack called delegatability attack on (S)DVS. The general idea of delegatability attack is that the signer and the verifier can illegitimately delegate his ability of signing or verifying to any third party he wants through transferring a common value relating to their private keys to the third party, while the third party disables to extract their private keys from the common value. The proposed delegatability attack makes most of the previous schemes insecure. For the sake of achieving the goal of non-delegatability, [5, 12, 25] were proposed in succession. Unfortunately, Shim et al. [20] figured out the schemes [12, 25] were delegatable and Zhang et al. [26] also proved the scheme [5] was not secure for its delegatability. Recently, Tian et al. proposed a non-delegatable SDVS on elliptic curves [22] and a corresponding identity-based version [23] subsequently. The two schemes were both constructed on the basis of Schnorr digital signature. Until now, they seem to have not been found suffering from the delegatability attack [20].

Appearing later than certificate-based cryptography and identity-based cryptography, certificateless cryptography was firstly proposed by Al-Riyami et al. [1] in 2003. Each user's full private key is constituted by two parts called partial private key and secret value in certificateless cryptography. They are derived from the KGC and the user himself/herself respectively. The user keeps the secret value all the time and the KGC is prohibited from obtaining it. Since the certificateless cryptography was presented relatively late, only several certificateless (S)DVS schemes were proposed [3, 4, 6, 8, 24]. According to the attack methods in [2], the scheme in [6] suffered from malicious KGC attack. Liu et al. [17] proved the scheme [8] also did not resist malicious KGC attack. Furthermore, utilizing the delegatability attack methods based on [20], we find that the above schemes are subjected to delegatability attack due to the leakage of common value in the signature construction.

1.2 Contributions

In this paper, by means of improving the Schnorr digital signature, we construct the first certificateless strong designated verifier signature scheme with non-delegatability. We formally prove the proposed scheme can resist the two types of attack method including public key replacement attack and malicious KGC attack in certificateless cryptography. The security proofs also contain the properties of non-delegatability and source hiding which are necessary properties of an SDVS. To the best of our knowledge, there is no certificateless SDVS satisfying the property of

non-delegatability at present and our scheme is the first one. Besides, We make a comparison with other existing certificateless SDVS schemes to show the proposed scheme possesses a good level of security and performance.

1.3 Organizations

The rest of this paper is organized as follows. In Section 2, we briefly review some preliminaries including bilinear pairings and mathematical problems involved in our scheme. We describe the definition, security properties and adversary model of certificateless SDVS in Section 3. Then in Section 4, we present our certificateless SDVS scheme concretely. Security analysis of the proposed scheme is discussed in Section 5. A comparison of performance and security with other existing certificateless SDVS schemes is in Section 6. Finally, Section 7 concludes this paper.

2 Preliminaries

In this section, we briefly introduce the concept of bilinear pairings [13, 16] and the complexity assumptions involved in the proposed certificateless SDVS scheme.

Assume \mathbb{F}_p is a finite field in which p is a large prime. Choose randomly $a, b \in_R \mathbb{F}_p$ as two elements to define a curve \mathbb{E} . Let \mathbb{G} be an additive cyclic group whose prime order is q , \mathbb{G}_T be a multiplicative cyclic group with the same order and P be a generator of \mathbb{G} .

The mapping $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is an admissible bilinear pairing with the following properties:

Bilinearity: $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$, where $P, Q \in \mathbb{G}$ and $a, b \in_R \mathbb{Z}_q^*$.

Non-degeneracy: There exists $P, Q \in \mathbb{G}$ such that $\hat{e}(P, Q) \neq 1$, which is an identity element of \mathbb{G}_T .

Computability: There must be an efficient algorithm to compute $\hat{e}(P, Q)$ for all $P, Q \in \mathbb{G}$.

Bilinear Diffie-Hellman Problem (BDHP): Given a random instance $(P, aP, bP, cP) \in \mathbb{G}$ for unknown $a, b, c \in \mathbb{Z}_q^*$, it is difficult to compute $\hat{e}(P, P)^{abc}$.

Elliptic Curve Discrete Logarithm Problem (ECDLP): Given two random points $P, Q \in \mathbb{G}$, it is difficult to compute an integer $a \in \mathbb{Z}_q^*$ to satisfy $Q = aP$.

3 Model for the Proposed Certificateless SDVS

3.1 Definition of the Certificateless SDVS

There are two entities in a certificateless SDVS scheme, the real signer Alice and the designated verifier Bob and a certificateless SDVS scheme consists of eight algorithms which are shown below.

Setup: This algorithm takes the security parameter k to output the system parameter sp and the master key s .

Partial-Private-Key-Extract: Given the master key s and the entity's identity id , the KGC generates the entity's partial private key S_{id} .

Set-Secret-Value: The entity chooses randomly a value x_{id} as his/her secret value.

Set-Private-Key: Given the partial private key S_{id} and the secret value x_{id} , the entity outputs his/her full private key sk_{id} .

Set-Public-Key: Given the secret value x_{id} , the public parameter P , this algorithm generates the entity's public key pk_{id} .

Sign: Given the message m , Alice's private key sk_A , Bob's public key pk_B and the system parameter sp , Alice generates the designated verifier signature δ and sends it to Bob.

Verify: Given the message m , Alice's public key pk_A , Bob's private key sk_B , the system parameter sp and the signature δ , Bob outputs *True* if the signature is correct, otherwise outputs \perp .

Transcript-Simulation: Given the message m , Alice's public key pk_A , Bob's private key sk_B and the system parameter sp , Bob generates an indistinguishable designated verifier signature δ' .

3.2 Security Properties of the Certificateless SDVS

- 1) Correctness: If the signer produces a valid SDVS in the signing phase, it must be accepted in the verifying phase successfully.
- 2) Unforgeability: Without the private key of the signer or the designated verifier, it is computationally infeasible to forge a valid SDVS for the third party.
- 3) Source hiding: Given a message-signature pair, the private keys of the signer and the designated verifier, it is computationally infeasible for any polynomial-time distinguisher to determine who is the real signer between the signer and the designated verifier.
- 4) Non-delegatability: If a third party is capable of producing a valid signature, he/she must 'know' the private key of the signer or the designated verifier.

Remark: Especially, we present the significance of the non-delegatability property for a designated verifier signature in real applications briefly. As stated previously, the designated verifier signature can be used in software licensing. In order to prevent the software buyers from selling the software they have bought to other people and

protect the dealers' benefit, the dealers can produce a designated verifier signature binding with the merchandise to the buyers. In this way, only the actual buyer is able to check the validity of signature, namely, the legality of software. We can utilize the scheme in [11] to realize this real application. The *Signing* phase and the *Verifying* phase can be described as follows.

- Signing: the dealer chooses $r \in_R \mathbb{Z}_q$ and computes $U = rQ_A$, $\sigma = H_2(m, e(S_A, rQ_B))$. Then the signature will be (U, σ) .
- Verifying: the buyer checks if $\sigma = H_2(m, e(U, S_B))$ holds or not.

Unfortunately, this scheme can not satisfy the property of non-delegatability because of the common value between the signer and the verifier. The buyer can disclose the common value $e(Q_A, S_B)$ to the third party. Once the third party gets this value, he will be able to check the correction of the equation $\sigma = H_2(m, e(U, S_B))$. Thus, the third party will trust that the software got from the buyer is legal and he will buy it. The non-delegatability can prevent this circumstance from happening perfectly. In the scheme that is equipped with non-delegatability, the common value should not be found.

3.3 Adversary Model of the Certificateless SDVS

There are two types of adversaries proposed by Al-Riyami et al. [1] in certificateless cryptography as follows.

Type 1 Adversary: The adversary can not obtain the master key, namely, the adversary can not obtain the partial private key from the KGC. However, it is capable of replacing the public key of any entity, because there is no public key certificate involved. We can define the attack model as the following game between a challenger C and Type 1 adversary A_1 .

Setup: The challenger C firstly takes the security parameter k to generate the system parameter sp and the master key s . C transfers sp to A_1 and keeps the master key s secret meanwhile.

Queries: The adversary A_1 issues the following queries adaptively for polynomially many times:

- Hash queries: Given a hash query for any input, C returns a result to the adversary A_1 .
- Partial-Private-Key-Extract queries: Given a partial private key query for any user ID_i , C returns a partial private key S_i for the corresponding user ID_i to the adversary A_1 .
- Set-Secret-Value queries: Given a secret value query for any user ID_i , C returns a secret value x_i for the corresponding user ID_i to the adversary A_1 .

- **Public-Key-Extract queries:** Given a public key query for any user ID_i , C returns a public key pk_i for the corresponding user ID_i to the adversary A_1 .
- **Public-Key-Replacement queries:** The adversary A_1 can select a new public key pk'_i for user ID_i to replace the previous public key pk_i . In this way, pk'_i will be the new public key of ID_i .
- **Sign queries:** Given any message m with signer's identity ID_i and designated verifier's identity ID_j , C returns the corresponding signature δ to the adversary A_1 .
- **Verify queries:** The adversary A_1 can ask for the verification of a message-signature pair (m, δ) with the signer's identity ID_i and verifier's identity ID_j , then C executes the verify algorithm and outputs *True* if (m, δ) is valid. Otherwise, C outputs \perp .

Forgery: Finally, A_1 produces a forged message-signature pair (m^*, δ^*) with signer's identity ID_i and verifier's identity ID_j . The adversary A_1 wins the game if

- 1) $Verify(m^*, \delta^*, sk_i, pk_j) \rightarrow 1$;
- 2) A_1 did not issue queries to C on input ID_i and ID_j through Partial-Private-Key-Extract queries, Set-Secret-Value queries or Public-Key-Replacement queries;
- 3) A_1 did not issue queries to C on input ID_i and ID_j to get the certificateless SDVS on m^* through Sign queries.

Type 2 Adversary: The adversary can obtain the master key, namely, the adversary can generate the entity's partial private key from the KGC. Contrary to Type 1 adversary, this adversary is not capable of replacing the public key of any entity. We can define the attack model as the following game between a challenger C and the Type 2 adversary A_2 .

Setup: The challenger C firstly takes the security parameter k to generate the system parameter sp and the master key s . C transfers sp to A_2 and keeps the master key s secret meanwhile.

Queries: The adversary A_2 issues the following queries adaptively for polynomially many times:

- **Hash queries:** Given a hash query for any input, C returns a result to the adversary A_2 .
- **Set-Secret-Value queries:** Given a secret value query for any user ID_i , C returns a secret value x_i for the corresponding user ID_i to the adversary A_2 .
- **Public-Key-Extract queries:** Given a public key query for any user ID_i , C returns a public key pk_i for the corresponding user ID_i to the adversary A_2 .

- **Sign queries:** Given any message m with signer's identity ID_i and designated verifier's identity ID_j , C returns the corresponding signature δ to the adversary A_2 .
- **Verify queries:** The adversary A_2 can ask for the verification of a message-signature pair (m, δ) with signer's identity ID_i and verifier's identity ID_j , then C executes the verify algorithm and outputs *True* if (m, δ) is valid. Otherwise, C outputs \perp .

Forgery: Finally, A_2 produces a forged message-signature pair (m^*, δ^*) with signer's identity ID_i and verifier's identity ID_j . The adversary A_2 wins the game if

- 1) $Verify(m^*, \delta^*, sk_i, pk_j) \rightarrow 1$;
- 2) A_2 did not issue queries to C on input ID_i and ID_j through Partial-Private-Key-Extract queries or Set-Secret-Value queries;
- 3) A_2 did not issue queries to C on input ID_i and ID_j to get the certificateless SDVS on m^* through Sign queries.

4 Our Proposed Scheme

In this section, we specify our certificateless SDVS scheme which is composed of the following eight algorithms.

Setup: Assume \mathbb{F}_p is a finite field in which p is a large prime. Choose randomly $a, b \in_R \mathbb{F}_p$ as two elements to define a curve \mathbb{E} . Let \mathbb{G} be an additive cyclic group whose prime order is q , \mathbb{G}_T be a multiplicative cyclic group with the same order and P be a generator of \mathbb{G} . The mapping $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is an admissible pairing. Let $H_1 : \{0, 1\}^* \rightarrow \mathbb{G}$, $H_2 : \{0, 1\}^* \times \mathbb{G} \rightarrow \mathbb{G}$, $H_3 : \mathbb{G} \times \mathbb{G}_T \rightarrow \mathbb{Z}_q^*$ be three cryptographic hash functions. The system parameter sp is $(\mathbb{F}_p, a, b, P, q, \hat{e}, H_1, H_2, H_3)$, the KGC randomly selects $s \in \mathbb{Z}_q^*$ as master key and keeps it secret.

Partial-Private-Key-Extract: This algorithm accepts an identity $ID_i \in \{0, 1\}^*$, $i \in A, B$ and constructs the partial private key for the user as follows:

- 1) Compute $Q_i = H_1(ID_i)$.
- 2) Output the partial private key $S_i = sQ_i$.

Set-Secret-Value: This user selects a random $x_i \in \mathbb{Z}_q^*$ and outputs x_i , $i \in A, B$ as his/her secret value. That is, the sender Alice randomly selects $x_A \in \mathbb{Z}_q^*$ and the designated verifier Bob randomly selects $x_B \in \mathbb{Z}_q^*$.

Set-Private-Key: The full private key of Alice and Bob will be $sk_A = (x_A, S_A)$ and $sk_B = (x_B, S_B)$.

Set-Public-Key: This algorithm computes $pk_A = x_AP$ and $pk_B = x_BP$ as Alice and Bob's public keys respectively.

Sign: Assume the message is m , then the signer Alice randomly selects $r, l \in \mathbb{Z}_q^*$ and computes

$$\begin{aligned} A &= lP, \\ C_0 &= rP, \\ C_1 &= H_2(m, A) \\ C &= C_0 + C_1 = (c_x, c_y), \\ v &= l + c_x x_A \\ R &= rpk_B, \\ \sigma &= H_3(R, \hat{e}(S_A, Q_B)). \end{aligned}$$

Finally, the signature δ on message m for the designated verifier Bob is (C, v, σ) .

Verify: Once receiving the signature δ , the verifier Bob computes

$$\begin{aligned} A' &= vP - c_x pk_A, \\ C'_1 &= H_2(m, A), \\ C'_0 &= C - C'_1, \\ R' &= x_B C'_0, \\ \sigma' &= H_3(R', \hat{e}(Q_A, S_B)). \end{aligned}$$

Bob accepts the signature δ if and only if the equation $\sigma = \sigma'$ holds.

Transcript-Simulation: The verifier Bob can produce a valid signature δ' intended for himself by executing the following operations: Randomly selects $C \in \mathbb{G}$, $v \in \mathbb{Z}_q^*$ and computes

$$\begin{aligned} A &= vP - c_x pk_A, \\ C_1 &= H_2(m, A), \\ C_0 &= C - C_1, \\ R &= x_B C_0, \\ \sigma &= H_3(R, \hat{e}(Q_A, S_B)). \end{aligned}$$

Then the signature δ' is (C, v, σ) .

5 Security Analysis

5.1 Correctness

The transcript-simulation algorithm is correct obviously and the correctness of the verifying algorithm is validated as follows:

$$\begin{aligned} A' &= vP - c_x pk_A \\ &= (l + c_x s)P - c_x pk_A \\ &= lP + c_x pk_A - c_x pk_A \\ &= lP \\ &= A. \\ R' &= x_B C'_0 \\ &= x_B rP \\ &= rpk_B = R. \end{aligned}$$

5.2 Unforgeability against Type 1 Adversary

Theorem 1. *The proposed certificateless SDVS scheme is existentially unforgeable against Type 1 adversary in the random oracle model under the hardness of BDHP.*

Proof. Assume that A_1 is Type 1 adversary who can forge a valid certificateless SDVS with a non-negligible probability and within the polynomial time t . There exists an algorithm C which treats A_1 as a black box to solve the BDHP with a non-negligible probability. That is, for given a random instance $(P, aP, bP, cP) \in \mathbb{G}$ and for the unknown $a, b, c \in \mathbb{Z}_q^*$, C is able to compute $\hat{e}(P, P)^{abc}$. The game is shown as follows:

Setup: The challenger C firstly takes the security parameter k to generate the system parameter $sp = (\mathbb{F}_p, a, b, P, q, \hat{e}, H_1, H_2, H_3)$ and the master key s . C transfers sp to A_1 and keeps the master key s secret meanwhile.

Queries: The adversary A_1 issues the following queries adaptively for polynomially many times:

- Hash queries to H_1 : Suppose that A_1 can send at most q_{H_1} times H_1 queries and C preserve a list $L_{H_1}^{list}$. The list is used to store the tuple of form (ID_i, Q_i, d_i) and set to be empty initially. C responds as follows if A_1 transfers a H_1 query with ID_i .
 - 1) If $ID_i = ID_A$, return $Q_i = H_1(ID_i) = aP$ to A_1 , then append a new tuple (ID_i, Q_i, \perp) to the list $L_{H_1}^{list}$.
 - 2) Else if $ID_i = ID_B$, return $Q_i = H_1(ID_i) = bP$ to A_1 , then append a new tuple (ID_i, Q_i, \perp) to the list $L_{H_1}^{list}$.
 - 3) Else, return $Q_i = H_1(ID_i) = d_i P$ to A_1 , where $d_i \in \mathbb{Z}_q^*$, then append a new tuple (ID_i, Q_i, d_i) to the list $L_{H_1}^{list}$.
- Partial-Private-Key-Extract queries: The challenger C preserves a list L_{ppke}^{list} composed of the tuple of the form (ID_i, D_i, S_i) . Once receiving a Partial-Private-Key-Extract query on ID_i , C looks up the tuple (ID_i, Q_i, S_i) from L_{ppke}^{list} and responds as follows:
 - 1) If $ID_i \neq ID_A$ and $ID_i \neq ID_B$, C looks up the tuple (ID_i, Q_i, d_i) in the list $L_{H_1}^{list}$. If the tuple exists, C returns $S_i = d_i cP$ to A_1 . Otherwise, C chooses randomly a number $d_i \in \mathbb{Z}_q^*$, then returns $S_i = d_i cP$ to A_1 . Afterwards, C appends (ID_i, Q_i, S_i) to L_{ppke}^{list} .
 - 2) Else if $ID_i = ID_A$ or $ID_i = ID_B$, C terminates the protocol.
- Public-Key-Extract queries: C preserves a list L_{pk}^{list} composed of the tuple of the form

(ID_i, Q_i, pk_i, x_i) . Once A_1 calls a Public-Key-Extract query on ID_i , C looks up the tuple (ID_i, Q_i, pk_i, x_i) from the list L_{pk}^{list} and responds as follows:

- 1) If L_{pk}^{list} includes (ID_i, Q_i, pk_i, x_i) , C returns pk_i to A_1 .
 - 2) Else if, C randomly chooses a value $x_i \in \mathbb{Z}_q^*$, computes $pk_i = x_i P$ and returns pk_i to A_1 , then appends a new tuple (ID_i, Q_i, pk_i, x_i) to L_{pk}^{list} .
- Set-Secret-Value queries: Once receiving a Set-Secret-Value query on ID_i from A_1 , C looks up the tuple (ID_i, Q_i, pk_i, x_i) from the list L_{pk}^{list} . If L_{pk}^{list} includes (ID_i, Q_i, pk_i, x_i) , C returns x_i . Otherwise, C performs a Public-Key-Extract query on x_i to produce (ID_i, Q_i, pk_i, x_i) , returns the secret value x_i to A_1 and appends the tuple to L_{pk}^{list} .
 - Public-Key-Replacement queries: Once receiving a Public-Key-Replacement query on (ID_i, pk'_i) , C looks up the tuple (ID_i, Q_i, pk_i, x_i) from the list L_{pk}^{list} . If the L_{pk}^{list} includes (ID_i, Q_i, pk_i, x_i) , C sets $pk_i = pk'_i$ and updates the tuple $(ID_i, Q_i, pk_i, x_i = \perp)$. Otherwise, C executes a Public-Key-Extract query to produce (ID_i, Q_i, pk_i, x_i) , sets $pk_i = pk'_i$ and updates the tuple $(ID_i, Q_i, pk_i, x_i = \perp)$. Then appends the new tuple $(ID_i, Q_i, pk_i, x_i = \perp)$ to L_{pk}^{list} .
 - Hash queries to H_2 : C preserves a list H_2^{list} composed of the tuple of the form $(m, A \in \mathbb{G}, C_1)$. Once receiving a Hash queries to H_2 on (m_i, A_i) , C executes as follows:
 - 1) if H_2^{list} includes the tuple (m_i, A_i, C_{1i}) , C returns C_{1i} to A_1 as a response.
 - 2) Otherwise, C randomly chooses $C_{1i} \in \mathbb{G}$, sends it to A_1 and appends (m_i, A_i, C_{1i}) to the list H_2^{list} .
 - Hash queries to H_3 : C preserves a list H_3^{list} composed of the tuple of the form $(R \in \mathbb{G}, T \in \mathbb{G}_T, \sigma)$. Once receiving a Hash queries to H_3 on (R_i, T_i) , C executes as follows:
 - 1) if H_3^{list} includes the tuple (R_i, T_i, σ_i) , C returns σ_i to A_1 .
 - 2) Otherwise, C randomly chooses $\sigma_i \in \mathbb{Z}_q^*$, sends it to A_1 and appends (R_i, T_i, σ_i) to the list H_3^{list} .
 - Sign queries: Once receiving a Sign query on input a message m , a signer's identity ID_i and a designated verifier's identity ID_j from A_1 , C responds as follows:
 - 1) If $ID_i \neq ID_A$, or $ID_i \neq ID_B$, C extracts (ID_i, Q_i, S_i) and (ID_i, Q_i, pk_i, x_i) from the list L_{ppke}^{list} and L_{pk}^{list} respectively to

get the signer ID_i 's private key $(x_i, S_i) = (x_i, d_i(cP))$. C randomly selects $r, l \in \mathbb{Z}_q^*$, computes $A = lP$, $C_0 = rP$, $C_1 = H_2(m, A)$, $C = C_0 + C_1 = (c_x, c_y)$, $v = l + c_x x_i$, $R = rpk_j$, $\sigma = H_3(R, \hat{e}(S_i, Q_j))$ to produce the signature (C, v, σ) and returns it to A_1 .

- 2) Else if $ID_j \neq ID_A$, or $ID_j \neq ID_B$, C extracts (ID_j, Q_j, S_j) and (ID_j, Q_j, pk_j, x_j) from the list L_{ppke}^{list} and L_{pk}^{list} respectively. C randomly selects $C \in \mathbb{G}, v \in \mathbb{Z}_q^*$, computes $A = vP - c_x pk_i$, $C_1 = H_2(m, A)$, $C_0 = C - C_1$, $R = x_j C_0$, $\sigma = H_3(R, \hat{e}(Q_i, S_j))$ to produce the signature (C, v, σ) and returns it to A_1 .
- 3) Else, C terminates the protocol.

- Verify queries: Once receiving a Verify query on input a message-signature pair (m, δ) , a signer's identity ID_i and a designated verifier's identity ID_j from A_1 , C responds as follows:

- 1) If $ID_i = ID_A, ID_j = ID_B$ or $ID_i = ID_B, ID_j = ID_A$, C aborts the protocol execution.
- 2) Otherwise, C extracts (ID_j, Q_j, S_j) and (ID_j, Q_j, pk_j, x_j) from the list L_{ppke}^{list} and L_{pk}^{list} respectively to get the designated verifier ID_j 's private key $(x_j, S_j) = (x_j, d_j(cP))$, then validates the signature through the verify algorithm in our proposed scheme.

Forgery: In the end, A_1 produces a valid certificateless SDVS $\delta = (C^*, v^*, \sigma^*)$ on input a chosen message m^* , a signer's identity ID_i and a designated verifier's identity ID_j . If $(ID_i, ID_j) \neq (ID_A, ID_B)$ or $(ID_i, ID_j) \neq (ID_B, ID_A)$, C aborts the protocol execution and outputs *Fail*. Otherwise, C produces a valid signature $\sigma^* = H_3(R^*, \hat{e}(S_A, Q_B))$ for figuring out $\hat{e}(S_A, Q_B) = \hat{e}(acP, bP) = \hat{e}(P, P)^{abc}$. Thus, the BDHP is resolved. Unfortunately, It is infeasible to address the intractable BDHP by any polynomial time algorithm. □

5.3 Unforgeability against Type 2 Adversary

Theorem 2. *The proposed certificateless SDVS scheme is existentially unforgeable against the adversaries 2 in the random oracle model under the hardness of ECDLP.*

Proof. Assume that A_2 is Type 2 adversary who can forge a valid certificateless SDVS with a non-negligible probability and within the polynomial time t . There exists an algorithm C which treats A_2 as a black box to solve the ECDLP with a non-negligible probability. That is, for given two random points $P, Q \in \mathbb{G}$, C is able to compute

Table 1: Notation and description of cryptographic operations

Notation	Description
C_P	Pairing operation
C_S	Scalar multiplication operation in \mathbb{G}
C_H	Hash operation
C_E	Exponentiation operation
C_I	Inversion operation
C_A	Add operation in \mathbb{G}

Table 2: Performance comparison of our scheme with other existing schemes

Schemes	Signature-size	Sign-cost	Verify-cost
Huang et al. [6]	$ \mathbb{Z}_q^* $	$1C_P + 1C_S + 1C_H + 1C_I$	$3C_P + 1C_S + 1C_H$
Chen et al. [3]	$ \mathbb{Z}_q^* $	$1C_P + 1C_S + 1C_H$	$1C_P + 1C_S + 1C_H$
Du et al. [4]	$2 \mathbb{Z}_q^* + \mathbb{G} $	$3C_S + 1C_H + 1C_E$	$2C_P + 3C_S + 1C_H$
Yang et al. [24]	$2 \mathbb{G} $	$1C_P + 4C_S + 1C_H$	$1C_P + 2C_S + 1C_H$
Hafizul et al. [8]	$2 \mathbb{G} $	$3C_P + 3C_S + 2C_H + 1C_E$	$1C_P + 1C_S + 1C_H + 1C_E$
Ours	$2 \mathbb{Z}_q^* + \mathbb{G} $	$1C_P + 3C_S + 2C_H$	$1C_P + 3C_S + 2C_H$

Table 3: Security comparison of our scheme with other existing schemes

Schemes	Non-delegatability	Resilience against Type 1 adversary	Resilience against Type 2 adversary
Huang et al. [6]	NO	YES	NO
Chen et al. [3]	NO	YES	YES
Du et al. [4]	NO	YES	YES
Yang et al. [24]	NO	YES	YES
Hafizul et al. [8]	NO	YES	NO
Ours	YES	YES	YES

an integer $a \in \mathbb{Z}_q^*$ to satisfy $Q = aP$. The game is shown as follows:

Setup: The challenger C firstly takes the security parameter k to generate the system parameter $sp = (\mathbb{F}_p, a, b, P, q, \hat{e}, H_1, H_2, H_3)$ and the master key s . C transfers sp to A_2 and keeps the master key s secret meanwhile.

Queries: The adversary A_2 issues the following queries adaptively for polynomially many times:

- Hash queries to H_1 : C preserves a list H_1^{list} composed of the tuple of the form (ID_i, Q_i, d_i) . Once A_2 issues a Hash queries to H_1 on ID_i , C searches the tuple (ID_i, Q_i, d_i) from the list H_1^{list} . If H_1^{list} includes (ID_i, Q_i, d_i) , C returns the previous value Q_i . Otherwise, C randomly chooses a value $d_i \in \mathbb{Z}_q^*$, returns $Q_i = d_iP$ to A_2 and inserts (ID_i, Q_i, d_i) to the list H_1^{list} .
- Public-Key-Extract queries: C preserves a list L_{pk}^{list} composed of the tuple of the form (ID_i, Q_i, pk_i, x_i) . Once A_2 issues a Public-Key-Extract query on ID_i , C searches the tuple (ID_i, Q_i, pk_i, x_i) from the list L_{pk}^{list} and executes the following steps.

- 1) If L_{pk}^{list} includes (ID_i, Q_i, pk_i, x_i) and

- If $ID_i \neq ID_A, ID_i \neq ID_B$, the challenger C returns the previous value pk_i .
- Else if $ID_i = ID_A$ or $ID_i = ID_B$, the challenger C returns $pk_i = aP$ or $pk_i = bP$ as response and appends a new tuple (ID_i, Q_i, pk_i, \perp) to the list L_{pk}^{list} .

- 2) Else if there does not exist this tuple, C randomly selects a value $x_i \in \mathbb{Z}_q^*$, returns $pk_i = x_iP$ and inserts a new tuple (ID_i, Q_i, pk_i, x_i) to the list L_{pk}^{list} .

- Set-Secret-Value queries: Once A_2 issues a Set-Secret-Value query on ID_i , C searches (ID_i, Q_i, pk_i, x_i) from the list L_{pk}^{list} .

- 1) If L_{pk}^{list} includes (ID_i, Q_i, pk_i, x_i) and
 - If $ID_i \neq ID_A, ID_i \neq ID_B$, the challenger C returns the previous value x_i to A_2 .
 - Else if $ID_i = ID_A$ or $ID_i = ID_B$, C terminates the protocol.

- 2) Else if there does not exist this tuple, C randomly returns a value $x_i \in \mathbb{Z}_q^*$, computes $pk_i = x_iP$ and inserts a new tuple (ID_i, Q_i, pk_i, x_i) to the list L_{pk}^{list} .

- Hash queries to H_2 , Hash queries to H_3 , Sign queries, Verify queries: Since these steps are the

same as the corresponding steps in Theorem 1, we do not make those statements again.

Forgery: In the end, A_2 produces a valid certificateless SDVS $\delta = (C^*, v^*, \sigma^*)$ on input a chosen message m^* , a signer's identity ID_i and a designated verifier's identity ID_j . If $(ID_i, ID_j) \neq (ID_A, ID_B)$ or $(ID_i, ID_j) \neq (ID_B, ID_A)$, C aborts the protocol execution and outputs *Fail*. Otherwise, C produces a valid $v^* = l + c_x x_A$ for figuring out $x_A = pk_A/P$. Thus, the ECDLP is resolved. Unfortunately, It is infeasible to address the intractable ECDLP by any polynomial time algorithm.

□

Theorem 3. *The proposed certificateless SDVS scheme is equipped with the property of source hiding in the random oracle model.*

Proof. Given a message-signature pair (m, δ) , the signer's private key (x_A, S_A) and the designated verifier's private key (x_B, S_B) used in the proposed construction, a third party can not distinguish who is the real signer. The reason is that the following two equations always hold.

$$\begin{aligned} R &= rpk_B = x_B C_0, \\ \sigma &= H_3(R, \hat{e}(S_A, Q_B)) \\ &= H_3(R, \hat{e}(Q_A, S_B)). \end{aligned}$$

Theorem 4. *The proposed certificateless SDVS scheme is equipped with the resistance against delegatability attack in the random oracle model.*

Proof. In our scheme, the signer's secret value x_A and the verifier's secret value x_B are used solely in the signing phase and the verifying phase such that there does not exist disclosing of the common value $(x_A x_B P)$. Although another common value $\hat{e}(S_A, Q_B)$ is possible to be transferred to the third party, the fact that the third party can not figure out the value $v = l + c_x x_A$ prevents the third party from creating a valid signature. The delegatability attack only could happen when the secret value x_A and the common value $\hat{e}(S_A, Q_B)$ are disclosed concurrently, but the probability is negligible. In this situation, it is infeasible for the delegatability attacker to defeat our scheme.

□

6 Comparison

In this section, we present a comparison of the proposed scheme with other existing certificateless SDVS in terms of performance and security. The notations and the corresponding descriptions of cryptographic operations are shown in Table 1. Table 2 is for performance comparison and Table 3 is for security comparison. We assume that the bit length of element in \mathbb{G} is $|\mathbb{G}|$ and the bit

length of element in \mathbb{Z}_q^* is $|\mathbb{Z}_q^*|$. The length of the signature in our scheme is equal to the length in [4], so it is acceptable. Among the cryptographic operations listed in Table 1, pairing operation is recognized as the most time-consuming operation and add operation in \mathbb{G} can be neglected because of its low computational cost. By contrast with the existing schemes, we can see our scheme only requires one pairing operation no matter in the signing phase or in the verifying phase such that the computing consumption of our scheme is at a very low level. Table 3 shows that only our scheme is able to satisfy the three important properties in certificate SDVS scheme simultaneously. In summary, our scheme is relatively efficient and provably secure among the existing schemes.

7 Conclusions

This paper proposes the first certificateless SDVS scheme with non-delegatability. The proposed scheme extends the Schnorr digital signature to a certificateless SDVS. We provide the security proof of the proposed scheme on the basic properties of SDVS. We also prove that our scheme can resist the two types of adversaries in certificateless cryptography. In addition, the comparison with other existing certificateless SDVS shows that our scheme has a higher level of efficiency and security.

Acknowledgments

This work is partially supported by National Natural Science Foundation of China under Grant Nos. 61003230, 61370026, 61300191 and 61272029.

References

- [1] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *9th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT'03)*, pp. 452–473, Taipei, Taiwan, Nov.–Dec. 2003.
- [2] M. H. Au, Y. Mu, J. Chen, D. S. Wong, J. K. Liu, and G. Yang, "Malicious kgc attacks in certificateless cryptography," in *2nd ACM Symposium on Information, Computer and Communications Security (ASIACCS'07)*, pp. 302–311, Singapore, Mar. 2007.
- [3] H. Chen, R. Song, F. Zhang, and F. Song, "An efficient certificateless short designated verifier signature scheme," in *4th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM'08)*, pp. 1–6, Dalian, China, Oct. 2008.
- [4] H. Du and Q. Wen, "Efficient certificateless designated verifier signatures and proxy signatures," *Chinese Journal of Electronics*, vol. 18, no. 1, pp. 95–100, 2009.

- [5] Q. Huang, G. Yang, D. S. Wong, and W. Susilo, "Identity-based strong designated verifier signature revisited," *Journal of Systems and Software*, vol. 84, no. 1, pp. 120–129, 2011.
- [6] X. Huang, W. Susilo, Y. Mu, and F. Zhang, "Certificateless designated verifier signature schemes," in *20th International Conference on Advanced Information Networking and Applications (AINA'06)*, pp. 15–19, Vienna, Austria, Apr. 2006.
- [7] X. Huang, W. Susilo, Y. Mu, and F. Zhang, "Short (identity-based) strong designated verifier signature schemes," in *7th International Conference on Information Security Practice and Experience (ISPEC'11)*, pp. 214–225, Hangzhou, China, May–Jun. 2006.
- [8] S. H. Islam and G. P. Biswas, "Provably secure certificateless strong designated verifier signature scheme based on elliptic curve bilinear pairings," *Journal of King Saud University-Computer and Information Sciences*, vol. 25, no. 1, pp. 51–61, 2013.
- [9] M. Jakobsson, K. Sako, and R. Impagliazzo, "Designated verifier proofs and their applications," in *International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT'96)*, pp. 143–154, Saragossa, Spain, May 1996.
- [10] P. K. Kancharla, S. Gummadidala, and A. Saxena, "Identity based strong designated verifier signature scheme," *Informatika*, vol. 18, no. 2, pp. 239–252, 2007.
- [11] B. Kang, C. Boyd, and E. Dawson, "Identity-based strong designated verifier signature schemes: attacks and new construction," *Computers and Electrical Engineering*, vol. 35, no. 1, pp. 49–53, 2009.
- [12] B. Kang, C. Boyd, and E. D. Dawson, "A novel identity-based strong designated verifier signature scheme," *Journal of Systems and Software*, vol. 82, no. 2, pp. 270–273, 2009.
- [13] A. V. N. Krishna, A. H. Narayana, K. M. Vani, "Window method based cubic spline curve public key cryptography," *International Journal of Electronics and Information Engineering*, vol. 4, no. 2, pp. 94–102, 2016.
- [14] C. T. Li and Hwang M. S. A., "secure and anonymous electronic voting scheme based on key exchange protocol," *International Journal of Security and Its Applications*, vol. 7, no. 1, pp. 59–70, 2009.
- [15] H. Lipmaa, G. Wang, and F. Bao, "Designated verifier signature schemes: attacks, new security notions and a new construction," in *32nd International Colloquium on Automata, Languages and Programming (ICALP'05)*, pp. 459–471, Lisbon, Portugal, July 2005.
- [16] L. Liu and Z. Cao, "A note on efficient algorithms for secure outsourcing of bilinear pairings," *International Journal of Electronics and Information Engineering*, vol. 5, no. 1, pp. 30–36, 2016.
- [17] T. Liu, X. Wang, and X. Ding, "security analysis and improvement of certificateless strong designated verifier signature scheme," *Computer Science*, vol. 40, no. 7, pp. 126–128, 2013 (in Chinese).
- [18] C. Y. Ng, W. Susilo, and Y. Mu, "Universal designated multi verifier signature schemes," in *11th International Conference on Parallel and Distributed Systems (ICPADS'05)*, pp. 305–309, Fukuoka, Japan, July 2005.
- [19] S. Saeednia, S. Kremer, and O. Markowitch, "An efficient strong designated verifier signature scheme," in *6th International Conference on Information Security and Cryptology (ICISC'03)*, pp. 40–54, Seoul, Korea, Nov. 2004.
- [20] K. A. Shim, "On delegatability of designated verifier signature schemes," *Information Sciences*, vol. 281, pp. 365–372, 2014.
- [21] W. Susilo, F. Zhang, and Y. Mu, "Identity-based strong designated verifier signature schemes," in *9th Australasian Conference on Information Security and Privacy (ACISP'04)*, pp. 313–324, Sydney, Australia, July 2004.
- [22] H. Tian, X. Chen, Z. Jiang, and Y. Du, "Non-delegatable strong designated verifier signature on elliptic curves," in *14th International Conference on Information Security and Cryptology (ICISC'11)*, pp. 219–234, Seoul, Korea, Nov.–Dec. 2012.
- [23] H. Tian, X. Chen, F. Zhang, B. Wei, Z. Jiang, and Y. Liu, "A non-delegatable strong designated verifier signature in id-based setting for mobile environment," *Mathematical and Computer Modelling*, vol. 58, no. 5, pp. 1289–1300, 2013.
- [24] B. Yang, Z. Hu, and Z. Xiao, "Efficient certificateless strong designated verifier signature scheme," in *International Conference on Computational Intelligence and Security (CIS'09)*, vol. 1, pp. 432–436, Beijing, China, Dec. 2009.
- [25] J. Zhang and J. Mao, "A novel id-based designated verifier signature scheme," *Information Sciences*, vol. 178, no. 3, pp. 766–773, 2008.
- [26] M. Zhang, T. Takagi, Y. A. N. G. Bo, and L. I. Fagen, "Cryptanalysis of strong designated verifier signature scheme with non-delegatability and non-transferability," *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 95, no. 1, pp. 259–262, 2012.

Biography

Yang Chen is a teaching assistant of Sichuan Aerospace Vocational College. He received his M.S. degree from University of Electronic Science and Technology of China (UESTC). His research covers cryptography and information security.

Yang Zhao is an associate professor at UESTC. His research interests are in the area of networking security and e-commerce protocol.

Hu Xiong is an associate professor at UESTC. He received his Ph.D degree from UESTC in 2009. His research interests include: cryptography and network security.

Feng Yue received his B.S. degree in the School of International Education, Henan University of Science and Technology (HAUST) in 2008. He is currently pursuing his M.S. degree in the School of Computer Science and Engineering, UESTC. His research interests include: cryptography and information security.

COL-MOD: A New Module to Quantify the Weight of Damage Incurred by Collision Attacks

Mina Malekzadeh¹, Moghis Ashroostaghi²

(Corresponding author: Mina Malekzadeh)

Computer Department & Faculty of Electrical and Computer Engineering, Hakim Sabzevari University¹

P. O. Box 379, Tohid Shahr, Sabzevar 9617916487, Iran

Computer Department & Mirdamad Institute of Higher Education, Gorgan, Iran²

(Email: corresponding_m.malekzadeh@hsu.ac.ir)

(Received May 12, 2016; revised and accepted Sept. 3 & Oct. 3, 2016)

Abstract

The wireless technology is inherently susceptible to many types of attacks. There are few studies that have investigated the collision attacks. However, to the best of our knowledge, there is no prior work on investigating the consequences of the collision attacks on performance of the wireless networks. Hence, this work proposes a new module specifically for NS2 simulator which is capable of implementing and measuring the impact of the collision attacks on performance of the functional wireless networks. With the same conditions, we further design a testbed to measure the effectiveness of the collision attacks in real networks. Finally, in order to prove the accuracy of the proposed module, its results are compared with the results from the testbed. The purpose is to accurately determine the impact of the collision attacks which is essential for evaluation and testing the potential defense appliances against the attack. The results signify the extensive impact of the attack on disrupting the normal operation of the wireless networks.

Keywords: Collision attacks, NS2 module, wireless testbed, Ubuntu attacks

1 Introduction

Despite offering many benefits, wireless networks are exposed to many types of attacks including Collision attacks [3]. In collision attack, the attackers do not follow the rules implied in the Medium Access Control (MAC) protocol. Based on the MAC protocol, a collision occurs when two distinct transmissions happen simultaneously on the same media. When the packets collide, they are discarded and the retransmissions are required [1]. The attackers exploit the MAC protocol to launch the collision attacks. They deliberately induce collisions to the target media even by sending small packets [10]. Adversaries may only need to induce a collision in one octet of

a transmission to disrupt the packet. Huge retransmission rate of the legitimate lost packets can severely slow down the victims normal operation and eventually render it unavailable for the intended users [12].

In this work, we provide an attempt to determine the severity and effectiveness of the collision attacks on IEEE802.11n MAC layer of the wireless networks. A new module called COL-MOD is created for NS2 tool to simulate a wireless network environment in which the collision attacks are implemented under different scenarios. Furthermore, a testbed is set up to implement the same attacks under the same scenarios against real wireless network. The purpose of the testbed is to validate the accuracy of the simulation results in term of how close the testbed results are to the simulation results.

The rest of the paper is organized as follows. Section 2 reviews the related researches. Section 3 describes both our proposed testbed setup and simulation environment. We present and analyze the experimental results in Section 4. We conclude this paper in Section 5.

2 Related Works

The Communications between the end users in wireless networks involve transmission of the signals through the open-air which exposes the wireless networks to a variety of attacks [11, 14] including collision attacks [2]. In [15] the authors attempt to detect some attacks including Jamming, exhaustion, and flooding. However, collision attacks are not considered. In [5] the authors consider two attacks called sinking behavior and collision behavior. However, they do not evaluate their findings in real world. Additionally, network topology, metrics, and types of attacks are the other parameters that differ from our work.

Impact of e-DoS attacks on energy consumption level of the targets is investigated in [13]. An energy model is designed to examine the impact of the attack on different

layers of the protocol stack. However, the impact of collision attacks on performance of the wireless networks is not investigated. In [6], the authors use GloMoSim tool to simulate smurf attack which they consider as a type of DDoS attack. However, no testbed confirms the accuracy of the findings. The network security is also discussed in [4, 7, 8, 9].

Most of the previous studies show that the capacity of the DoS attacks seems endless to disable processing of the users requests. However, these studies only enable a limited investigation of the security policy problems associated with DoS attacks and cannot provide in-depth investigations in quantifying impact and severity of the collision attacks. Hence, as the primary contribution of this work, we build on these earlier approaches and extend them particularly by implementing the collision attacks against the IEEE 80.11n wireless networks. By modeling a simulation environment a testbed environment, the main motive is to precisely measure the damage created by the collision attacks and provide a careful comparison of the results from the simulation and the testbed experiments with different attack scenarios and system parameters. This will aid ISPs and network administrators in their evaluation and analysis of the effectiveness of the collision defenses applications.

3 Experimental Setup

In this section, we describe both our proposed simulation environment and testbed setup along with the tools that we have utilized to conduct the collision attacks against the IEEE802.11n wireless networks.

3.1 COL-MOD Module

In order to precisely determine the amount of damage produced by the collision attacks, we first need to quantify the baseline operation of the network which is referred to the network state at which there is no on-going attack. Therefore, by using NS2, we design a simulation environment.

In the baseline case, a wireless network topology with five legal nodes (numbered from 0 to 4), operates under normal conditions. Then we construct a new module and call it COL-MOD with different scalable capabilities to directly implement the collision attacks. We equip the attacker (node5) with the COL-MOD module to be capable of conducting the collision attacks against the target (node0 which also has the router functionality role). The simulation topology is shown in Figure 1.

The total simulation time is 60 seconds which is divided into three 20 seconds. The first 20 seconds (0-19s) is the normal duration at which the target wireless network operates normally. Then, the attacker launches the collision attacks for 20 seconds (20-39s). Finally, the last 20 seconds (40-60s) shows the network states after termination of the attacks. The DSDV routing protocol is used

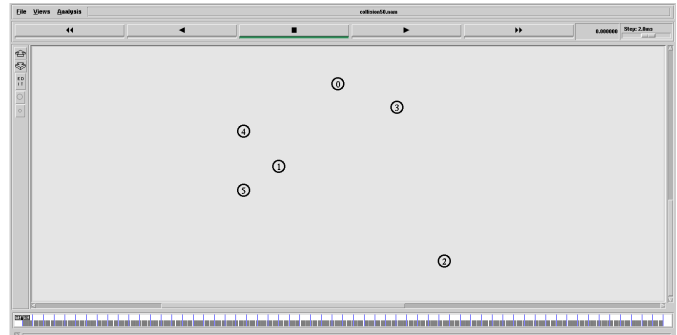


Figure 1: Simulation topology environment

in the simulation environment to establish and maintain the route between the users.

3.2 Testbed Architecture

To achieve the same behavior and a level of control comparable to our simulation, we setup a wireless testbed with the exact same topology as our simulation environment. The network observation duration in the testbed, like the simulation, is 60 seconds. In our testbed, like the simulation, the node0 (which is also switched with a wireless access point during our experiments) is considered as the target of the attacker.

In order to start collision attacks, some preparations in terms of software and hardware are required. The list of software and hardware used in our testbed to conduct the collision attacks are described in Table 1.

3.3 Experiments Setting

The effectiveness of the collision attacks depends on different parameters. Thus, to determine how varying these parameters can influence the success rate of the attack, we take into account the following parameters.

- Legitimate traffics in the simulation experiments: this parameter describes the communication patterns in the target network. In our simulation, the legitimate traffics are created by a CBR UDP agent that continuously sends 500 bytes packets at regular 0.02s intervals. .
- Attack traffics in the simulation experiments: we can also call this feature as attack density or attack frequency. It describes the attributes of the malicious packets arriving at the victim. The goal is to determine the corresponding possible effects on the victim machines involved in the attack. In our simulation, the attack traffics are generated by a CBR agent that pulses three different packet sizes 50B, 100B, and 500B, at three different intervals, 0.05s, 0.02s, and 0.01s.
- Legitimate traffics in the testbed experiments: to achieve a fair comparison with the simulation envi-

ronment, the packets with the exact characteristics (500 bytes at 0.02s intervals) are transmitted into the testbed.

- Attack traffics in testbed experiments: to achieve the same behavior, the attacks are conducted in our testbed with the same specifications as our simulation. Therefore, three different packet sizes (50B, 100B, 500B), at three different packet intervals (0.05s, 0.02s, 0.01s) are generated and injected to the victim in our testbed.

Considering the combination of the above parameters, this research will generate different attack scenarios based on the following three key variables.

Table 1: Preparations for the testbed

Tools	Name	Description
Software	Kali Linux with Builtin Metasploit framework and Nmap	Penetration tool that we use for packet crafting which is prerequisite for launching the collision attacks.
	Wireshark	Network analyzer to examine the network state before, during, and after the collision attacks.
	Operating system	Ubuntu Linux and Windows 7 with default security configurations are used as the OS of the nodes in the target network to examine if the type of OS has any role on survivability of the networks under the collision attacks.
Hardware	Wireless router	Linksys, Asus
	Wireless NIC	Netgear, Atheros chipsets
	CPU	Netgear, Intel; i7, dual core
	RAM	2GB, 4GB

- Type of targets: two factors are aimed to select the victim of the collision attacks in our testbed to test their possible resilience to the attacks. These factors include OS of the target (either Windows or Linux) and role of the target machine (either a computer or access point).
- Security level of the targets: in the real world, different level of protection is provided for the systems and machines in the networks. Considering this fact, we implement the collision attacks in our testbed against the target with a pre-installed antivirus (brand remains unmentioned). Furthermore, we do these attack experiments against Windows-based machines with and without Windows Firewall (WF) configuration respectively. The experiments without WF validate the effectiveness of the collision attacks against this OS, and those with WF investigate the effectiveness of WF to provide a level of protection against these attacks.
- Attack rate: due to the attackers malicious intentions, they typically desire to remain anonymous. Therefore, the attackers generally conduct their attack in a low rate which has two advantages: (1) making it difficult to be detected and (2) consuming less resource of the attackers wireless equipments. Therefore, this work focuses on low rate collision attacks which are achieved by small attack packets size and rate. For this reason, we have set these parameters relatively low as mentioned above in the attack traffics features.

Finally, metrics including throughput, delay, and data lost rate are measured to show divergence during the collision attacks from the baseline case. Therefore, this research generates six distinct experiments as the attack scenarios based on the above parameters, key variables, and metrics. A description of each experiment for the simulation and testbed is summarized in Table 2 and Table 3 respectively.

Table 2: Simulation experiments designed to conduct collision attacks

Parameter	Description
Experiment numbers	Experiment 1 (Attack interval=0.05s)
	Experiment 3 (Attack interval=0.02s)
	Experiment 5 (Attack interval=0.01s)
Attack packet size	50,100,500B

Table 3: Testbed experiments designed to conduct collision attacks

Parameter	Description
Experiment numbers	Experiment 2 (Attack interval=0.05s)
	Experiment 4 (Attack interval=0.02s)
	Experiment 6 (Attack interval=0.01s)
Attack packet size	50,100,500B
Target OS	Windows 7 and Ubuntu 11
Target machine	PC and Access Point
Level of Security	with antivirus and with/without WF

4 Results and Analysis

In this section we present the simulation results and testbed results obtained from implementation of the six experiments.

4.1 Experiment-1

In this experiment, the COL-MOD module runs the collision attacks against the target wireless network in our simulation environment. The normal 500 bytes data enters the wireless network during the entire simulation time i.e. since the beginning of the simulation (0s) until the end (60s). Meanwhile, at the 20th second, the COL-MOD starts the collision attacks using 50,100,500 bytes as the Attack Packet Size (APS) at 0.05s intervals. The attack lasts for 20 seconds (20-39s). The time 40-60s represents the network state after the termination of the attacks. The simulation results of this experiment in terms of throughput, delay, and packet lost are presented in Figure 2.

As the above simulation results show, the consequence of the attack with very low rate (0.05s) is insignificant even with larger attack packets (500B). Comparing the effect of the three sizes of the attack packets on throughput imply relatively similar impact for the smaller packets (50 and 100B). In these cases, the attack does not have noticeable impact on the throughput but delay increases

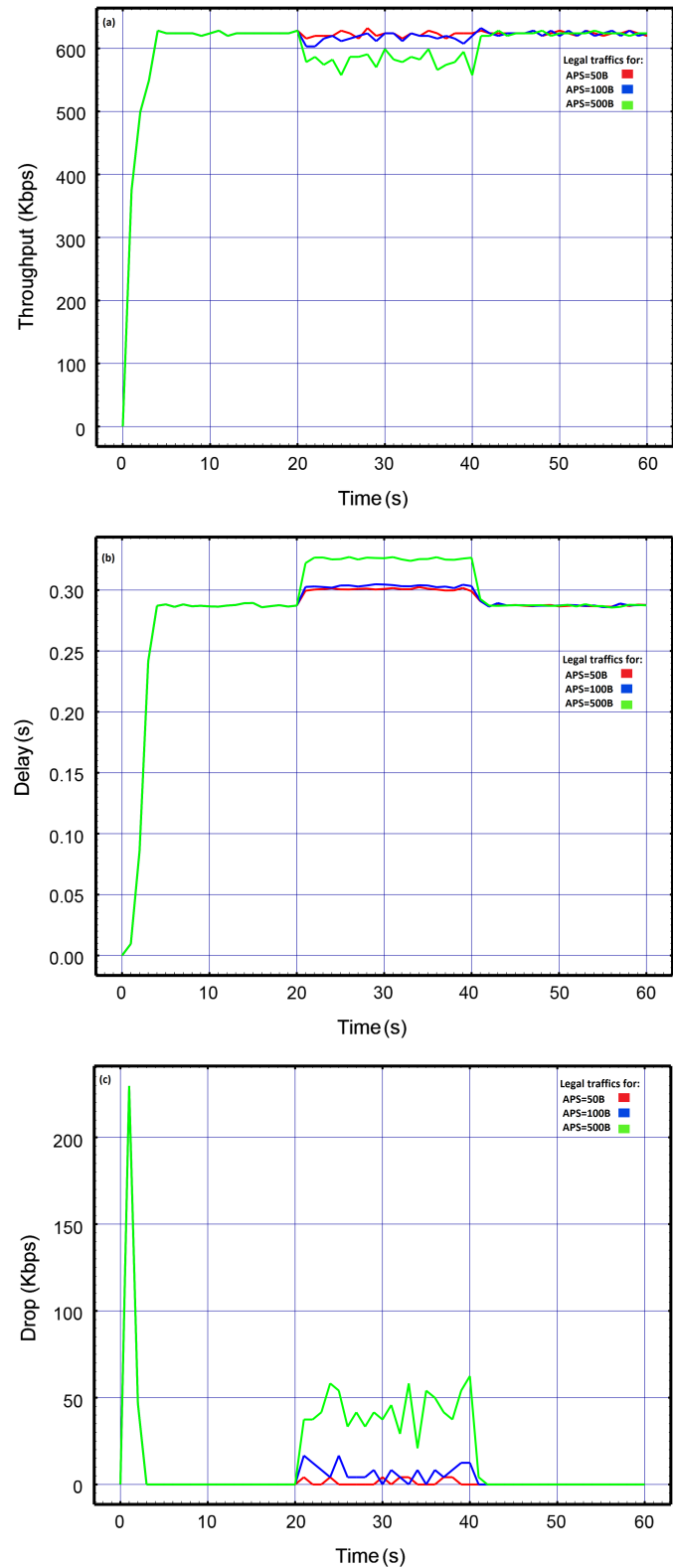


Figure 2: Simulation results: throughput, delay, packet lost

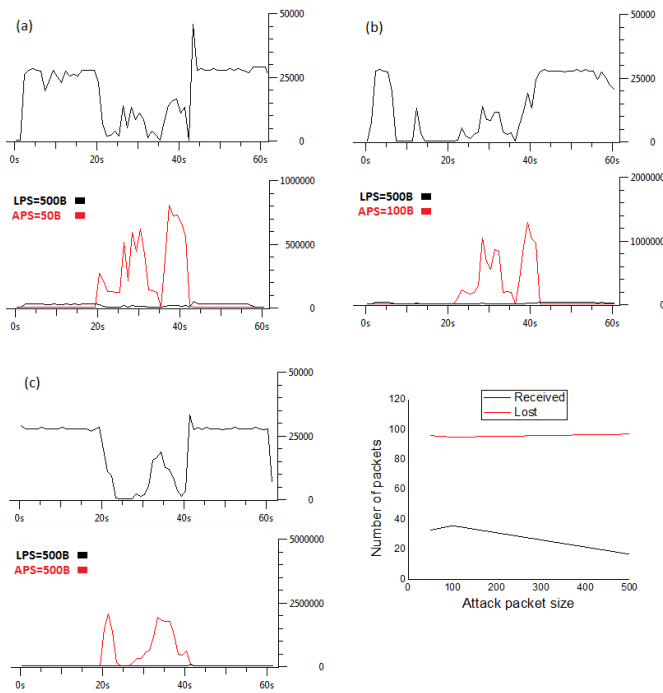


Figure 3: Testbed results on Windows target: throughput, packet lost

slightly. The sudden high peak in the lost packets graph is related to the transmission of the routing control packets by the DSDV protocol at the beginning of the route establishment. As it is depicted, the attack with 500B packets causes higher rate of the dropped packets than the smaller packets.

4.2 Experiment-2

In this experiment, the collision attacks run against the target wireless network in our testbed. The purpose is to measure the impact of the attacks in the real world to be compared against the simulation results obtained by COL-MOD from the Experiment1. The throughput results on the Windows-based victim machine with an installed and updated antivirus while the WF is enabled are provided in Figure 3.

The above results prove significant impact of the attack in the real world. Before the attack, normal data is transmitted steadily over the target network. However, as the attacks start at the 20th second, the attack packets collide with the normal traffics and the throughput fluctuates highly particularly by the 500 bytes attack packets. Although the network is highly affected by the attack, but after the attack (40-60s), the network is able to quickly recover from the attacks.

To determine whether the WF in active mode can provide any level of protection to prevent the collision attack in compare to when it is disabled, we repeat the above experiment with 500B attack packets and disabled WF. The results are provided in Figure 4.

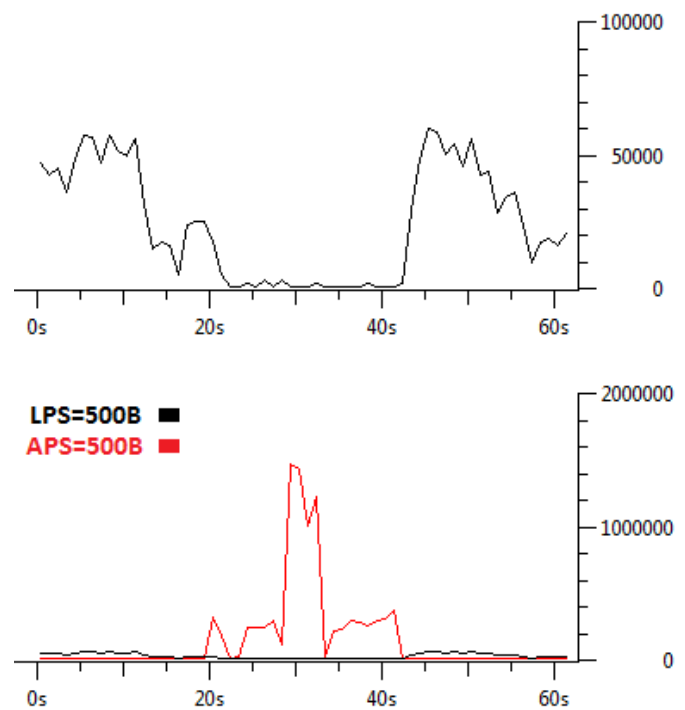


Figure 4: Testbed throughput with WF off

After we disabled the WF, the results confirm vulnerability of the Windows7-based machines to collision attacks regardless of presence or absence of the WF. In both cases the attack is completely destructive while when the WF is disabled there is a higher performance reduction. The results prove that even with small attack interval (0.05s), the attack packets collide with the legitimate packets and force them to drop. The null throughput during the attack signifies the great disturbance compelled by the attack to the wireless network to fully shut it down.

In order to investigate the impact of the same attacks on Linux-based machines, we conduct the above attacks over the target Ubuntu machine in our testbed. The throughput and packet lost results are provided in Figure 5.

The above results signify the high impact of the collision attack on Linux-based target even at a very low rate. As the results suggest, there is slight difference in term of the attack influence between the three sizes of the attack packets. Therefore, when targeting the Linux-based machines, the attackers even with very small 50B packets can interfere with the normal network transmissions and force them to drop. Comparing the above results with the results from targeting the Windows-based machines proves that without presence of the WF both OSs have comparable vulnerability to the collision attacks. However, enabling the WF makes the Windows-based machines to a small extent more resilience to the attacks with attributes tested in this experiment.

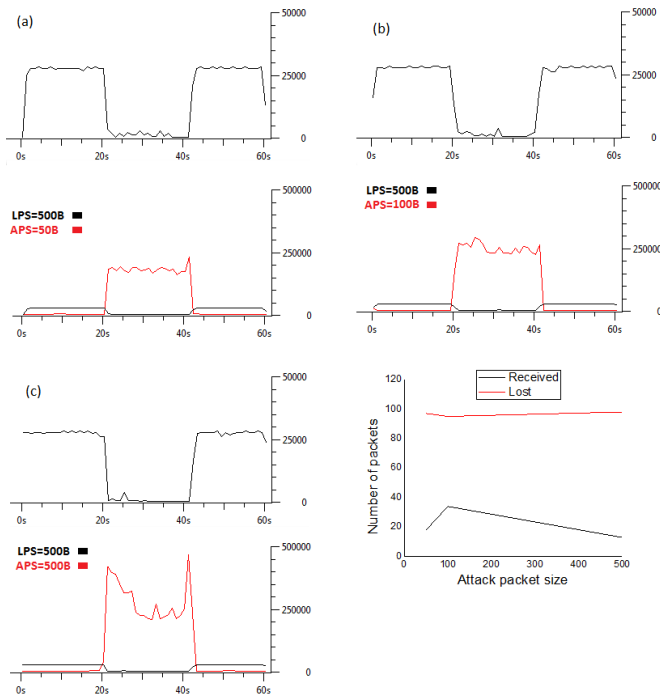


Figure 5: Testbed results on Linux target: throughput, packet lost

4.3 Experiment-3

In this experiment the COL-MOD runs the collision attack, with the corresponding details listed in Table2, against the target wireless network in our simulation environment. The simulation results in terms of throughput, delay, and packet lost rate are presented in Figure 6.

In the above simulation results, throughput falls from 610Kbps down to 490Kbps while the legitimate packets experience higher delay during the entire attack time. As mentioned, the steep rise at the beginning of the simulation in the packet lost graph is corresponding to the DSDV control packets to establish the route. The number of lost packets fluctuates significantly from zero before the attack to about 130Kbps during the attack which points out the effectiveness of the attack.

4.4 Experiment-4

Based on the corresponding attributes listed in Table3, this experiment makes an attempt to run the collision attacks against the target wireless network in our testbed. The throughput and packet lost results on Windows-based target machine with an installed and updated antivirus while the WF is enabled are provided in Figure 7.

The above outcomes prove the collision attacks can substantially disrupt the normal operation of the targets. The reason is related to vulnerabilities in TCP/IP processing. Therefore, even though victims are protected with high level of security, the attacks impact is significant. We observed that the attacks slow down the legiti-

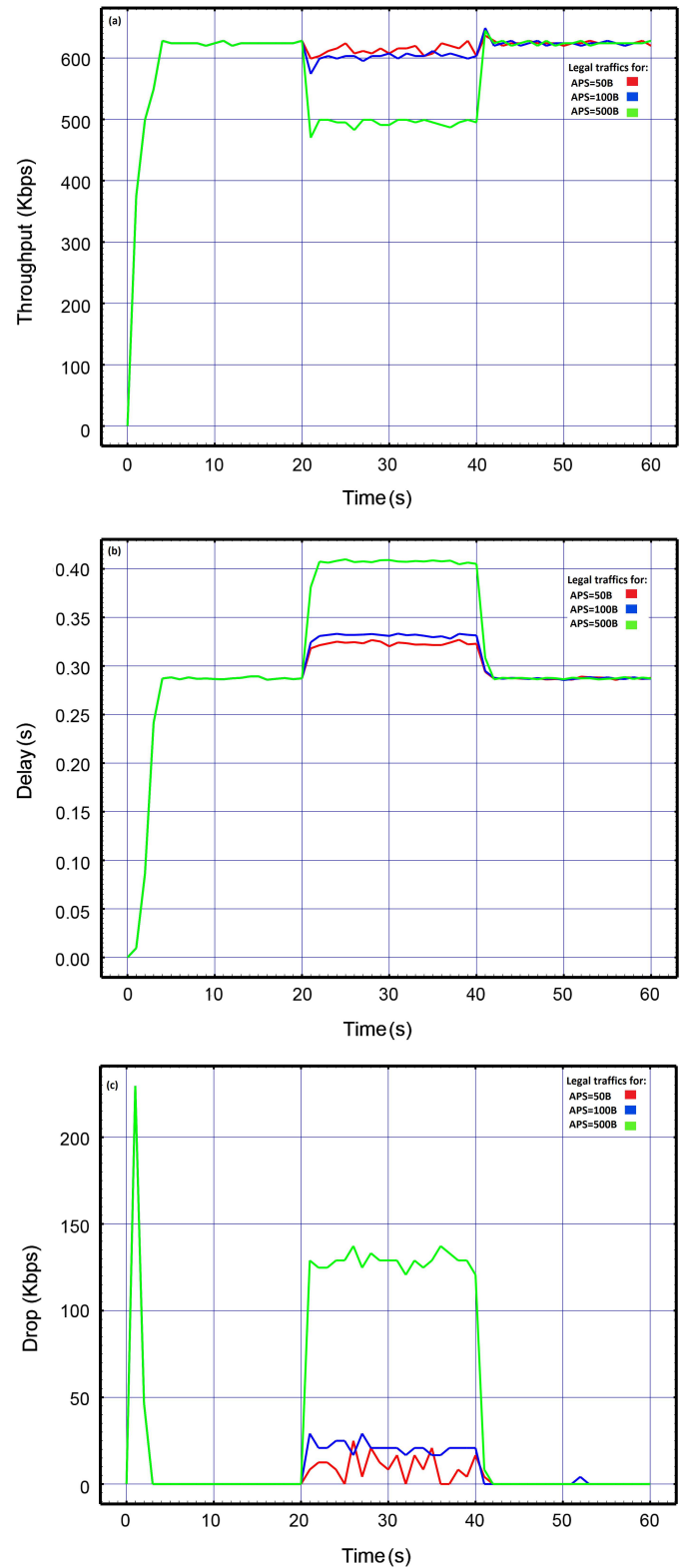


Figure 6: Simulation results: throughput, delay, packet lost

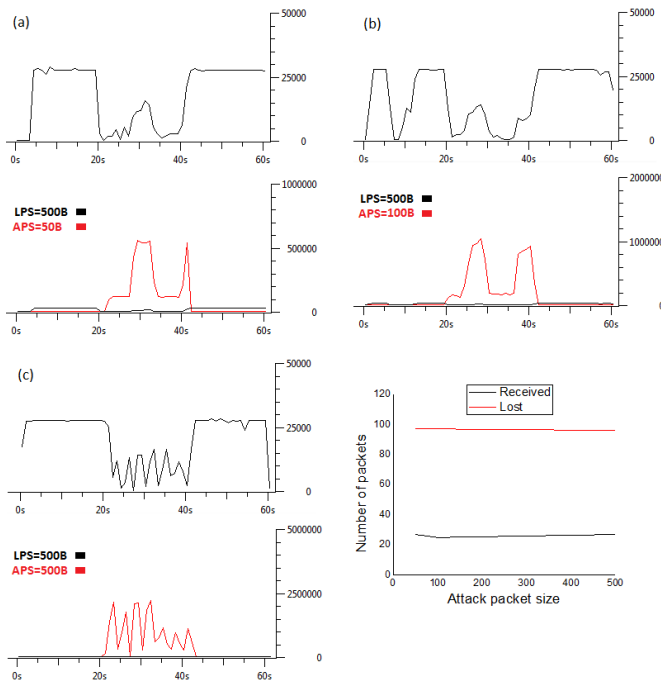


Figure 7: Testbed results on Windows target: throughput, packet lost

mate transmission rate so that even doing a simple task, for instance opening a webpage, was not possible. However, the target network was able to accomplish a fast recovery after the attacks.

In order to determine whether the WF had any effect on these results, we turned the WF off and repeated the above experiment for 500B attack packets. The results are presented in Figure 8.

The above results imply that disabling the WF can thoroughly open the network for penetration of the intruders. The null throughput during the attack reveals the significance of the attack. Using WF does not necessarily nullify the attack, but it has slight effect to reduce the impact.

Severely reduction of the throughput during the attack against the Windows-based machines motives our intention to test the same attack against the Linux-based target. The results of the attack against the Ubuntu target machine are presented in Figure 9.

The above outcomes provide evidence that the attack is quite successful against the target. We observed that, although the Ubuntu machine was not completely disconnected from the network, it was extremely slow to a level that from a practical point of view it was quite inaccessible for the intended users.

4.5 Experiment-5

In this experiment, the COL-MOD runs the collision attacks against the target wireless network in our simulation environment. The rate of the attack rises to a higher

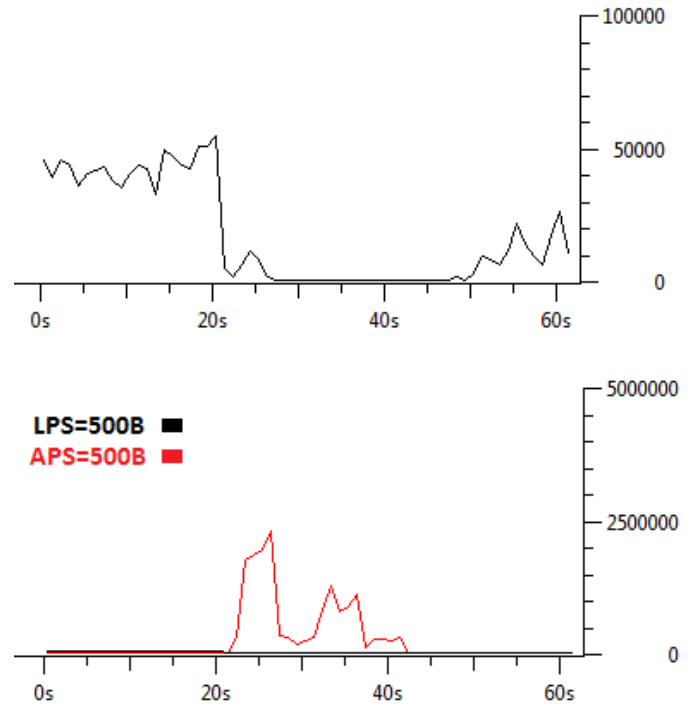


Figure 8: Testbed throughput with WF off

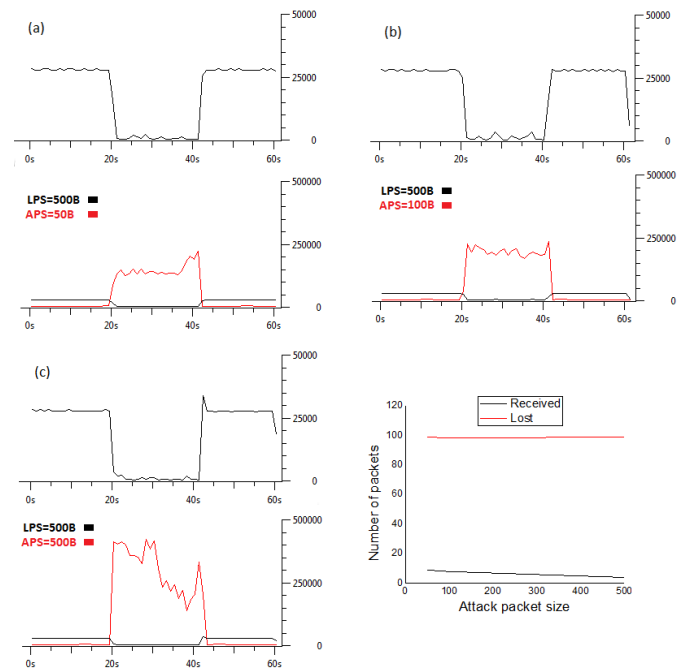


Figure 9: Testbed results on Linux target: throughput, packet lost

value (0.01s) than the previous experiments to examine any possible effects on the targets. The simulation results of this experiment in terms of throughput, delay, and packet lost rate are presented in Figure 10.

The above outcomes illustrate that in the simulation environment there is a direct relation between the attack rate and size of the attack packets on the impact of the attacks. As the attack rate grows to 0.01s, the network performance degrades severely in terms of lower throughput and higher delay and packet lost. Based on the results, the target suffers from a remarkable poor activity when the 500B attack packets are headed toward it.

4.6 Experiment-6

We run this experiment against the target in our testbed to determine the impact of 0.01s intervals between the attack packets on the performance of the target. The throughput and packet lost results on the Windows-based target with an installed and updated antivirus while the WF is enabled are provided in Figure 11.

The above results also confirm the significant impact of the collision attack on degrading the performance of the wireless networks even when protected by firewall and high level of security. At the beginning of the attack, the windows-based target can manage the collisions and the corresponding retransmissions. However, eventually the large numbers of retransmission of the legitimate packets that collide with the forgery packets consume the limited resources of the target which result in a remarkable performance reduction.

In order to see how disabling the WF varies the effect of the attack, we repeated the above attack against the Windows target machine with WF off in our testbed. The results for 500B attack packets are presented in Figure 12.

As we expected from our previous testbed experiments, disabling the WF exposes the network to the attackers. Null throughput during this experiment represents a 100% success rate for the attack.

The above experiment is repeated in order to determine the impact of the attack on Linux-based machines. The throughput and packet lost results are provided in Figure 13.

The above findings also reveal that the Ubuntu machine is fully vulnerable to the attack regardless of the size of the attack packets.

In order to complete our work, we repeated all the above testbed experiments against the wireless access point as the target to see whether it causes any changes on the impact of the attacks. The attacks results on the testbed reveal the same destructive impact on the overall performance of the wireless network.

5 Conclusions

By comparing the testbed and COL-MOD results against each other we can find some differences for the collision at-

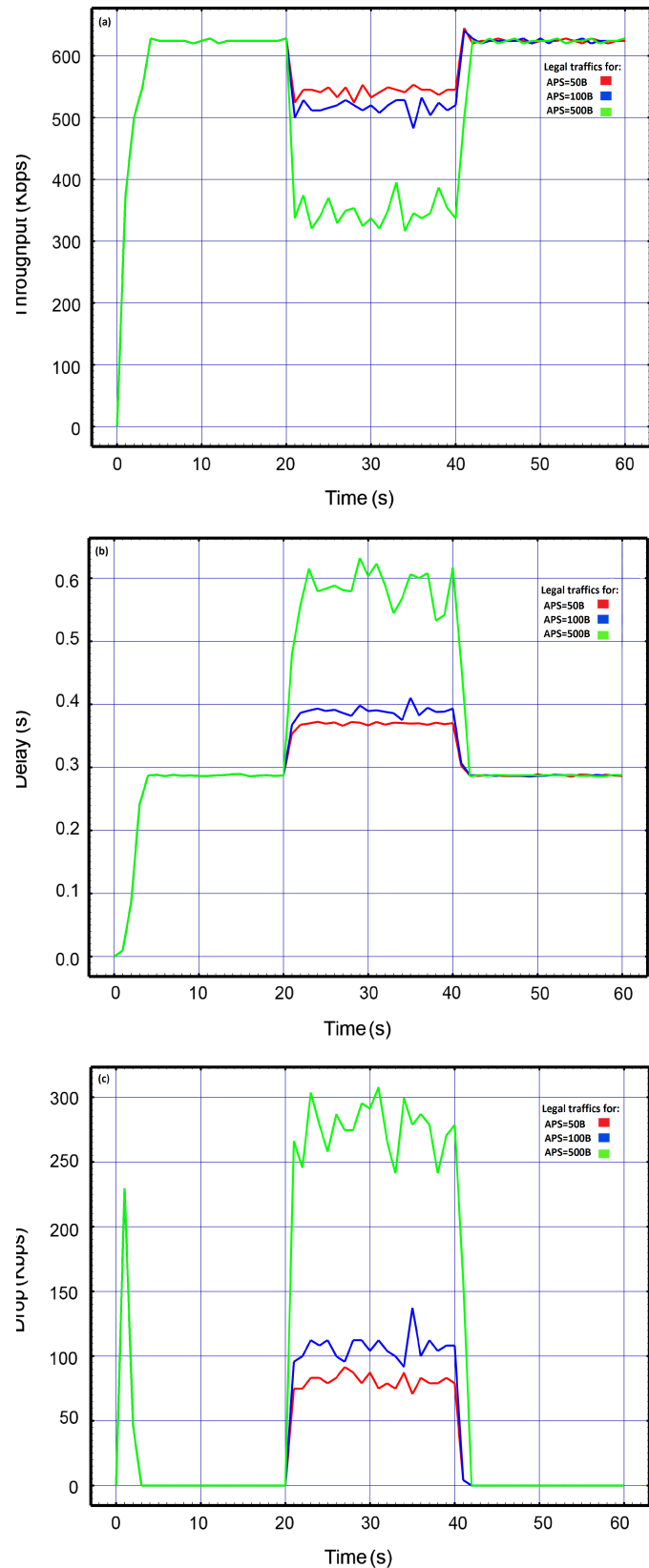


Figure 10: Simulation results: throughput, delay, packet lost

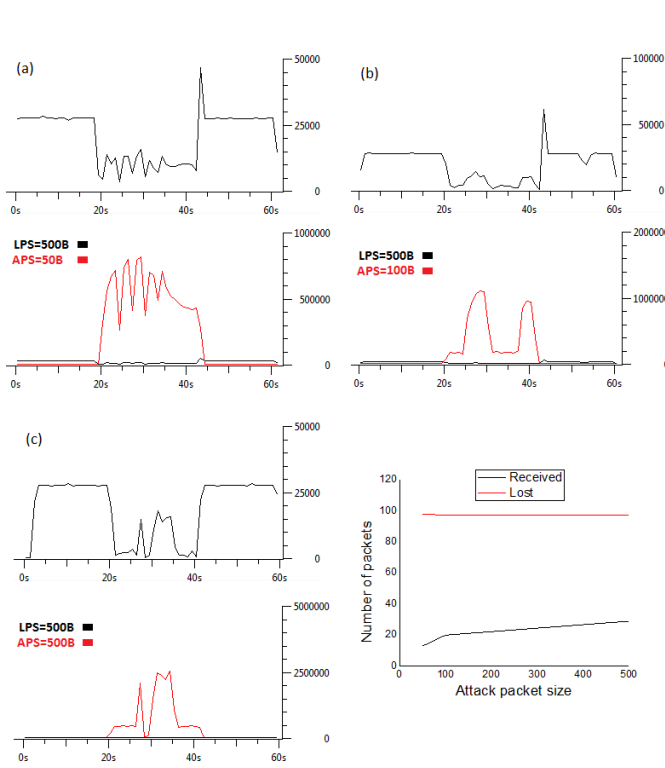


Figure 11: Testbed results on Windows target: throughput, packet lost

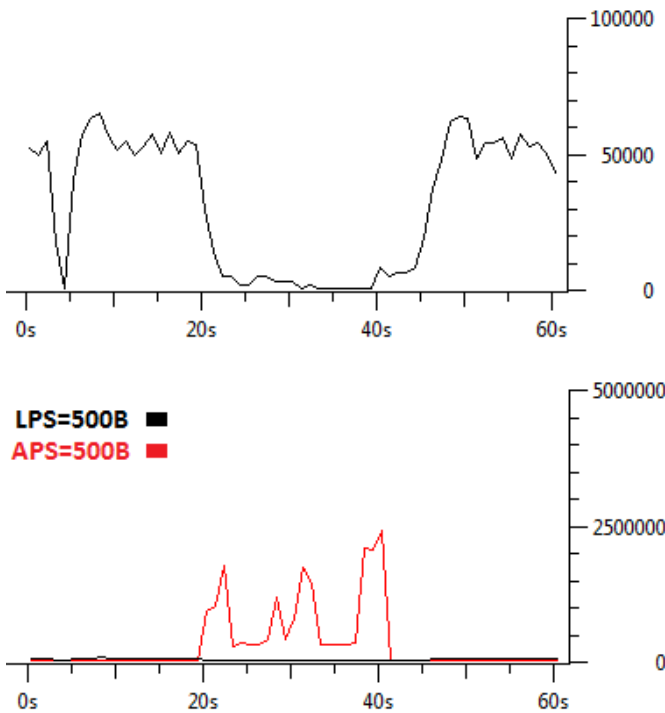


Figure 12: Testbed throughput with WF off

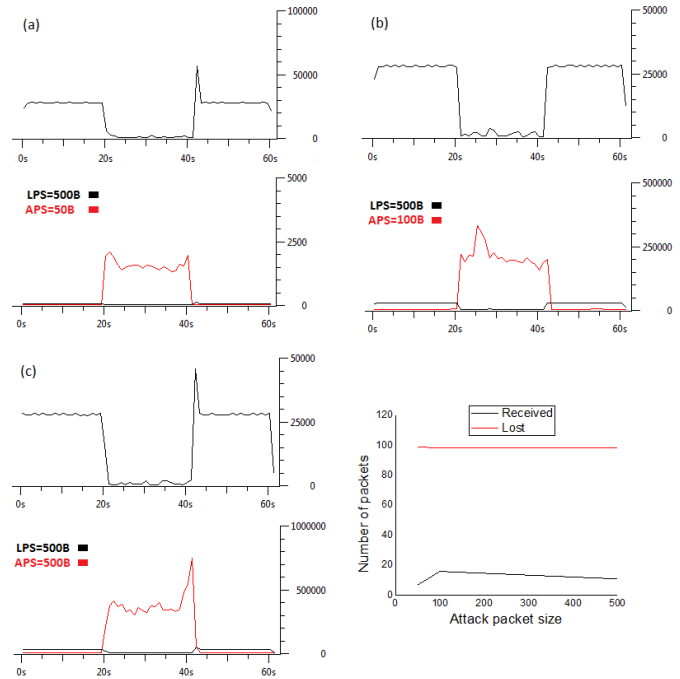


Figure 13: Testbed results on Linux target: throughput, packet lost

tacks. The testbed results show that all the attacks with attributes specified in this work are successful. Based on these results, all the attacks in the real world cause great disturbance and slow down or stop the normal operation of the target network. The collision attacks against the Windows-based machines with enabled WF cause to dramatically slow down the network. Moreover, the collision attacks against either the Linux-based machines or Windows-based machines with disabled WF were fully capable of rendering the targets shut down. The network behavior was relatively the same for all the attacks against the testbed.

In contrast, the COL-MOD module simulation results of the same attacks under the exact same conditions show a different behavior in some scenarios. For example, growing the attacks rate or size has a direct impact on significance of the attacks. We believe this difference between the testbed and simulation results is because the impact of a given attack on a real target network further depends on various network characteristics including its traffic and resources which are not precisely taken into account by the simulation tools.

References

- [1] M. R. Ahmed, X. Huang, and D. Sharma, "A taxonomy of internal attacks in wireless sensor network," *International Journal of World Academy Of Science, Engineering And Technology*, vol. 6, no. 2, pp. 427–430, 2012.

- [2] Z. Cao, C. Mao, L. Liu, "Analysis of one secure anti-collusion data sharing scheme for dynamic groups in the cloud," *International Journal of Electronics and Information Engineering*, vol. 5, no. 2, pp. 68–72, 2016.
- [3] H. C. Chaudhari and L. U. Kadam, "Wireless sensor networks: Security, attacks and challenges," *International Journal of Networking*, vol. 1, no. 1, pp. 4–16, 2011.
- [4] J. Han, "Fingerprint authentication schemes for mobile devices," *International Journal of Electrical and Computer Engineering*, vol. 5, no. 3, pp. 579–585, 2015.
- [5] S. Hemalatha, P. C. S. Mahesh, P. Rodrigues, and M. Raveendiran, "Analysing cross layer performance based on sinking and collision behaviour attack in manet," in *International Conference on Radar, Communication and Computing*, pp. 77–82, 2012.
- [6] M. Kumar and N. Kumar, "Detection and prevention of ddos attack in manets using disable ip broadcast technique," *International Journal of Application or Innovation in Engineering & Management*, vol. 2, no. 7, pp. 29–36, 2013.
- [7] P. H. Latha and R. Vasantha, "Mds-wlan: Maximal data security in wlan for resisting potential threats," *International Journal of Electrical and Computer Engineering*, vol. 5, no. 4, pp. 859–868, 2015.
- [8] N. Mohd, S. Annapurna, and H. S. Bhadauria, "Taxonomy on security attacks on self configurable networks," *International Journal of Electronics and Information Engineering*, vol. 3, no. 1, pp. 44–52, 2015.
- [9] E. U. Opara and O. A. Soluade, "Straddling the next cyber frontier: The empirical analysis on network security, exploits, and vulnerabilities," *International Journal of Electronics and Information Engineering*, vol. 3, no. 1, pp. 10–18, 2015.
- [10] P. Reindl, K. Nygard, and X. Du, "Defending malicious collision attacks in wireless sensor networks," in *IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, pp. 771–776, 2010.
- [11] D. Subhadrabandhu, S. Sarkar, and F. Anjum, "Efficacy of misuse detection in adhoc networks," in *First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (SECON'04)*, pp. 1–11, 2004.
- [12] M. N. Sudha and M. L. Valarmathi, "Minimization of collision in energy constrained wireless sensor network," *International Journal of Wireless Sensor Network*, vol. 1, pp. 350–357, 2009.
- [13] W. West and E. Agu, "Experimental evaluation of energy-based denial-of service attacks in wireless networks," *International Journal of Computer Science and Network Security*, vol. 7, no. 6, pp. 222–236, 2007.
- [14] A. D. Wood and J. A. Stankovic, *A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks, Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, CRC Press LLC, 2005.
- [15] O. Xi and X. Yang, "A novel framework of defense system against dos attacks in wireless sensor networks," in *IEEE International Conference on Wireless Communications, Networking and Mobile Computing (WiCom'11)*, pp. 1–5, 2011.

Biography

Mina Malekzadeh is an assistant professor and lecturer in the department of computer science at Hakim Sabzevari University. Her research interests include communication networks, network security, VoIP, and system development programming. She holds a Doctoral degree in computer security from UPM, MSc in software engineering from UPM, BSc in computer engineering from SBU.

Moghis Ashrotaghi received the B.S. degree in Computer Science from Golestan University. He is currently a master student. His research interests are Computer Networks and wireless security.

Chaotic Map Based Random Image Steganography Using LSB Technique

Sujarani Rajendran¹, Manivannan Doraipandian²

(Corresponding author: Sujarani Rajendran)

Department of Computer Science & Engineering, SASTRA University¹

Kumbakonam - 612001, Tamilnadu, India

(Email: rsujarani@src.sastra.edu)

School of Computing, SASTRA University²

Tirumalaisamudram Thanjavur-613401, Tamilnadu, India

(Received June 28, 2016; revised and accepted Sept. 3 & Sept. 25, 2016)

Abstract

Steganography play an important role to transfer secret data over insecure network. Moreover digital images are taken as a cover to communicate the sensitive data. One of the simplest approach of embedding the secret data into cover image is Least Significant Bit (LSB) method. This paper aims to propose a new symmetric key based image hiding technique. Pseudo random keys are generated by using 1D logistic map and those keys are used for choosing the pixel position of cover image randomly for hiding the secret image. The main security part of the projected method is the selection of pixel position in the cover image. Peak Signal Noise Ratio (PSNR) and Mean Square Error (MSE) measures are used for comparison and the result analysis shows that the proposed scheme provide efficient level of security.

Keywords: Chaos, image hiding, logistic map, steganography

1 Introduction

In today's communication technology images are playing a vital role in all fields such as military, social network, biometric system and so on. Sensitive images are transferred over insecure network, hiding those images from the intruders is an intellectual task. Steganography and cryptography are the two techniques which provide secure data communication. In cryptography secret images are converted into encrypted form and transferred over the networks. In steganography secret image are hidden in other multimedia carriers such as digital audio, video and images [7]. The encrypted form of images explicitly indicate that some sensitive images are transferred but in steganography secret images are hidden inside an another normal image so even attacker visualize the image he may not identify about the secret image. The

traditional mechanism used for hiding the data is watermarking which embed the secret data into cover image [8], then the cover image is considered as stego-image. It act as medium to transfer the secret image over unsecure networks. Two different styles of using the cover image for hiding the secret images are spatial domain and frequency domain [1].

In spatial domain intensity values of cover image are used to hide the secret information [19, 20]. In frequency domain, the secret image pixels are hidden in transforming coefficients values of the pixels in cover image [18, 21]. Different methods of spatial domain steganography techniques has been proposed using Watermarking [9], Least Significant Bit (LSB) substitution [2], Modulus function [6], Pixel Value Differencing method [16, 23], LSB matching [11, 14] and optimal pixel adjustment process [3]. Among these LSB substitution based hiding is one of the simple, fast hiding technology and also it provide efficient security. The proposed scheme utilized the LSB substitution technique for hiding the secret image [5]. In LSB based embedding technique the set of LSB of pixels in cover image are substituted by the bits of secret image. This process can be done either in sequential or in random manner. Randomly chosen pixels for hiding in cover image provide better security than sequential manner [17]. In our proposed scheme cover image pixels are select randomly by using the chaotic sequence generated by the chaotic map.

Chaos means a state of disorder. In mathematics, map is an evolution function that shows some sort of chaotic behavior [10]. A discrete time dynamical system is also called map. chaotic map has some inherent features [13] such as: 1) sensitive to initial conditions (also called butterfly effect) which means a small modification in initial conditions should produce high deviations of the corresponding output. 2) Ergodicity implies the output has the same distribution for any input. 3) Deterministic means a deterministic process can cause a pseudo-random behav-

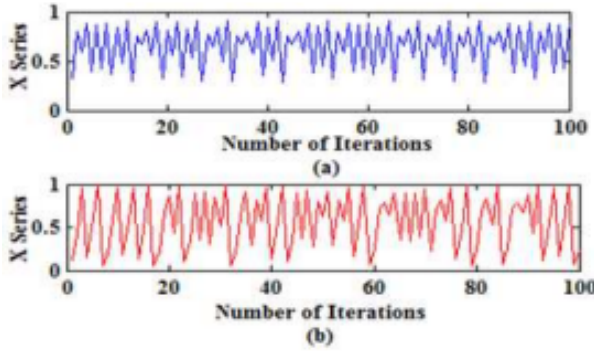


Figure 1: Randomness of 1D logistic map chaotic series
(a) $\alpha = 3.95$ and $x_0 = 0.12$ (b) $\alpha = 3.85$ and $x_0 = 0.25$

ior. 4) Structure complexity signifies a simple mathematical function has very high complexity. Different types of information hiding scheme has been proposed used chaotic sequence [13]. In our proposed scheme we have used One Dimensional (1D) logistic map for generating the chaotic sequence, which is used for selecting the pixel values randomly for hiding in cover image.

The remaining section of the paper is structured as follows: brief description of one dimensional logistic map has discussed on Section 2. Embedding algorithm proposed for hiding the secret image has illuminated in Section 3. Experimental result and result analysis are discoursed in Section 4. Conclusion of the paper declared in Section 5.

2 One Dimentional Logistic Map

It is the simplest form of chaotic system, which is developed by May [15]. Logistic map is described in Equation (1).

$$X_n = \alpha X_{n-1}(1 - X_{n-1}). \quad (1)$$

Here x_0 is initial value and n value denotes the number of rounds. 1D logistic map generate chaotic sequences only if the α value must be in the range of $3.5 \leq \alpha \leq 4$ [22]. It produce chaotic sequences within the range $[0, 1]$. Chaotic sequences generated by a map is greatly sensitive to initial values, a small variation in these parameters will affect the extraction of secret image from cover image, because by using these chaotic sequence only, the position of pixels in cover image are chosen for embedding the bits of secret image. For illustration, the plot diagram for the chaotic sequence generated by 1D logistic map by using the values $\alpha = 3.95$ and $x_0 = 0.12$ is given in Figure 1(a). Tiny changes in the initial parameters of 1D logistic map provide different chaotic sequence, we changed the value of α and x_0 as 3.97 and 0.15 and the plot diagram of the chaotic sequence of the changed values are given in Figure 1(b). From the figure it is clear that the tiny changes in the initial values will greatly affect the values of chaotic series.

3 Proposed Image Hiding Technique

The overall view of the proposed steganography technique is shown in Figure 2.

3.1 Embedding Process

Step by step procedure of the proposed steganography technique is illustrated below.

Step 1: Select the secret image S and cover image C , size of C must be double the size of S .

Step 2: Choose the initial value and system parameter value such as α and x_0 of 1D logistic map for generating the chaotic sequence.

$$X = \{x_1, x_2, x_3, \dots, x_n\}$$

where n is the row or column size of cover image.

Step 3: Sort the generated chaotic sequence X as follows.

$$[sx_i, ax_i] = \text{sort}(X_i), i = 1, 2, 3, \dots, N,$$

where sx is a new sorted sequence of X ; ax is a new index value of the series X .

Step 4: Convert the secret image and cover image in binary format. Binary images are represented as S' and C' .

Step 5: The binary value of secret image S' are divided into four separate two bits and each two bits are stored in separate two dimensional array S'' which is equal to the size of the cover image.

Step 6: Algorithm for embedding process is described as follows:

$S'' (M \times N)$ - Two bits representation of secret image;

$C' (M \times N)$ - Eight bits representation of cover image, where M and N denotes rows and columns of the images.

For i = 1: M

For j = 1: N

$C''(M \times N)$ = Replaced 2-LSB of cover image $C'(M, ax_j)$ into $S''(M, N)$

End

End

Step 7: Convert the binary format of cover image C'' into 8-bit grayscale pixel value then C'' is considered as stego-image.

Hence, secret image has embedded in to cover image and finally the stego-image is transferred to the receiver. Sender securely communicates the secret key and α value to the receiver.

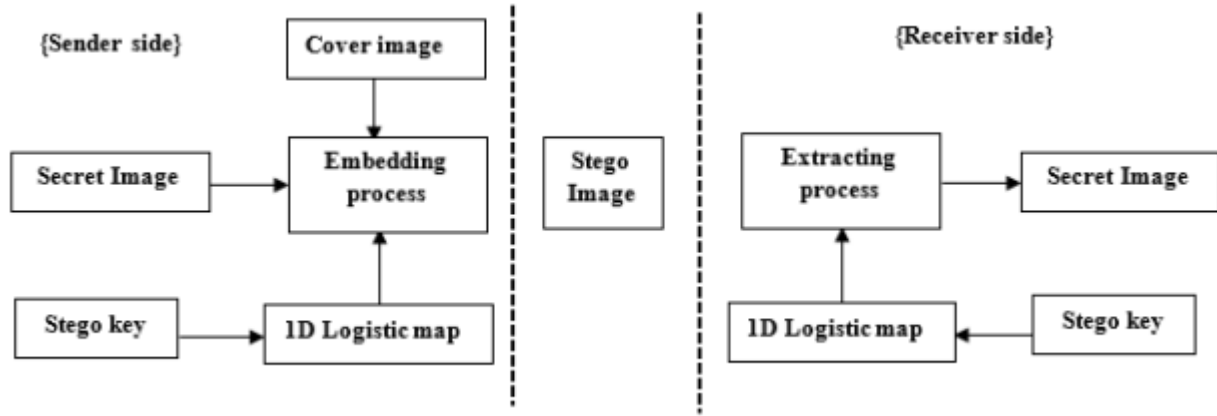


Figure 2: Overall block view of the proposed steganography algorithm

3.2 Extraction Process

Step 1: Generate the chaotic sequence using 1D logistic map and sort it by using the same procedure in embedding process. After sorting new index value (ax) is obtained, which is used for extracting the bits in random manner.

Step 2: Convert the 8-bit pixel value of stego-image C' in to binary form C' .

Step 3: Extraction of secret image from stego-image $C'(M \times N)$ M and N are rows and columns of stego-image.

Step 4: Extracting bits from stego-image.

For $i = 1: M$

For $j = 1: N$

$ES'(M \times N) = \text{Extract 2 LSB from } C'(M, ax_i)$
 $//ES = \text{Extracted Stego-Image}$

End

End

Step 5: Combining the four separate 2 bits in S' into 8-bit so $ES'(M \times N)$ transferred in to $ES''(I \times J)$, where $I = M/2$ and $J = N/2$.

Step 6: Convert the 8-bit binary form Extracted secret image ES'' into 8-bit pixel value and finally the secret image ES is extracted from the stego-image.

(PSNR) and MSE are the standard measures for finding the difference between the original cover image and the stego-image. High PSNR value represents that the cover image has small distortion after embedding. Low PSNR value indicates poor visual quality of the cover image. PSNR is defined in the following Equation (2).

$$PSNR = 10 \log_{10} \left(\frac{255^2}{MSE} \right), \quad (2)$$

where $MSE = \frac{1}{M \times N} \sum_{i=1}^N \sum_{j=1}^M (C_{i,j} - S_{i,j})^2$; MSE stands for Mean Square Error; C represents the original cover image; S represents the Stego image.

Table 1 list the PSNR comparison of proposed technique with other proposed methods. For comparison Boat image has used as secret image and Table 2 shows the comparison of MSE with different proposed scheme, house image has taken as secret image for MSE comparison. Based on the result analysis given in Tables 1 and 2 the proposed technique has better visual quality and less distortion than other techniques.

3.3 Experimental Result and Discussion

The proposed technique performance has evaluated by using different experiments. Four images with (256x256) size are used as cover images shown in Figure 3. The secret images has used for hiding of size (128x128) are shown in Figure 4. For implementation MATLAB (R2013a) has used on Windows 8. Secret image embedded on the LSB of pixels in cover image, selection of pixels for hiding in cover image has done by using the chaotic sequence generated by the 1D logistic map. Peak Signal to noise ratio

Table 1: PSNR value of different cover images after hiding the Boat image

Cover image	Basic LSB Hiding	Method given in Ref [12]	PSO Method Ref [4]	Hide 4 MSB in Ref [4]	Proposed Method
Lena	35.40	35.84	36.29	38.98	44.53
Baboon	35.61	36.14	36.64	39.29	44.54
Airplane	35.70	36.08	36.41	39.19	44.42
Elaine	35.55	36.02	36.20	39.36	44.53

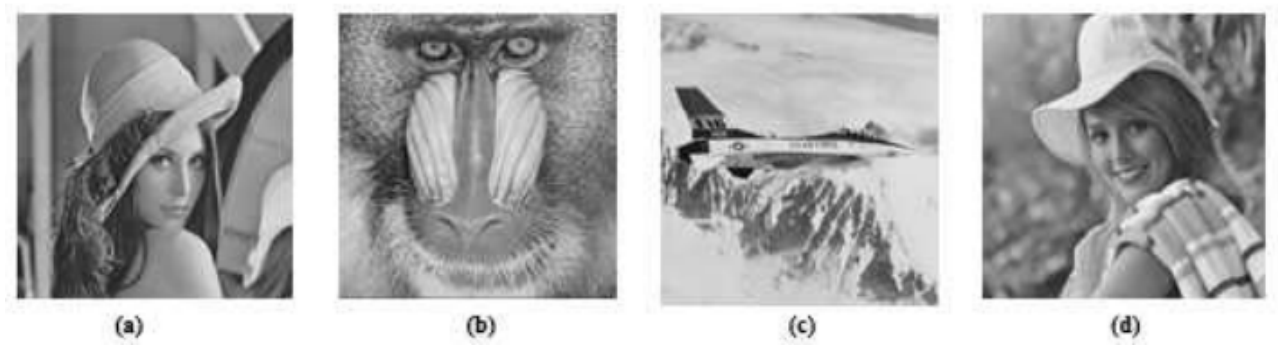


Figure 3: Standard 256 x 256 cover images (a) Lena (b) Baboon (c) airplane (d) Elaine



Figure 4: Standard 128 x 128 Secret images (a) Boat (b) House

Table 2: MSE value of different cover images after hiding the Boat image

Cover image	Basic LSB Hiding	Method given in Ref [12]	PSO Method Ref [4]	Hide 4 MSB in Ref [4]	Proposed Method
Lena	18.36	17.01	15.75	10.85	2.28
Baboon	17.51	15.89	14.59	9.68	2.28
Airplane	17.32	15.47	14.42	10.13	2.34
Elaine	17.55	16.09	15.73	9.78	2.28

Figure 5 Illustrates the graph format result of the PSNR and MSE comparison of different cover images and with different existing proposed techniques, it depicts that the proposed steganography technique has better visual quality than other proposed scheme.

3.4 Histogram Analysis

Histogram shows the exact occurrence of each pixels in the image. High similarity between the cover image histogram and stego image histogram shows that a tiny distortion occurred after embedding the secret image into cover image [22]. Figure 6(a) shows the histogram of cover image Lena and Figure 6(b) shows histogram after embedding the boat image into Lena image. As a result the proposed scheme fight against visual attack and statistical attack.

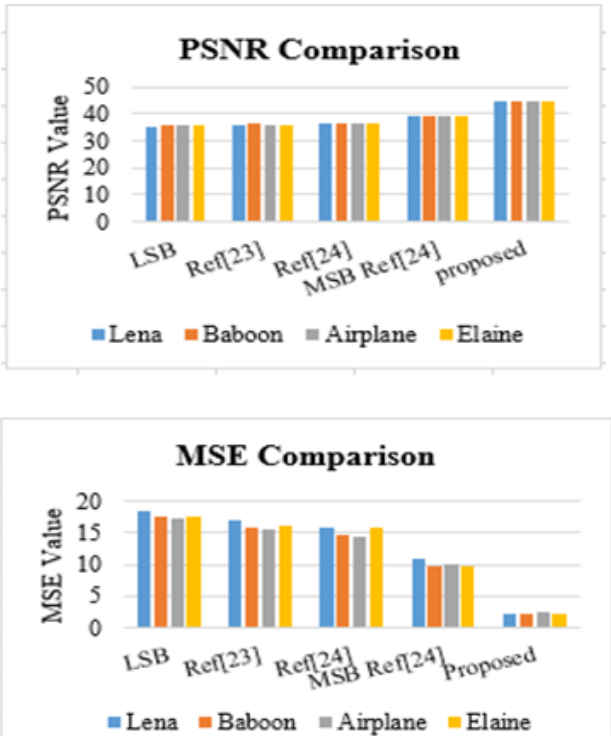


Figure 5: comparison chart (a) PSNR Values of Stego images (b) MSE values of Stego images

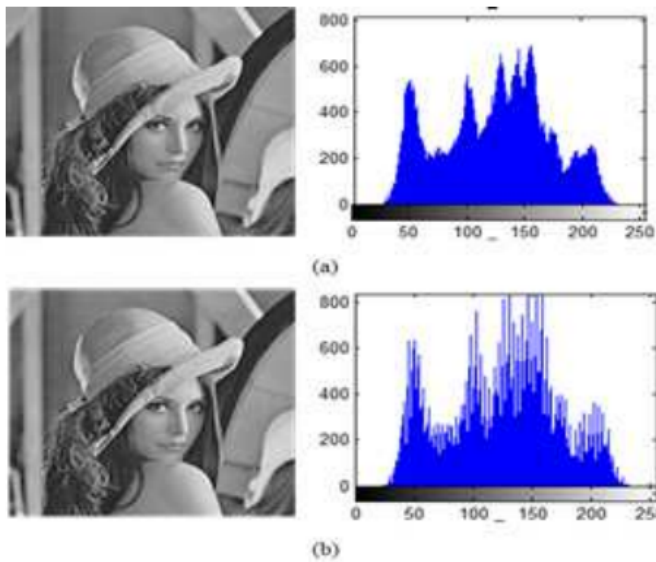


Figure 6: Histogram analysis (a) cover image (b) Stego image

4 Conclusion and Future Work

A new chaotic series based image hiding scheme has proposed by using 1D logistic map. Cover image pixel position has chosen randomly for embedding the secret image bits, so it minimize the security risk and increase the efficiency of the proposed algorithm. Four different grayscale images are used for testing to prove the performance, image quality and capacity of the proposed scheme. Comparison result proved that the proposed scheme provide better result than other steganography schemes. In future the proposed algorithm can also be used for securely transferring and storing the medical images.

References

- [1] R. Amirtharajan and J. B. B. Rayappan, "An intelligent chaotic embedding approach to enhance stego-image quality," *Information Sciences*, vol. 193, pp. 115–124, 2012.
- [2] R. Amirtharajan, R. Subrahmanyam, J. N. Teja, K. M. Reddy, and J. B. B. Rayappan, "Pixel indicated triple layer: A way for random image steganography," *Research Journal of Information Technology*, vol. 5, no. 2, pp. 87–99, 2013.
- [3] O. Banimelhem, M. Mowafi, M. Al-Batati, et al., "A more secure image hiding scheme using pixel adjustment and genetic algorithm," *International Journal of Information Security and Privacy*, vol. 7, no. 3, pp. 1–15, 2013.
- [4] P. Bedi, R. Bansal, and P. Sehgal, "Using pso in image hiding scheme based on lsb substitution," in *International Conference on Advances in Computing and Communications*, pp. 259–268, 2011.
- [5] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," *Pattern Recognition*, vol. 37, no. 3, pp. 469–474, 2004.
- [6] C. S. Chan, C. C. Chang, and Yu-C. Hu, "Image hiding scheme using modulus function and optimal substitution table," *Pattern Recognition and Image Analysis*, vol. 16, no. 2, pp. 208–217, 2006.
- [7] C. C. Chang, T. S. Nguyen, and C. C. Lin, "Reversible image hiding for high image quality based on histogram shifting and local complexity," *International Journal of Network Security*, vol. 16, no. 3, pp. 201–213, 2014.
- [8] H. Chen, X. Du, Z. Liu, and C. Yang, "Optical color image hiding scheme by using gerchberg–saxton algorithm in fractional fourier domain," *Optics and Lasers in Engineering*, vol. 66, pp. 144–151, 2015.
- [9] D. Essaidani, H. Seddik, and E. B. Braiek, "Asynchronous invariant digital image watermarking in radon field for resistant encrypted watermark," *International Journal of Network Security*, vol. 18, no. 1, pp. 19–32, 2016.
- [10] M. François, T. Grosge, D. Barchiesi, and R. Erra, "Pseudo-random number generator based on mixing of three chaotic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 4, pp. 887–895, 2014.
- [11] B. Jana, "Dual image based reversible data hiding scheme using weighted matrix," *International Journal of Electronics and Information Engineering*, vol. 5, no. 1, pp. 6–19, 2016.
- [12] M. Khodaei and K. Faez, "Image hiding by using genetic algorithm and lsb substitution," in *International Conference on Image and Signal Processing*, pp. 404–411, Springer, 2010.
- [13] Z. Liu and L. Xi, "Image information hiding encryption using chaotic sequence," in *International Conference on Knowledge-Based and Intelligent Information and Engineering Systems*, pp. 202–208, Springer, 2007.
- [14] T. C. Lu, C. Ya Tseng, and J. H. Wu, "Dual imaging-based reversible hiding technique using lsb matching," *Signal Processing*, vol. 108, pp. 77–89, 2015.
- [15] R. M. May, et al., "Simple mathematical models with very complicated dynamics," *Nature*, vol. 261, no. 5560, pp. 459–467, 1976.
- [16] S. Manoharan, D. RajKumar, "Pixel value differencing method based on CMYK colour model," *International Journal of Electronics and Information Engineering*, vol. 5, no. 1, pp. 37–46, 2016.
- [17] A. N. Pisarchik and M. Zanin, "Chaotic map cryptography and security," *International Journal of Computer Research*, vol. 19, no. 1, p. 49, 2012.
- [18] S. A. Seyyedi, V. Sadau, and N. Ivanov, "A secure steganography method based on integer lifting wavelet transform," *International Journal of Network Security*, vol. 18, no. 1, pp. 124–132, 2016.
- [19] Y. Yu Tsai, J. T. Chen, and C. S. Chan, "Exploring lsb substitution and pixel-value differencing

for block-based adaptive data hiding,” *International Journal of Network Security*, vol. 16, no. 5, pp. 363–368, 2014.

- [20] S. M. C. Vigila and K. Muneeswaran, “Hiding of confidential data in spatial domain images using image interpolation,” *International Journal of Network Security*, vol. 17, no. 6, pp. 722–727, 2015.
- [21] O. Wahballa, A. Wahaballa, F. Li, and C. Xu, “A secure and robust certificateless public key steganography based on svd-ddwt,” *International Journal of Network Security*, vol. 18, no. 5, pp. 888–899, 2016.
- [22] X. Wang, J. Zhao, and H. Liu, “A new image encryption algorithm based on chaos,” *Optics Communications*, vol. 285, no. 5, pp. 562–566, 2012.
- [23] Da-C. Wu and W. H. Tsai, “A steganographic method for images by pixel-value differencing,” *Pattern Recognition Letters*, vol. 24, no. 9, pp. 1613–1626, 2003.

Biography

Sujarani Rajendran received her M.Tech (Computer science and engineering) in 2010, from SASTRA University, Thanjavur. She is currently working as an Assistant Professor in the Department of CSE in SASTRA University, kumbakonam. She is currently working towards her Ph.D. Degree in SASTRA University. Her research area includes Chaotic Cryptography, DNA Cryptography and Steganography.

Manivannan Doraipandian obtained M.Tech and Ph.D. degree in Computer Science from SASTRA University, Thanjavur, India in 2002 and 2013, respectively. He is currently working as Senior Assistant Professor in the department of School of Computing, SASTRA University. His current research interests includes cryptography, Security in Embedded Systems, Wireless Sensor Networks using reconfigurable processors and Embedded Communication Systems.

A Secure Strong Designated Verifier Signature Scheme

Asif Uddin Khan, Bikram Kesari Ratha

(Corresponding author: Asif Uddin Khan)

Department of Computer Science & Utkal University¹

VaniVihar, Bhubaneswar, India

(Email: asif.utkal@gmail.com, b_ratha@hotmail.com)

(Received Aug. 7, 2012; revised Oct. 12, 2014 and July 18, 2015; accepted July 31, 2016)

Abstract

Recently Lee-Chang proposed a new strong designated verifier signature scheme. They claimed that their proposed scheme is more secure and suitable for the purpose of a strong designated verifier signature scheme. This paper shows that Lee-Chang scheme cannot withstand forgery attack which an adversary can forge a signature without knowing the secret key of the signer or the designated verifier and an improved scheme is presented to overcome the security weaknesses of their scheme. The security of the scheme is enhanced by adding the secret key of the signer in signature generation phase. The analysis shows that the new scheme resolves security problems in the previous scheme, meets the aspects of security features needed by strong designated verifier signature scheme.

Keywords: Cryptanalysis; Designated Verifier Signature Scheme; Digital Signature; Forgery Attacks

1 Introduction

Next generation wireless network is expected to include many applications and services such as voice, data and multimedia online gaming, software distribution with very high data rate. Use of new technologies and services such as internet of things cloud computing are growing rapidly day by day where numerous network based services and applications are provided through internet. Further internet of things (IOT) is the big revolution in the future networking technologies where communication for application, data and services can take place any where any time through any device. Providing guaranteed quality of service (QOS) to these applications and services is an important objective in the design of next generation network. At the same time various types of security threats in the network based services are increasing. Providing security such as confidentiality, authenticity and data integrity is a must in order to achieve guaranteed QOS.

A digital signature is very important in modern electronic data processing systems. Recently, to provide security services such as user authentication, data integrity, and non-repudiation, digital signature schemes are widely used in distributed network environments such as Internet or web. There are many variations of digital signature schemes such as proxy signature, blind signature; ring signature discussed in the papers [1, 2, 3, 10, 17, 20]. In an ordinary digital signature scheme, anyone can verify the validity of a signature using the signer's public key. However, in some scenarios, this public verification is not desired, if the signer does not want the recipient of a digital signature to show this signature to a third party at will. To address this problem above, in [6] authors introduced undeniable signature which allowed a signer to have complete control over his signature. In an undeniable signature scheme, the verification of a signature requires the participation of the signer, in order to avoid undesirable verifiers getting convinced of the validity of the signature. Motivated by the above problem, in [6] Jakobsson et al. proposed the concept of designated verifier signature (DVS) schemes. A DVS scheme is special type of digital signature which provides message authentication without non-repudiation. These signatures have several applications such as in E-voting, call for tenders and software licensing. Suppose Alice has sent a DVS to Bob. Unlike the conventional digital signatures, Bob cannot prove to a third party that Alice has created the signature. This is accomplished by the Bob's capability of creating another signature designated to him which is indistinguishable from Alice's signature. In [6] Jakobsson et al. also introduced a stronger version of DVS. In this stronger scheme, no third party can even verify the validity of a designated verifier signature, since the designated verifier's private key is required in the verifying phase. In 2003, Saeednia et al. [11] proposed a strong designated verifier signature scheme based on the Schnorr signature scheme [12] and Zheng's signcryption scheme [21].

In 2008, Lee-Chang [8], however, pointed out that Saeednia et al.'s scheme would reveal the identity of

the signer if the secret key of the signer is compromised. Then, they proposed a new strong designated verifier signature scheme based on the Schnorr signature scheme [12] and Wang et al.'s authenticated encryption scheme [15] which can be verified only with the designated verifier's secret key. Obviously, Lee-Chang's scheme provides signer ambiguity even in the situation in which the secret key of the signer is compromised since each secret key is protected under the DLP (Discrete Logarithm Problem) assumption. Lee-Chang claimed that their proposed scheme is more secure and suitable for the purpose of a strong designated verifier signature scheme, but in [5] Hyun, Suhng-Il, Eun-Jun Yoon et al. shown several attacks on Lee-Chang's scheme. In this paper we discuss the forgery attack on Lee-Chang's scheme and show that their scheme still cannot withstand forgery attack which an adversary can forge a signature without knowing the secret key of the signer or the designated verifier based on [5] and we then propose an improved designated verifier signature scheme which is more secure and safe.

The paper is organized as follows: In section-2 we discuss the related work, Section-3 reviews Lee-Chang's designated verifier signature scheme. Section-4 shows forgery attack on Lee-Chang's scheme. Section-5 shows the improved scheme, section-6 shows analysis of improved scheme and finally the conclusion comes in Section-7.

2 Related Work

Several researches have been conducted to design efficient strong designated verifier signature scheme (SDVS) for achieving Quality of service (QoS) for the next generation networks. In this section, we discuss the recent developments in SDVS. In [7] authors propose a strong designated verifier signature scheme with message recovery mechanism based on the discrete logarithm problem. In [18] a novel construction of a SDVS scheme with secure disavowability is proposed which utilizes a chameleon hash function and supports the signer to have a complete control of his signature. In [9] authors propose an efficient ID-based strong designated verifier signature schemes with message recovery and give its rigorous security proof in the random oracle model based on the hardness assumptions of the computational Bilinear Diffie-Hellman problem. This scheme can be used in some special environments where the bandwidth is one of the main concerns, such as PDAs, cell phones, RFID etc. [16] proposed a strong designated verifier signature in certificateless public key settings strong designated verifier signature in certificateless public key settings. [13] present a stronger security notion for the SDVS schemes, full non-delegatability, which not only needs the non-delegatability of signing, but also requires that non-delegatability of verifying. In [4], Huang, Susilo, Mu et al. proposed a variant of designated verifier signature scheme, i.e. short strong designated verifier signature scheme and its variant scheme which is a identity based scheme. In [19] Yang and Liao proposed

a strong designated verifier signature scheme, using key distribution mechanism where both sender and designated receiver share encryption/decryption key to fulfill encryption/decryption algorithm with low cost of communication and computation respectively and they proved their security based on Deffi-Helman assumptions. [14] provides general CL-SDVS schemes and instances, and discusses their security briefly.

3 Review of Lee-Chang's Strong Designated Verifier Scheme

This section reviews Lee-Chang's strong designated verifier signature scheme as shown in Figure 1. The common parameters used in Lee-Chang's scheme are as follows:

- Alice: The signer.
- Bob: The designated verifier.
- p : A large prime.
- q : A prime factor of $p - 1$.
- g : A generator εZq^* of order q .
- m : A message.
- $H(\cdot)$: A secure one-way hash function such as SHA-2 that outputs values in Zq^*
- (x_A, y_A) : Alice's key pair, where x_A is a randomly selected secret key in Zq^* and the corresponding Public key $y_A = g^{x_A} \bmod p$.
- (x_B, y_B) : Bob's key pair, where x_B is a randomly selected secret key in Zq^* and the corresponding public key $y_B = g^{x_B} \bmod p$.

There are three phases in Lee-Chang's strong designated verifier signature scheme i.e. signature generation, signature verification and signature simulation.

3.1 Signature Generation

- 1) Alice selects a random value $k \varepsilon Zq^*$;
- 2) Alice computes r, s and t as follows:

$$\begin{aligned} r &= g^k \bmod p \\ s &= k + x_A r \bmod q \\ t &= H(m, y_B^s \bmod p). \end{aligned}$$

- 3) The signature is then $\sigma = (r, t)$.

3.2 Signature Verification

Upon receiving m and $\sigma = (r, t)$, Bob can verify the validity of the signature by checking whether

$$t = H(m, (ry_A^r)^{x_B} \bmod p).$$

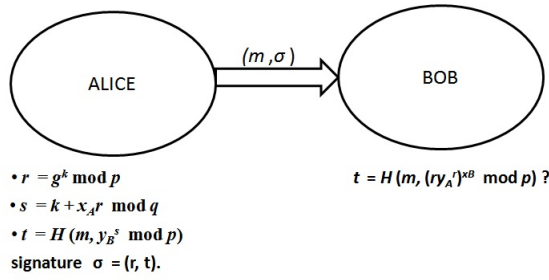


Figure 1: Lee-Chang's scheme

3.3 Signature Simulation

Now Bob can simulate the transcript (r_s, t_s) for the message m by selecting a random number $k_s \in Zq^*$ and computes r_s and t_s as follows

$$\begin{aligned} r_s &= g^{k_s} \bmod p \\ t_s &= H(m, (r_s y_A^{r_s})^{x_B} \bmod p). \end{aligned}$$

4 Forgery Attack on Lee-Chang's Scheme

Based on [5] this section shows that Lee-Chang's scheme still cannot withstand forgery attack which an adversary can forge a signature without knowing the secret key of the signer or the designated verifier.

Suppose that an adversary E intercepts the signature $m, \sigma = (r, t)$ sent from Alice to Bob and then E can perform the following forgery attack:

- 1) Chooses a forged message m^* .
- 2) Find an integer r^* which satisfies $r^* y_A^{r^*} \bmod p = g$.
- 3) Compute $t^* = H(m^*, y_B \bmod p)$.
- 4) Send a forged signature $\sigma^* = (r^*, t^*)$ with m^* to Bob.
- 5) Upon receiving the forged message m^* and the modified signature $\sigma^* = (r^*, t^*)$, Bob will verify the validity of the signature by checking whether

$$t^* = H(m^*, (r^* y_A^{r^*})^{x_B} \bmod p). \quad (1)$$

Its correctness can be seen as follows: Left hand side is

$$t^* = H(m^*, y_B \bmod p)$$

and the right-hand side is

$$\begin{aligned} H(m^*, (r^* y_A^{r^*})^{x_B} \bmod p) &= H(m^*, (g)^{x_B} \bmod p) \\ &= H(m^*, y_B \bmod p). \end{aligned}$$

We can see that Equation (1) is always confirmed as a legal signature of Alice by Bob. Therefore, Bob will believe that the real singer is Alice. However, the signature

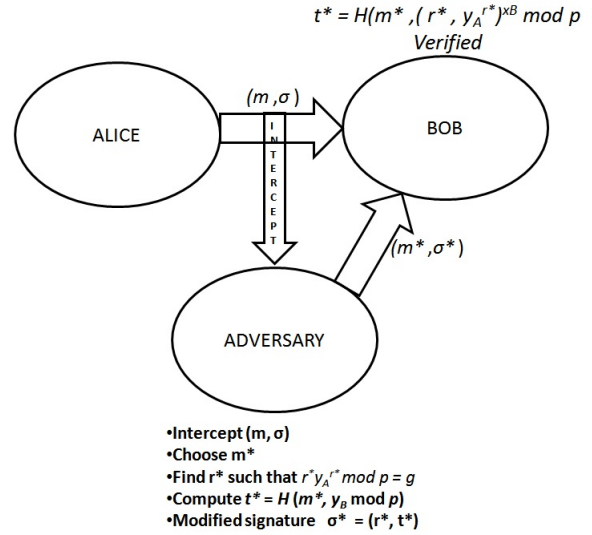


Figure 2: Forgery attack on Lee-Chang's scheme

$\sigma^* = (r^*, t^*)$ is signed by an adversary E . As a result, since the message m^* is obviously not the Alice's original message m , Lee-Chang's scheme is vulnerable to the forgery attack. Figure 2 shows the attack on Lee-Chang's scheme. The following example taken from [5] shows the forgery attack.

Let the parameters $p = 23, q = 11, g = 2, x = 8, y_A = 2^8 \bmod 23 = 3$, then it is easy to find an integer r^* which satisfies $r^* y_A^{r^*} \bmod p = g$. For example, If $r = 4$, then $r^* y_A^{r^*} \bmod p = 4 \cdot 3^4 \bmod 23 = 324 \bmod 23 = 2 = g$. If $r = 8$, then $r^* y_A^{r^*} \bmod p = 8 \cdot 3^8 \bmod 23 = 52488 \bmod 23 = 2 = g$. If $r = 13$, then $r^* y_A^{r^*} \bmod p = 13 \cdot 3^{13} \bmod 23 = 20726199 \bmod 23 = 2 = g$.

5 Improved Scheme

Since Lee-Chang scheme is not secure against forgery attack, in this section we propose an improved scheme which is more secure than the previous one. Figure 3 illustrate the improved scheme.

The common parameters used in the improved scheme can be summarized as follows:

- Alice: The signer;
- Bob: The designated verifier;
- p : A large prime;
- q : A prime factor of $p - 1$;
- g : A generator $\in Zq^*$ of order q which is greater than 2;
- m : A message;
- $H(\cdot)$: A secure one-way hash function such as SHA-2 that outputs values in Zq^* ;

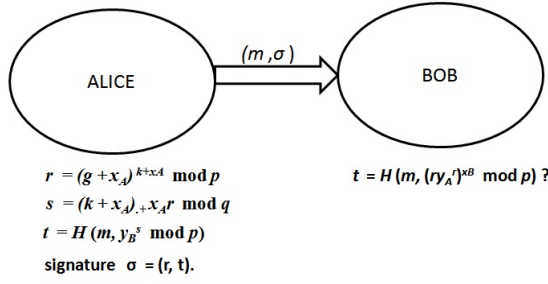


Figure 3: Improved scheme

- (x_A, y_A) : Alice's key pair, where x_A is a randomly selected secret key in Zq^* and the corresponding Public key $y_A = g^{x_A} \bmod p$;
- (x_B, y_B) : Bob's key pair, where x_B is a randomly selected secret key in Zq^* and the corresponding public key $y_B = g^{x_B} \bmod p$.

There are three phases in the improved scheme. The security is enhanced by adding the secret key of Alice in signature generation phase during calculating r and s as follows.

5.1 Signature Generation

- 1) Alice selects a random value $k \in Zq^*$;
- 2) Alice computes r , s and t as follows:

$$\begin{aligned}
 r &= (g + x_A)^{k+x_A} \bmod p \\
 s &= (k + x_A) + x_A r \bmod q \\
 t &= H(m, y_B^s \bmod p).
 \end{aligned}$$

- 3) The signature is then $\sigma = (r, t)$.

5.2 Signature Verification

Upon receiving m and $\sigma = (r, t)$, Bob can verify the validity of the signature by checking whether

$$t = H(m, (ry_A^r)^{x_B} \bmod p). \quad (2)$$

5.3 Signature Simulation

Now Bob can simulate the transcript (r_s, t_s) for the message m by selecting a random number $k_s \in Zq^*$ and computes r_s and t_s as follows.

$$\begin{aligned}
 r_\Psi &= g^{k_\Psi} \bmod p \\
 t_\Psi &= H(m, (r_\Psi y_A^{r_\Psi})^{x_B} \bmod p).
 \end{aligned}$$

5.4 Correctness Proof

In order to verify the signature as mentioned in Equation (2), we have to prove that

$$t = H(m, (ry_A^r)^{x_B} \bmod p).$$

But $t = H(m, y_B^s \bmod p)$, so if we can prove that $y_B^s = (ry_A^r)^{x_B}$, then Equation (2) is proved.

$$\begin{aligned}
 (ry_A^r)^{x_B} &= (r(g^{x_A})^r)^{x_B} \\
 y_B^s &= y_B^{(k+x_A)+x_A r} \\
 &= (g^{x_B})^{(k+x_A)+x_A r} \\
 &= (g^{x_B})^{(k+x_A)} \cdot (g^{x_B})^{x_A r} \\
 &= (g^{(k+x_A)})^{x_B} \cdot ((g^{x_A})^r)^{x_B} \\
 &= r^{x_B} \cdot ((y_A)^r)^{x_B} \\
 &= (ry_A^r)^{x_B}.
 \end{aligned}$$

So from the above we observe that Equation (2) is proved and the signature is verified.

6 Analysis of The Improved Scheme

6.1 Security Analysis

Basic Unforgeability: Because the problem of getting Private Key x_A from the public key y_A equals to solving DLP, no one else can create normal digital signature of the original signer.

6.2 Unforgeability

Because the private key x_A of the signer Alice is added ie $r = (g + x_A)^{k+x_A} \bmod p$ and $s = (k + x_A) + x_A r \bmod q$, any adversary cannot forge the signature without knowing x_A and also finding x_A from y_A is same as solving DLP which is a hard problem. Therefore our scheme is provably secure. In the previous example of we have seen that Adversary can only forge the signature if he/she find r^* such that $r^* y_A^{r^*} \bmod p = g$.

In the improved scheme the private key x_A of the signer Alice is added ie ie $r = (g + x_A)^{k+x_A} \bmod p$ and $s = (k + x_A) + x_A r \bmod q$ in Step-2.

In order to do forgery attack adversary has to guess r^* such that $r^* y_A^{r^*} \bmod p = g + x_A$.

Because of addition of x_A in Step-2 of signature generation adversary cannot guess r^* which satisfies $r^* y_A^{r^*} \bmod p = g + x_A$, as it does not know the value of x_A which is used in signature generation phase, only the original signer knows the value of x_A . Adversary can only forge the signature if and only if he/she get x_A from y_A which is same as DLP a Hard problem with large prime. Hence this proves that our improved scheme is safe and secure.

Table 1: Performance comparison between improved scheme and Lee Chang's scheme

Computations Cost	Lee-Chang's Scheme	Improved Scheme
Signature Generation	2TE+TM+TH	2TE+TM+TH
Signature Verification	2TE+TM+TH	2TE+TM+TH
Signature Simulation	3TE+TM+TH	3TE+TM+TH

TE = Time taken for an exponential operation.

TM = Time taken for a modular multiplication.

TH = Time taken for a one-way hash function.

6.3 Performance Comparison of The Improved Scheme with Lee Chang's Scheme

In this section, we compare the computational costs of different phases of our scheme with those for Lee Chang's scheme. We have compared the computational costs of different phases of our scheme with those for Lee Chang's scheme in Table 1 where TE = Time taken for an exponential operation, TM = Time taken for a modular multiplication and TH = Time taken for a one-way hash function. From this table, we see that both schemes have same computational costs.

7 Conclusions

In this paper, we discuss the drawbacks of Lee Chang's strong designated verifier signature scheme and proposed a new strong designated verifier signature scheme based on DLP. The improved scheme can remedy the weaknesses of Lee Chang's scheme and meets the security aspects needed by the strong designated verifier signature scheme. In other words, the new scheme is more secure than the existing scheme keeping the computational cost same as the previous scheme.

Acknowledgments

We would like to thank the anonymous reviewers for their valuable comments and suggestions which have helped us to improve the contents and presentation of the paper significantly.

References

- [1] S. G. Aki, "Digital signatures: a tutorial survey," *Computer*, vol. 16, no. 2, pp. 15–24, 1983.
- [2] T. Cao, D. Lin, and R. Xue, "Security analysis of some batch verifying signatures from pairings," *International Journal of Network Security*, vol. 3, no. 2, pp. 138–143, 2006.
- [3] M. L. Das, A. Saxena, and D. B. Phatak, "Algorithms and approaches of proxy signature: A survey," *arXiv preprint cs/0612098*, 2006.
- [4] X. Huang, W. Susilo, Y. Mu, and F. Zhang, "Short designated verifier signature scheme and its identity-based variant," *International Journal of Network Security*, vol. 6, no. 1, pp. 82–93, 2008.
- [5] S. I. Hyun, E. J. Yoon, and K. Y. Yoo, "Forgery attacks on lee-chang's strong designated verifier signature scheme," in *IEEE Second International Conference on Future Generation Communication and Networking Symposia (FGCNS'08)*, vol. 2, pp. 5–8, 2008.
- [6] M. Jakobsson, K. Sako, and R. Impagliazzo, "Designated verifier proofs and their applications," in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 143–154, 1996.
- [7] J. S. Lee and J. H. Chang, "Strong designated verifier signature scheme with message recovery," in *The 9th International Conference on Advanced Communication Technology*, vol. 1, pp. 801–803, 2007.
- [8] J. S. Lee and J. H. Chang, "Comment on saeednia et al.'s strong designated verifier signature scheme," *Computer Standards & Interfaces*, vol. 31, no. 1, pp. 258–260, 2009.
- [9] M. Li and T. Fang, "Provably secure and efficient id-based strong designated verifier signature scheme with message recovery," in *2014 17th International Conference on Network-Based Information Systems*, pp. 287–293, 2014.
- [10] C. Pan, S. Li, Q. Zhu, C. Wang, and M. Zhang, "Notes on proxy signcryption and multi-proxy signature schemes," *International Journal of Network Security*, vol. 17, no. 1, pp. 29–33, 2015.
- [11] S. Saeednia, S. Kremer, and O. Markowitch, "An efficient strong designated verifier signature scheme," in *International conference on information security and cryptography*, pp. 40–54, 2003.
- [12] C. P. Schnorr, "Efficient signature generation by smart cards," *Journal of Cryptology*, vol. 4, no. 3, pp. 161–174, 1991.
- [13] F. Tang, C. Lin, Y. Li, and S. Zhang, "Identity-based strong designated verifier signature scheme with full non-delegatability," in *2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 800–805, 2011.
- [14] H. Tian, "General certificateless strong designated verifier signature schemes," in *2013 5th International Conference on Intelligent Networking and Collaborative Systems*, pp. 392–397, 2013.

- [15] G. Wang, F. Bao, C. Ma, and K. Chen, "Efficient authenticated encryption schemes with public verifiability," in *2004 IEEE 60th International Conference on Vehicular Technology (VTC'04)*, vol. 5, pp. 3258–3261, 2004.
- [16] Z. Xiao, Bo Yang, and S. Li, "Certificateless strong designated verifier signature scheme," in *2010 IEEE 2nd International Conference on E-business and Information System Security*, pp. 1–5, 2010.
- [17] Hu Xiong, Ji Geng, Z. Qin, and G. Zhu, "Cryptanalysis of attribute-based ring signcryption scheme," *International Journal of Network Security*, vol. 17, no. 2, pp. 224–228, 2015.
- [18] Bo Yang, Y. Sun, Y. Yu, and Qi Xia, "A strong designated verifier signature scheme with secure disavowability," in *4th International Conference on Intelligent Networking and Collaborative Systems (INCoS'12)*, pp. 286–291, 2012.
- [19] F.-Yi Yang and C.-M. Liao, "A provably secure and efficient strong designated verifier signature scheme," *International Journal of Network Security*, vol. 10, no. 3, pp. 220–224, 2010.
- [20] X. Zhang, R. Lu, H. Zhang, and C. Xu, "A new digital signature scheme from layered cellular automata," *International Journal of Network Security*, vol. 18, no. 3, pp. 544–552, 2016.
- [21] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) cost (signature)+ cost (encryption)," in *Annual International Cryptology Conference*, pp. 165–179, 1997.

Bikram Kesari Ratha born on 20th May 1965. He completed his MCA (Tech) from NIT Rourkela, India in 1988 and subsequently completed his Master Of Engineering (CSE) from the same institute. Under the able guidance of Prof. Rajib Mall of IIT Kharagpur he completed his PhD from Utkal University Bhubaneswar, India. He has teaching experience over 25 years in several program such as B.E (CSE), MCA, MSc. (CS), M.E. (K.E0, M.Tech(CS)) in different Universities and Institutes. He has worked as a Professor in Nepal Engineering College a constituent college of Pokhara University, Kathmandu, Nepal from 2000-2005. During this period he has worked hard to spread IT in the country with active support from His Majesty's Government of Nepal. Further he has worked as a Professor in SRTM University's Latur sub centre. During his tenure apart from teaching and research he was actively involved in social work such as empowering women through ICT on various issues by organizing road shows, workshops and drama. He has delivered many invited lectures on the environment, impact of technology on health and society at large. For these activities he has been awarded the best technocrat award by Green Forum an NGO working on environment in the year 2015. He has published about 50 research papers and delivered many talks on cyber space in various forums in India. His research interest is Software Engineering, Data Mining and ICT Applications, Computer Networks, computer security and image Processing.

Biography

Asif Uddin Khan received BE in Computer Science and Engineering from C.V Raman College of Engineering, Bhubaneswar BPUT, India. M.Tech in Computer Science and Engg from IIIT Bhubaneswar, India. Presently he is working towards his PhD in Computer Science from Department of Computer science, Utkal University, Bhubaneswar, Odisha, India. His research interest includes cryptography and network security, mobile ad-hoc network, software defined network, vehicular ad hoc networks and cloud computing.

On the Security of a Mutual Verifiable Provable Data Auditing in Public Cloud Storage

Jianhong Zhang^{1,3}, Pengyan Li¹, and Min Xu²

(Corresponding author: Jianhong Zhang)

College of Sciences & North China University of Technology, Beijing 100144, China¹

Department of Education & Baoding University, Baoding 07100, China²

Guangxi Key Lab of Multi-source Information Mining & Security, Guilin, China³

(Email: xumin@163.com)

(Received Jan. 29, 2016; revised and accepted Apr. 23 & Sept. 24, 2016)

Abstract

Provable Data Possession (PDP) enables cloud users to verify the integrity of their outsourced data without retrieving the entire file from cloud servers. At present, to execute data checking, many PDP schemes is delegated to some proxy to implement remote data possession checking task. Because the proxy may store some state information in cloud storage servers, it makes that many PDP scheme are insecure. To solve this problem, Ren et al. proposed an mutual verifiable provable data possession scheme and claimed that their scheme is secure. Unfortunately, in this work, we show that their scheme is insecure. It exists forgery attack and replay attack. After giving the corresponding attacks, we give an improved scheme to overcome the above flaws. By analyzing, we show that our improved PDP scheme is secure under the Chosen-Target-CDH problem and the CDH problem.

Keywords: *Diffie-Hellman Key Agreement; Forgery Attack; Mutual Verifiable; Provable Data Possession (PDP).*

1 Introduction

Due to providing dynamically scalable resources provisioned as a service over the Internet, Cloud computing has been emerged as a new computing paradigm in Internet's evolution. Many advantages in Cloud computing draw people attentions [12]. These advantages make it has become an inevitable trend that individuals and IT enterprises store data remotely to the cloud in a flexible on-demand manner, namely cloud storage. As an important service of cloud computing, cloud storage allows the data owner to migrate his data files from their local disk to the remote cloud server, which is one of the most important cloud services. Meanwhile, it allows the cloud clients to flexibly access their outsourced files at anytime and from anywhere. For IT enterprises, it avoids the ini-

tial investment of expensive infrastructure setup, large equipment, and daily maintenance cost.

Although cloud storage can provide convenience for people, it also makes people face numerous security challenges since cloud server is not fully trusted [15]. Firstly, data owners would worry that their outsourced data could be revealed or accessed by the unauthorized users. Secondly, they would also worry that their outsourced data could be lost in the Cloud since cloud sever may discard the data which has not been accessed or rarely accessed to save the storage space or keep fewer replicas than promised. To the best of my knowledge, there exists a lot of incidents of data loss or leakage in recent years. For example, it was reported that "Amazon's huge EC2 cloud services crash permanently destroyed some data, and Hundreds of Dropbox Passwords are leaked. Based on the above worries, data owners hope a kind of cloud service to assure the integrity checking of the outsourced data.

To solve the above security challenging problem, Ateniese et al. [1] proposed the model of Provable Data Possession (PDP) to solve the storage auditing problem by spot-checking technique. And gave two provably secure and practical PDP schemes from the RSA assumption in 2007. They can achieve the data integrity checking of static data. In the same year, Juels et al. [6] proposed the notion of Proof of Retrievability (PoR), in which the integrity of the data file is completed by checking the correctness of the inserted sentinel blocks. The number of times that the file can do integrity verification is limited since the sentinel blocks are one-time labels. Subsequently, Shacham and Waters [10] put forward two efficient and compact PoR schemes. The first one which is based on BLS signature, is publicly verifiable; the second one which is based on pseudo-random functions (PRFs), only supports private verification.

According to the roles of the verifier, the PDP protocols are divided into two categories: private PDP and public PDP. In some cases, private PDP is very nec-

essary. For example, in Cloud-EHR (Electronic Health Records), the patient only hopes his own or the designated doctors to check the integrity of health records in case that these sensitive information is leaked. Recently Shen and Tzeng proposed a delegable provable data possession scheme [11], in which data owner produces the delegation key for delegated verifier and stores the key in cloud storage service (CSS) for verification. In [14], Wang et al. proposed a proxy provable data possession (PPDP) model. In PPDP, data owner is able to delegate a proxy to enforce its remote data possession checking on behalf of his own. Unfortunately, the two private PDP schemes are shown to be insecure since the state information of the proxy or delegated verifier is controlled by a malicious CSS [?].

With the proliferation of cloud storage, a variety of cloud auditing protocols and their variants [2, 3, 4, 5, 7, 8, 13, ?, 17, 18] were proposed for catering some specific properties, such as public verification, dynamic operations and privacy preserving. According to the different requirements of the stored data and various properties of cloud storage services, A majority of the storage services are provided. For example, Spideroak [2], it is a good solution for security and privacy, which might be particularly appealing if a user would like to store sensitive data; Dropbox [2, 16], as one of the first online storage services, is useful, reliable and works across multiple platforms.

Recently, to overcome the above problems in private PDP, Ren et al. proposed an efficient mutual verifiable provable data possession (MV-PDP) scheme by using Diffie-Hellman key agreement. In their MV-PDP scheme, the verifier is stateless and independent from CSS, thus, the scheme efficiently overcomes the problem which the verifier can be optionally specified by a malicious CSS. Very regretfully, in this work, we show that Ren et al.'s MV-PDP scheme is insecure, it exists forgery attack, replay attack and the deleting attack of malicious cloud server. After we give the corresponding attacks, the reasons to produce such attacks are analyzed. Finally, to overcome our attacks, an improved PDP scheme is proposed. And the improved scheme is shown to be secure under the Chosen-Target-CDH problem and the CDH problem.

2 Preliminaries

2.1 System Model

For a PDP scheme, it involves three entities: cloud client, cloud storage server and the verifier. The cloud server has huge storage space and computational resources. It provides data storage service and charges cloud users according to pay-per-use regulation. In general, cloud users are the resource-constrained devices, it needs to rent data storage service and interact with the cloud server to upload, access and update their stored data. The verifier may be a cloud user or a delegated party.

2.2 Computational Assumptions

The security of the improved signature schemes is based on the hardness of the CDH problem for the scheme in [?]. The Chosen-Target-CDH problem is defined as follows: the solver S receives as input a pair (g, g^a) , where g is a generator of G_1 with the prime order q , and $a \in \mathbb{Z}_q$ is a random value. The solver S has adaptive access to two oracles:

- 1) Target oracle: this oracle outputs a random element $Z_i \in G$;
- 2) Helper oracle: this oracle takes as input an element $W_i \in G$ and outputs the element W_i^a .

We say that the solver $S(q_t, q_h, d)$ -solves the Chosen-Target-CDH problem, for $q_t \geq d > q_h$, if it makes q_t and q_h queries, respectively, to the target and helper oracles, and after that it outputs d pairs $((V_1, j_1), \dots, (V_d, j_d))$ such that:

- 1) All the elements V_i are different;
- 2) For all $i \in \{1, 2, \dots, d\}$, the relation $V_i = Z_{j_i}^a$ is satisfied where Z_{j_i} is the element output by the target oracle in the j_i -th query.

3 Reviews of Ren et al.'s Public Auditing Scheme

Recently, to overcome the proxy which stores some state information in cloud storage servers, Ren et al. proposed a mutual verifiable public auditing scheme. In their scheme, the verifier is stateless and independent of cloud server, and the scheme is very efficient in terms of auditing cost. In the following, we briefly review Ren et al.'s scheme. Please the interested reader refer to [9] for the detail.

Setup: Let λ be a security parameter, taking λ as an input, output the following parameters. G is a cyclic multiplicative group with the large prime order q . g is a generator of group G . Choose two hash functions H_1 and H_2 , which satisfy $H_1 : \{0, 1\}^* \rightarrow \mathbb{Z}_q$ and $H_2 : \{0, 1\}^* \rightarrow \mathbb{Z}_q$. The system parameters are

$$(g, G, q, H_1, H_2).$$

KeyGen: For a client, it chooses a random number $x \in \mathbb{Z}_q$ as private key and produces public key $X = g^x$. And the client designates a trust verifier DV to enforce integrity checking. At the same time, DV runs **KeyGen** to produce a public-private pair $(y, Y = g^y)$.

TagGen: Assume that the outsourced file F is divided into n blocks $\{m_1, m_2, \dots, m_n\}$, to produce authentication tag on data block m_i , it computes as follows:

- 1) The client computes $k_{i1} || k_{i2} = H_1(Y^x, m_i)$;

2) Then it computes

$$\begin{aligned}\delta_{i1} &= (Y^{H_2(m_i)k_{i1}+k_{i2}}) \\ \delta_{i2} &= X^{k_{i1}} \\ \delta_{i3} &= X^{k_{i2}}.\end{aligned}$$

3) Finally, the authentication tags are denoted as $\phi = (\delta_{i1}, \delta_{i2}, \delta_{i3}), i \leq i \leq n$.

The client sends (F, ϕ) to the cloud server and deletes them from its local disk.

Challenge phase: In their protocol, only the client or the designated verifier (DV) is able to verify the integrity checking of the outsourced data with the cloud server. To execute the integrity checking, the verifier randomly chooses a c -element subset I of the set $[1, n]$, and for $i \in I (1 \leq i \leq c)$, it selects random element $v_i \in Z_q$. Finally, the verifier sends the challenge information $chall = \{(i, v_i)\}_{i \in I}$ to the cloud server.

GenProof: On receiving the challenge information, the cloud server computes as follows.

$$\begin{aligned}\sigma &= \sum_{i=1}^c \delta_{i1}^{v_i} \\ \delta &= \sum_{i=1}^c \delta_{i2}^{H_2(m_i)v_i} \\ \eta &= \sum_{i=1}^c \delta_{i3}^{v_i}.\end{aligned}$$

The cloud server outputs the proof information $pf = (\sigma, \delta, \eta)$ to the verifier as the corresponding response.

VerifyProof: After receiving the returned proof information $pf = (\sigma, \delta, \eta)$ the designated verifier checks whether the following equation holds by using public key X and his private key y .

$$\sigma = (\delta \cdot \eta)^y$$

If the equation holds, then it outputs true, otherwise, outputs false.

4 Security Analysis of Ren et al.'s Scheme

In [1], by using the Diffie-Hellman agreement key, Ren et al. proposed an auditing protocol in public cloud. Their protocol only supports the verification of the client and the designated verifier, and they also claimed that their scheme is secure, the security of their scheme is based on the CDH problem. Unfortunately, by analyzing the security of the scheme, we show that their scheme is insecure. Any one can produce a forged proof information to make that the designated verifier ensures the returned response

satisfies the verification equation. That is to say, the designated verifier's integrity checking cannot guarantee the security of outsourced data in cloud server.

In the following, we give the corresponding attack and analyze the reason to produce such attack.

4.1 Forgery Attack

Let A be an adversary, to forge a false proof information, it randomly chooses $R_1 \in G$ and $r \in Z_q$ to set

$$\begin{aligned}\delta^* &= R_1 \\ \eta^* &= R_1^{-1} \cdot g^r \\ \sigma^* &= Y^r.\end{aligned}$$

Thus, the forged proof information is $(\delta^*, \eta^*, \sigma^*)$.

In the following, we show the forged proof information $(\delta^*, \eta^*, \sigma^*)$ can pass the verification of the designated verifier. since the designated verifier can use its private key y to compute

$$\begin{aligned}(\eta^* \delta^*)^y &= (R_1 \cdot R_1^{-1} \cdot g^r)^y \\ &= (g^{ry}) \\ &= Y^r \\ &= \sigma^*\end{aligned}$$

It means that the forged proof information $(\delta^*, \eta^*, \sigma^*)$ satisfies verification equation. Thus, our attack is valid.

The reason to produce such attack is that each component in the proof information $pf = (\sigma, \delta, \eta)$ is free, the relation of each component with the other ones among the proof information cannot be constrained each other. At the same time, for each challenge, the challenge information has not shown in the verification equation, it gives the attacker to provide a forgery chance. To overcome such attacker, the relation of elements in the proof information must be restrained.

4.2 Replay Attack of Cloud Server

In cloud storage, cloud server is a un-trusted entity. Here, we will show that cloud server how to implement replay attack.

Let $pf = (\sigma, \delta, \eta)$ be a valid proof information which is from a challenge. When the designated verifier makes a new challenge with cloud server. Cloud server randomly chooses $r \in Z_q$ to compute

$$\begin{aligned}\delta^* &= \delta^r \\ \eta^* &= \eta^r \\ \sigma^* &= \sigma^r\end{aligned}$$

Then, it sets $prf^* = (\delta^*, \eta^*, \sigma^*)$ as a proof information and returns it to the designated verifier.

In the following, we show that the returned proof information can pass the verification of the designated verifier.

Since

$$\begin{aligned}
 (\delta^* \cdot \eta^*)^y &= (\delta^r \cdot \eta^r)^y \\
 &= (\delta^r \cdot \eta^r)^y \\
 &= (\delta \cdot \eta)^{y \cdot r} \\
 &= \sigma^r \\
 &= \sigma^*
 \end{aligned}$$

Obviously, it satisfies the verification equation of the designated verifier. It means that cloud server's replay attack is valid.

The reason to produce such attack is that verification equation is independent of each proof information. And verification equation has homomorphism. Thus, it is very easy to result in replay homomorphism attack.

4.3 Delete Attack

According to Ren et al.'s scheme, in the VerifyProof phase and GenProof phase, the stored message F is not used. Thus, the malicious cloud server can delete the stored message F , it only keeps all block's authentication tags $\phi = (\delta_{i1}, \delta_{i2}, \delta_{i3})$, $1 \leq i \leq n$ and each block's hash value $H_2(m_i)$, $1 \leq i \leq n$. Then the cloud server can produce a valid proof information by all $H_2(m_i)$ and ϕ . Thus, their scheme exists the cloud server's deleting attack.

5 An Improved Auditing Scheme in Public Cloud

To overcome the above attacks, based on Diffie- Hellman key agreement idea, we give an improved auditing scheme. The details are as follows:

Setup: Let λ be a security parameter, taking λ as an input, output the following system parameters. G is a cyclic multiplicative group with the large prime order q . g is a generator of group G , and select three hash functions H , H_1 and H_2 , which satisfy $H_0 : \{0, 1\}^* \rightarrow G$, $H_1 : \{0, 1\}^* \rightarrow Z_q$ and $H_2 : \{0, 1\}^* \rightarrow Z_q$. Let $f : \{0, 1\}^k \times \{0, 1\}^{\log_2 n} \rightarrow \{0, 1\}^l$ denotes a pseudo-random function and $\pi : \{0, 1\}^k \times \{0, 1\}^{\log_2 n} \rightarrow \{0, 1\}^{\log_2 n}$ represents a pseudo-random permutation. The system parameters are

$$(g, h, G, q, \pi, f, H_0, H_1, H_2)$$

KeyGen: In this phase, KeyGen is the same as that of Ren et al's scheme.

TagGen: Let F denote the outsourced file, it is separated into n blocks $\{m_1, m_2, \dots, m_n\}$, to produce authentication tag on data block m_i , it computes as follows:

- 1) The client computes $k_{i1} || k_{i2} = H_1(Y^x, m_i)$;

- 2) Then it computes

$$\begin{aligned}
 \delta_{i1} &= H_0(\text{name}, i, Y^x) Y^{x m_i} (Y^{H_2(m_i) k_{i1} + k_{i2}})^x \\
 \delta_{i2} &= X^{k_{i1}} \\
 \delta_{i3} &= X^{k_{i2}}
 \end{aligned}$$

- 3) Finally, the authentication tags are denoted as $\phi = (\delta_{i1}, \delta_{i2}, \delta_{i3})$, $i \leq i \leq n$.

The client sends (F, ϕ) to the cloud server and deletes them from its local disk.

Challenge phase: The same as Ren et al.'s protocol, in our improved protocol, only the client or the designated verifier (DV) is allowed to verify the integrity checking of the outsourced data. To achieving the integrity checking, the verifier randomly chooses an integer c and two keys k_1 and k_2 for f and π respectively. Then, the verifier sends the challenge information $\text{chall} = (c, k_1, k_2)$ to the cloud server.

GenProof: Upon receiving the challenge information $\text{chall} = (c, k_1, k_2)$, the cloud server computes as follows.

- 1) For $j = 1$ to c , it computes $i_j = \pi_{k_2}(j)$ as the challenged blocks' indices, and it computes $a_j = f_{k_1}(j)$ as random coefficients.
- 2) Then compute

$$A = \sum_{i=1}^c a_i m_i$$

;

- 3) Next it computes

$$\begin{aligned}
 \sigma &= \sum_{i=1}^c \delta_{i1}^{v_i} \\
 \delta &= \sum_{i=1}^c \delta_{i2}^{H_2(m_i) v_i} \\
 \eta &= \sum_{i=1}^c \delta_{i3}^{v_i}.
 \end{aligned}$$

The cloud server outputs the proof information $pf = (D = X^A, \sigma, \delta, \eta)$ to the verifier as the corresponding response.

VerifyProof: After receiving the returned proof information $pf = (D, \sigma, \delta, \eta)$ the designated verifier executes as follows:

- 1) It firstly produces the challenged blocks i and the corresponding coefficients a_i .
- 2) Then, it computes

$$R = \prod_{i=1}^c H_0(i, X^y)^{a_i}$$

- 3) It checks whether the following equation holds by using public key X and his private key y .

$$\sigma \cdot X^{-yA} = (\delta \cdot \eta)^y \cdot R.$$

If the equation holds, then it outputs true, otherwise, outputs false.

6 Security Analysis of the Improved Scheme

In the section, we show that our improved scheme can achieve the properties of completeness, soundness and data privacy.

6.1 Completeness

For the client and the cloud server, if both of them are honest, then for each authentication tag $(\delta_{i1}, \delta_{i2}, \delta_{i3})$ and the challenged information (c, k_1, k_2) , the completeness of the protocol is demonstrated as follows.

$$\begin{aligned} \sigma \cdot X^{-yA} &= \prod_{i=1}^c \delta_{i1}^{a_i} \cdot (X^y)^{-A} \\ &= \left(\prod_{i=1}^c H_0(\text{name}, i, Y^x) Y^{xm_i} (Y^{H_2(m_i)k_{i1}+k_{i2}})^x \right)^{a_i} \\ &\quad \cdot (X^y)^{-A} \\ &= \left(\prod_{i=1}^c H_0(\text{name}, i, Y^x) \right)^{a_i} \prod_{i=1}^c (Y^{H_2(m_i)k_{i1}+k_{i2}})^{a_i x} \\ &= \left(\prod_{i=1}^c H_0(\text{name}, i, Y^x) \right)^{a_i} \prod_{i=1}^c (X^{H_2(m_i)k_{i1}+k_{i2}})^{a_i y} \\ &= (\delta \cdot \eta)^y \cdot R. \end{aligned}$$

6.2 Soundness

Theorem 1. *If there exists a malicious cloud server can produce a false proof information to convince the designated verifier that the outsourced data is integrity in our improved scheme, then the CDH problem in group G can be solved.*

Proof. We will show for any PPT adversary A who wins the soundness of the game, there exists a challenger B that can construct a simulator S to solve an instance of the CDH problem.

Setup: Let (g, g^a, g^b) be an instance of the CDH problem. B sets (G, g, q) as system parameters. Let the attacked client's public key be pk_c and set $pk_c = g^a$. And B randomly choose $r \in Z_q$ as private key of the designated verifier and computes its public key $pk_v = g^r$.

Queries: A can adaptively make the following queries H_0 -Oracle, H_1 -Oracle, H_2 -Oracle and TagGen-oracle during the execution. B responses these oracles as follows.

H_1 -Oracle: When an adversary A makes a H_1 -query with $(*, m_i)$, if the record $(*, m_i)$ exists, then it outputs (k_{i1}, k_{i2}) . Otherwise, it tosses a coin with the probability $Pr[\text{coin}_i = 1] = \zeta$ and randomly chooses $y_i \in Z_q$ to answer the following query.

- 1) If $\text{coin}_i = 0$, then B sets $Y^{H_2(m_i)k_{i1}+k_{i2}} = g^b$; and insert $(*, m_i, g^b, \perp, \perp, \text{coin}_i)$ in the H_1 -list which is initially empty.
- 2) If $\text{coin}_i = 1$, then B sets $Y^{H_2(m_i)k_{i1}+k_{i2}} = g^{y_i}$; and insert $(*, m_i, g^{y_i}, k_{i1}, k_{i2}, \text{coin}_i)$ in the H_1 -list, where k_{i1}, k_{i2} are two random numbers.

H_2 -Oracle: When an adversary A queries the H_2 -oracle with m_i . If the record (m_i, χ_i) exists in the H_2 -list which is initially empty, then χ_i is returned. Otherwise, B randomly selects $\chi_i \in Z_q$ and returns it to A . And insert (m_i, χ_i) in the H_2 -list.

TagGen Oracle: When the adversary A makes a TagGen oracle query with m_i . If $\text{coin}_i = 0$ which corresponds to m_i in the H_1 -list, then it aborts it. Otherwise, if m_i does not exist in the H_1 -list, then it randomly chooses $k_{i1}, k_{i2} \in Z_q$ to compute

$$\begin{aligned} \delta_{i1} &= (pk_c^{H_2(m_i)k_{i1}+k_{i2}})^r \\ \delta_{i2} &= pk_c^{k_{i1}} \\ \delta_{i3} &= pk_c^{k_{i2}}. \end{aligned}$$

If m_i exists in the H_1 -list, then it uses the returned k_{i1}, k_{i2} to produce authentication tag. Finally, B returns $(\delta_{i1}, \delta_{i2}, \delta_{i3})$ to the adversary A .

Forgery: The adversary A outputs the forgery authentication tag on message m^* as follows:

$$(m^*, \delta_{i1}^*, \delta_{i2}^*, \delta_{i3}^*).$$

If the verification fails or the $\text{coin}_i^* = 0$ which corresponds to m^* in the H_1 -list, then B claims it is failure. Otherwise,

$$\begin{aligned} \delta_{i1}^* &= (pk_v^{H_2(m^*)k_{i1}^*+k_{i2}^*})^a \\ &= (g^{H_2(m^*)k_{i1}^*+k_{i2}^*})^a \\ &= g^{ab} \end{aligned}$$

It means that the CDH problem can be solved. Obviously, it is in contradiction with the difficulty of solving the CDH problem. □

Theorem 2. *For the cloud server, if it can return a false proof information which passes the verification of the designators, then the Chosen-Target-CDH problem is able to be solved.*

Proof. Assume that there exists a probabilistic adversary A which breaks our improved mutual PDP scheme, then we are able to construct a solver B of the Chosen-Target-CDH problem, which uses A to solve the Chosen-Target-CDH problem.

First of all, B initializes A by setting up the system parameters. Therefore, the solver B chooses a group G_1 with prime order q . g is a generator of group G_1 .

The solver B asks for an instance of the Chosen-Target-Inverse-CDH problem in the group G_1 . It receives 2-tuple (g, g^a) for some random secret number $a \in Z_q$. And it is allowed to access the target oracles and the helper oracles.

In the following game, B randomly chooses $k \in Z_q$ to compute $X = g^k$ as the public key of the challenged client. And set $Y = g^a$ as the public key of the designated verifier.

Queries: Once A is started with public parameters and public keys X, Y as input, a series of following queries may occur, where H_1 -Oracle, H_2 -Oracle, and TagGen Oracle are the same as those of Theorem 1.

Proof-Oracle: In this query, the challenger C behaves as the verifier and the adversary acts as the prover and query the solver B . And C makes at most q_p proof queries.

C makes a challenge information $chall = (c_i, k_{i1}, k_{i2})$ to the adversary A , then the adversary A does as follows.

- 1) For $j = 1$ to c_i , it computes $i_j = \pi_{k_{i2}}(j)$ as the challenged block's indices, and it computes $a_{ji} = f_{k_{i1}}(j)$ as random coefficients. And it computes

$$R_i = \prod_{j=1}^c H_0(j, X)^{a_j}$$

where $H_0(j, X)$ has already been queried by the adversary.

- 2) Then it queries the solver B for a random element, and B makes a query to its target oracle, and receives a random element $S_i \in G_1$ as answer from its target oracle.
- 3) Subsequently, it randomly selects $r \in Z_q, Q_i \in G_1$ and sets $\delta_i = Q_i, D_i = g^r$ and $\eta_i = S_i / (Q_i \cdot D_i)$.
- 4) Next the adversary sends S_i to the solver B , at the same time, the solver B sends to the helper oracle the value S_i , and obtains as answer the value $T_i = S_i^a$. Finally, return it the adversary A .
- 5) Finally, it sets $\sigma_i = T_i / R_i$ and returns proof information $(D_i, \delta_i, \eta_i, \sigma_i)$.

Output: Eventually, the adversary outputs a proof information $(D_i^*, \delta_i^*, \eta_i^*, \sigma_i^*)$, it should satisfies

$$\sigma^* = (\delta^* \cdot \eta^* \cdot D^*)^y \cdot R^*.$$

Obviously, (S_i, T_i) and $(S^* = \delta^* \cdot \eta^* \cdot D^*, T^* = \sigma^* / R^*)$ are different. It means that the solver B can output it outputs $q_p + 1$ pairs (S_i, T_i) , however, it only makes q_p target oracle queries. Due to difficulty of solving the Chosen-Target-CDH, our improved PDP scheme is secure. □

7 Performance Analysis

In this section, we evaluate the performance of the improved scheme in terms of computational cost. In cloud storage, data owner is a resource-restricting entity and the auditor is a very resource demanding service entity in terms of computational resource. Their computation efficiency has very important influence on the whole system. Therefore, we simulate the computational cost of the data owner and the verifier on a Mac OS X system with an Intel Core 2 Duo CPU at 2.5 GHz and 4.00-GB RAM. The code uses the pairing-based cryptography library version 0.5.12 to simulate the improved scheme.

7.1 Computational Cost of Data Owner

In our scheme, computational cost of data owner is determined by the number of producing tags for data block. For a constant size data file M , the number of data block is computed as $n = \frac{\text{sizeof}(M)}{\text{sizeof}(m_{\text{block}})}$, where $\text{sizeof}(m_{\text{block}})$ denotes the length of each data block. When we consider the time of producing a tag for one data block, it is easy to see that the computational time can be denoted as

$$\text{Time}_{\text{tag}} = 5C_{\text{Mul}} + 2C_H$$

where the symbols C_H and C_{Mul} denote hash operation which map to point of group G and point multiplication.

The total tag generation time for a constant size of data M can be computed as

$$T\text{Time}_{\text{tag}} = \frac{\text{sizeof}(M)}{\text{sizeof}(m_{\text{block}})} (2C_H + 5C_{\text{Mul}}). \quad (1)$$

According to Equation (1), we know the size of data block has influences on computation time of data owner. Figure 1 shows the total computation time of generating all the data tags for 1 MByte data component versus the size of each data block.

7.2 Computational Cost of the Verifier

In our scheme, the computational cost of the verifier includes the verification of data integrity checking equation. And it is linear to the number c of the challenged data

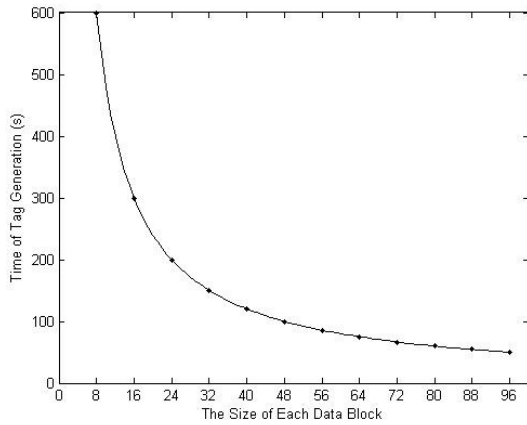


Figure 1: Impact of data block's size on computation time of data owner

blocks. It is easy to see that the computational time can be described as

$$Time_{ver} = (c)C_H + (c + 2)C_{Mul} + 3C_e.$$

According to the above equation, we know that computation cost of the verifier is influenced by the challenged block's number. However, the time-consuming pairing operation is required in our improved scheme.

8 Conclusions

In this paper, we analyze the security of Ren et al.'s mutual PDP scheme, and show that their scheme is insecure against forgery attack, replay attack and deleting attack. It does not satisfy the security which are claimed in their scheme. After analyzing the reasons to produce such attacks, we proposed an improved PDP scheme to overcome the attacks which we launch on their scheme. Finally, we also analyze the security of the improved PDP scheme, and show that it is secure under the Chosen- Target-CDH problem.

Acknowledgments

This work is supported by Beijing Natural Science Foundation (No:4162020), subject construction of North China University of Technology (NO:YN-083) and Research Fund of Guangxi Key Lab of Multi-source Information Mining & Security (No. MIMS16-01).

References

- [1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," *ACM Conference on Computer and Communications Security*, pp. 598–609, 2007.
- [2] S. Cornelius, "Best online backup: Backblaze vs crashplan vs carbonite vs dropbox vs sugarsync vs crashplan vs spideroak & more!," May 17, 2016. (<http://www.werockyourweb.com/best-online-backup/>)
- [3] W. Fu Hsien, C. C. Yang, and M. S. Hwang, "A survey of public auditing for secure data storage in cloud computing," *International Journal of Network Security*, vol. 18, no. 1, pp. 133–142, 2016.
- [4] M. S. Hwang, C. C. Lee, T. H. Sun, "Data error locations reported by public auditing in cloud storage service," *Automated Software Engineering*, vol. 21, no. 3, pp. 373–390, 2014.
- [5] M. S. Hwang, T. H. Sun, C. C. Lee, "Achieving dynamic data guarantee and data confidentiality of public auditing in cloud storage service," *Journal of Circuits, Systems, and Computers*, vol. 26, no. 5, 2017. (DOI: 10.1142/S0218126617500724)
- [6] A. Juels, S. Burton, and Jr. Kaliski, "PORS: Proofs of retrievability for large files," in *ACM Conference on Computer and Communications Security*, pp. 584–597, Nov. 2007.
- [7] C. W. Liu, W. Fu Hsien, C. C. Yang, and M. S. Hwang, "A survey of attribute-based access control with user revocation in cloud data storage," *International Journal of Network Security*, vol. 18, no. 5, pp. 900–916, 2016.
- [8] C. W. Liu, W. Fu Hsien, C. C. Yang, and M. S. Hwang, "A survey of public auditing for shared data storage with user revocation in cloud computing," *International Journal of Network Security*, vol. 18, no. 4, pp. 650–666, 2016.
- [9] Y. Ren, J. Shen, J. Wang, J. Han, and S. Lee, "Mutual verifiable provable data auditing in public cloud storage," *Journal of Internet Technology*, vol. 16, no. 2, pp. 317–323, 2015.
- [10] H. Shacham and B. Waters, "Compact proofs of retrievability," *Journal of Cryptology*, vol. 26, no. 3, pp. 442–483, 2013.
- [11] S. T. Shen and W. G. Tzeng, "Delegable provable data possession for remote data in the clouds," *Proceedings of ICICS'11*, pp. 93–111, 2011.
- [12] J. Singh, "Cloud based technique for Blog search optimization," *International Journal of Electronics and Information Engineering*, vol. 4, no. 1, pp. 32–39, 2016.
- [13] M. Stanek, "A note on security protocol for multicast communications," *International Journal of Network Security*, vol. 14, no. 1, pp. 59–60, 2012.
- [14] H. Wang, D. He, and S. Tang, "Identity-based proxy-oriented data uploading and remote data integrity checking in public cloud," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1165–1176, 2016.
- [15] Z. Wang, Y. Lu, G. Sun, "A policy-based deduplication mechanism for securing cloud storage," *International Journal of Electronics and Information Engineering*, vol. 2, no. 2, pp. 70–79, 2015.

- [16] Q. Q. Xi, S. R. Jiang, L. M. Wang, and C. C. Chang, "Composable secure roaming authentication protocol for cloud-assisted body sensor networks," *International Journal of Network Security*, vol. 18, no. 5, pp. 816–831, 2016.
 - [17] J. Zhang and Q. Dong, "Efficient id-based public auditing for the outsourced data in cloud storage," *Information Sciences*, vol. 343-344, no. 2, pp. 1–14, 2016.
 - [18] J. Zhang, P. Li, and J. Mao, "Ipad: Id-based public auditing for the outsourced data in the standard model," *Cluster Computing*, vol. 19, no. 1, pp. 127–138, 2016.
- Pengyan Li** received the BS. in Mathematics and Education from Luoyang Normal University in 2015. She is now a master in College of Science, North China University of Technology. She has published 2 papers in international conferences and journals. His research interest includes applied mathematics, education theory and multimedia processing..
- Min Xu** received the MS. in School of Electronic and Information Engineering from Hebei Normal University in 1998. She is now an Associate Professor in Department of Education, Baoding University. She has published more than 30 papers in international conferences and journals. His research interest includes applied cryptography, web security, computer software and multimedia processing.

Biography

Jianhong Zhang received his Ph.D. degrees in Cryptography from Xidian University, Xian, Shanxi, in 2004 and his M.S. degree in Computer Software from Guizhou University, Guiyang, Guizhou, in 2001. He was engaging in postdoctoral research at Peking University from October 2005 to December 2007. He has been an Assistant Processor of College of Sciences, North China University of Technology, Beijing China, since 2001. His research interests include computer networks, cryptography, electronic commerce security, computer software.

Linear Complexity of Quaternary Sequences Over \mathbb{Z}_4 Derived From Generalized Cyclotomic Classes Modulo $2p$

Zhixiong Chen¹ and Vladimir Edemski²

(Corresponding author: Zhixiong Chen)

School of Mathematics, Putian University, Putian, Fujian 351100, P. R. China¹

Department of Applied Mathematics and Informatics, Novgorod State University, Veliky Novgorod 173003, Russia²

(Email: ptczx@126.com, Vladimir.Edemsky@novsu.ru)

(Received Mar. 31, 2016; revised and accepted June 1 & July 19, 2016)

Abstract

We determine the exact values of the linear complexity (LC) of $2p$ -periodic quaternary sequences over \mathbb{Z}_4 (the residue class ring modulo 4) defined from the generalized cyclotomic classes modulo $2p$ in terms of the theory of Galois rings of characteristic 4, where p is an odd prime. It is more difficult and complicated to consider sequences over \mathbb{Z}_4 than that over finite fields due to the zero divisors in \mathbb{Z}_4 . Hence it brings some interesting twists. We prove the main results as follows

$$\text{LC} = \begin{cases} 2p, & \text{if } p \equiv -3 \pmod{8}, \\ 2p-1, & \text{if } p \equiv 3 \pmod{8}, \\ p, & \text{if } p \equiv -1 \pmod{16}, \\ p+1, & \text{if } p \equiv 1 \pmod{16}, \\ (p+1)/2, & \text{if } p \equiv -9 \pmod{16}, \\ (p+3)/2, & \text{if } p \equiv 9 \pmod{16}, \end{cases}$$

which answers an open problem proposed by Kim, Hong and Song.

Keywords: Cryptography; Galois Rings; Generalized Cyclotomic Classes; Linear Complexity; Quaternary Sequences; Stream Ciphers

1 Introduction

Due to applications of quaternary sequences in communication systems, radar and cryptography [12], it is of interest to design large families of quaternary sequences.

Certain quaternary sequences were defined in the literature¹ by using generalized cyclotomic classes modulo $2p$ for an odd prime p . Let g be an odd number such that g is a primitive root modulo p and modulo $2p$ simultaneously. We note that such g always exists, see [14]. We denote by $\mathbb{Z}_{2p} = \{0, 1, \dots, 2p-1\}$ the

residue class ring modulo $2p$. Put $D_0 = \langle g^2 \rangle = \{g^{2n} \pmod{2p} : n = 0, 1, \dots, (p-3)/2\} \subset \mathbb{Z}_{2p}$, and $D_1 = \{g^{2n+1} \pmod{2p} : n = 0, 1, \dots, (p-3)/2\} \subset \mathbb{Z}_{2p}$. If we write $E_i = \{2u \pmod{2p} : u \in D_i\}$ for $i = 0, 1$, we have the following partition

$$\mathbb{Z}_{2p} = D_0 \cup D_1 \cup E_0 \cup E_1 \cup \{0, p\}.$$

We remark that $D_0 \cup D_1$ is exactly the set of all odd numbers in $\mathbb{Z}_{2p} \setminus \{p\}$ and $E_0 \cup E_1$ is exactly the set of all even numbers in $\mathbb{Z}_{2p} \setminus \{0\}$.

In terms of the generalized cyclotomic classes above, Chen and Du [5] defined a family of quaternary sequences $(e_u)_{u \geq 0}$ with elements in the finite field $\mathbb{F}_4 = \{0, 1, \alpha, 1 + \alpha\}$ as

$$e_u = \begin{cases} 0, & \text{if } u = 0 \text{ or } u \in D_0, \\ 1, & \text{if } u \in D_1, \\ 1 + \alpha, & \text{if } u = p \text{ or } u \in E_0, \\ \alpha, & \text{if } u \in E_1. \end{cases}$$

They determined the linear complexity of $(e_u)_{u \geq 0}$ in [5]. Later Ke, Yang and Zhang [15] calculated their autocorrelation values.² In fact, before [5, 15] Kim, Hong and Song [17] defined another family of quaternary sequences $(s_u)_{u \geq 0}$ with elements in $\mathbb{Z}_4 = \{0, 1, 2, 3\}$, the residue class ring modulo 4, as follows

$$s_u = \begin{cases} 0, & \text{if } u = 0 \text{ or } u \in D_0, \\ 1, & \text{if } u \in D_1, \\ 2, & \text{if } u = p \text{ or } u \in E_0, \\ 3, & \text{if } u \in E_1. \end{cases} \quad (1)$$

They derived the periodic autocorrelation function of $(s_u)_{u \geq 0}$. However, as we know, the question about the

¹The generalized cyclotomic classes modulo $2p$ are also used to define binary sequences [3, 4, 7, 11, 26].

²Ke and Zhang extended to define quaternary cyclotomic sequences of length $2p^m$ [16]. Chang and Li defined quaternary cyclotomic sequences of length $2pq$ [1]. Both are over the finite field \mathbb{F}_4 .

linear complexity of $(s_u)_{u \geq 0}$ is still open due to the phenomenon of zero divisors in \mathbb{Z}_4 . In this work, we will develop a way to solve this problem using the theory of Galois rings of characteristic 4. We note that there are many quaternary sequences over \mathbb{Z}_4 have been investigated in the literature, see e.g., [2, 8, 9, 10, 21, 22, 25].

We recall that the *linear complexity* $LC((s_u)_{u \geq 0})$ of $(s_u)_{u \geq 0}$ above is the least order L of a linear recurrence relation (i.e., linear feedback shift register, or LFSR for short) over \mathbb{Z}_4

$$s_{u+L} + c_1 s_{u+L-1} + \dots + c_{L-1} s_{u+1} + c_L s_u = 0 \quad \text{for } u \geq 0,$$

which is satisfied by $(s_u)_{u \geq 0}$ and where $c_1, c_2, \dots, c_L \in \mathbb{Z}_4$, see [23]. The *connection polynomial* is $C(X)$ given by $1 + c_1 X + \dots + c_L X^L$. We note that $C(0) = 1$. Let

$$S(X) = s_0 + s_1 X + \dots + s_{2p-1} X^{2p-1} \in \mathbb{Z}_4[X]$$

be the *generating polynomial* of $(s_u)_{u \geq 0}$. Then an LFSR with a connection polynomial $C(X)$ generates $(s_u)_{u \geq 0}$, if and only if [23],

$$S(X)C(X) \equiv 0 \pmod{X^{2p} - 1},$$

where $C(X) \in \mathbb{Z}_4[X]$ satisfies $C(0) = 1$. That is,

$$LC((s_u)) = \min\{\deg(C(X)) : C(X) \in \mathbb{Z}_4[X], C(0) = 1, S(X)C(X) \equiv 0 \pmod{X^{2p} - 1}\}. \quad (2)$$

Let r be the order of 2 modulo p . We denote by $GR(4^r, 4)$ the Galois ring of order 4^r of characteristic 4, which is isomorphic to the residue class ring $\mathbb{Z}_4[X]/(f(X))$, where $f(X) \in \mathbb{Z}_4[X]$ is a *basic irreducible polynomial* of degree r [24, 19]. The group of units of $GR(4^r, 4)$, denoted by $GR^*(4^r, 4)$, contains a cyclic subgroup of order $2^r - 1$. Since $p \mid (2^r - 1)$, let $\beta \in GR^*(4^r, 4)$ be of order p . Then we find that $\gamma = 3\beta \in GR^*(4^r, 4)$ is of order $2p$ ³. From Equation (2), we will consider the values $S(\gamma^v)$ for $v = 0, 1, \dots, 2p-1$, which allow us to derive the linear complexity of $(s_u)_{u \geq 0}$. Due to $S(X) \in \mathbb{Z}_4[X]$, we cannot consider it in the same way as those in finite fields. For example, 1 and 3 are the roots of $2X - 2 \in \mathbb{Z}_4[X]$, but $2X - 2$ is not divisible by $(X - 1)(X - 3)$, i.e., in the ring $\mathbb{Z}_4[X]$ the number of roots of a polynomial can be greater than its degree. So we need to develop some necessary technique here. Indeed, the theory of Galois ring enters into our problem by means of the following lemmas.

Lemma 1. *Let $P(X) \in \mathbb{Z}_4[X]$ be a non-constant polynomial. If $\xi \in GR(4^r, 4)$ is a root of $P(X)$, we have $P(X) = (X - \xi)Q_1(X)$ for some polynomial $Q_1(X) \in GR(4^r, 4)[X]$.*

Furthermore, if $\eta \in GR(4^r, 4)$ is another root of $P(X)$ and $\eta - \xi$ is a unit, we have $P(X) = (X - \xi)(X - \eta)Q_2(X)$, where $Q_1(X) = (X - \eta)Q_2(X)$.

Lemma 2. *Let $\gamma \in GR^*(4^r, 4)$ be of order $2p$, and let $P(X) \in \mathbb{Z}_4[X]$ be any non-constant polynomial.*

(I). *If $P(\gamma^v) = 0$ for all $v \in D_i$, where $i = 0, 1$, then we have*

$$P(X) = P_1(X) \prod_{v \in D_i} (X - \gamma^v)$$

for some polynomial $P_1(X) \in GR(4^r, 4)[X]$. Similarly, If $P(\gamma^v) = 0$ for all $v \in E_i$, where $i = 0, 1$, then we have

$$P(X) = P_2(X) \prod_{v \in E_i} (X - \gamma^v)$$

for some polynomial $P_2(X) \in GR(4^r, 4)[X]$.

(II). *If $P(\gamma^v) = 0$ for all $v \in \{p\} \cup D_0 \cup D_1$, then we have*

$$P(X) = P_3(X)(X^p + 1)$$

for some polynomial $P_3(X) \in GR(4^r, 4)[X]$. Similarly, if $P(\gamma^v) = 0$ for all $v \in \{0\} \cup E_0 \cup E_1$, then we have

$$P(X) = P_4(X)(X^p - 1)$$

for some polynomial $P_4(X) \in \mathbb{Z}_4[X]$.

(III). *If $P(0) = 1$, $P(\gamma^v) = 0$ for $v \in \mathbb{Z}_{2p} \setminus \{0, p\}$, and $P(\pm 1) \in \{0, 2\}$, then we have $\deg P(X) \geq 2p - 1$. Furthermore, if either $P(1) = P(-1) = 0$ or $P(1) = P(-1) = 2$, we have $\deg P(X) \geq 2p$.*

We give a proof of both lemmas in the Appendix for the convenience of the reader.

2 Linear Complexity of $(s_u)_{u \geq 0}$

2.1 Auxiliary Lemmas

We describe a relationship among D_0, D_1, E_0 and E_1 .

Lemma 3. *Let $i, j \in \{0, 1\}$.*

(I). *For $v \in D_i$, we have*

$$vD_j \triangleq \{vu \pmod{2p} : u \in D_j\} = D_{i+j \bmod 2},$$

and

$$vE_j \triangleq \{vu \pmod{2p} : u \in E_j\} = E_{i+j \bmod 2}.$$

(II). *For $v \in E_i$, we have*

$$vD_j \triangleq \{vu \pmod{2p} : u \in D_j\} = E_{i+j \bmod 2},$$

and

$$vE_j \triangleq \{vu \pmod{2p} : u \in E_j\} = E_{i+j \bmod 2}$$

if $p \equiv \pm 1 \pmod{8}$, and otherwise

$$vE_j \triangleq \{vu \pmod{2p} : u \in E_j\} = E_{i+j+1 \bmod 2}.$$

³In the context we always suppose that $\gamma \in GR^*(4^r, 4)$ is of order $2p$.

(III). If $p \equiv \pm 1 \pmod{8}$, we have

$$D_i = \{(v + p) \pmod{2p} : v \in E_i\},$$

and otherwise

$$D_{i+1 \bmod 2} = \{(v + p) \pmod{2p} : v \in E_i\}.$$

(IV). If $p \equiv \pm 1 \pmod{8}$, we have

$$E_i = \{(v + p) \pmod{2p} : v \in D_i\},$$

and otherwise

$$E_{i+1 \bmod 2} = \{(v + p) \pmod{2p} : v \in D_i\}.$$

(V). If $p \equiv \pm 1 \pmod{8}$, we have

$$E_i = \{u + p : u \in D_i, u < p\} \cup \{u - p : u \in D_i, u > p\}.$$

Proof.

(I). If $v \in D_i$ for $i = 0, 1$ and $u \in D_j$ for $j = 0, 1$ then we can write $v \equiv g^{i+2k} \pmod{2p}$, $0 \leq k \leq (p-3)/2$ and $u \equiv g^{j+2l} \pmod{2p}$, $0 \leq l \leq (p-3)/2$. So, $vu \equiv g^{i+j+2k+2l} \pmod{2p}$, which implies $vu \in D_{i+j \bmod 2}$. Since $|vD_i| = |D_{i+j \bmod 2}|$, it follows that $vD_i = D_{i+j \bmod 2}$. The equality $vE_j = E_{i+j+1 \bmod 2}$ can be proved similarly.

(II). Let $v \in E_i$. We write $v \equiv 2u \pmod{2p}$, $u \in D_i$. Therefore, by (I) and our definitions we have

$$vD_j = 2uD_j = 2D_{i+j \bmod 2} = E_{i+j \bmod 2}.$$

Now, we consider vE_j . First, we have by (I) again

$$vE_j = 2uE_j = 2E_{i+j \bmod 2}.$$

Second, for any $w \in 2E_{i+j \bmod 2}$, we can write $w \equiv 4a \pmod{2p}$ for $a \in D_{i+j \bmod 2}$. Clearly w is even and $w \in E_0 \cup E_1$, so we get $w \equiv 2b \pmod{2p}$ for $b \in D_0 \cup D_1$. Then we have $b \equiv 2a \pmod{p}$.

For $p \equiv \pm 1 \pmod{8}$, in which case 2 is a quadratic residue modulo p [14], we have $b \in D_{i+j \bmod 2}$, which leads to $w \equiv 2b \pmod{2p} \in E_{i+j \bmod 2}$, i.e., $2E_{i+j \bmod 2} \subseteq E_{i+j \bmod 2}$. Since $2E_{i+j \bmod 2}$ and $E_{i+j \bmod 2}$ have the same cardinality, it follows that $vE_j = 2E_{i+j \bmod 2} = E_{i+j \bmod 2}$.

The case of $p \equiv \pm 3 \pmod{8}$ follows in a similar way, in which case 2 is a quadratic non-residue modulo p .

(III). Let $p \equiv \pm 1 \pmod{8}$, since 2 is a quadratic residue modulo p [14], we can find when \bar{v} runs through D_0 (resp. D_1), $p + 2\bar{v}$ modulo $2p$ runs through D_0 (resp. D_1). Since otherwise, if $p + 2\bar{v}_0 \pmod{2p} \in D_1$ for some $\bar{v}_0 \in D_1$, then we write $p + 2\bar{v}_0 \equiv g^{1+2k_0} \pmod{2p}$ for some integer k_0 , from which we derive $2\bar{v}_0 \equiv g^{1+2k_0} \pmod{p}$. It leads to the result that 2 is a quadratic non-residue modulo p , a contradiction.

So, $D_i = \{(v + p) \pmod{2p} : v \in E_i\}$ if $p \equiv \pm 1 \pmod{8}$.

The equality $D_{i+1 \bmod 2} = \{(v + p) \pmod{2p} : v \in E_i\}$ for $p \equiv \pm 3 \pmod{8}$ is proved similarly as the first. Here, if \bar{v} runs through D_0 (resp. D_1), then $p + 2\bar{v}$ modulo $2p$ runs through D_1 (resp. D_0).

(IV). Comes from (III).

(V). In fact first, the set

$$\{u + p : u \in D_1, u < p\} \cup \{u - p : u \in D_1, u > p\}$$

exactly contains $|D_1|$ even numbers. Second, we suppose that $a \in E_0$ for some

$$a \in \{u + p : u \in D_1, u < p\} \cup \{u - p : u \in D_1, u > p\}.$$

Write $a \equiv 2v \pmod{2p}$ for some $v \in D_0$. From the definition of D_0 , we see that v is a quadratic residue modulo p . Then a is a quadratic residue modulo p due to $p \equiv \pm 1 \pmod{8}$, in which case 2 is a quadratic residue modulo p [14]. However, a is of the form $u + p$ or $u - p$ for some $u \in D_1$, and $a \equiv u \pmod{p}$ is a quadratic non-residue modulo p , a contradiction. So

$$\{u + p : u \in D_1, u < p\} \cup \{u - p : u \in D_1, u > p\} \subseteq E_1,$$

and both have the same cardinality. \square

For $i = 0, 1$, let

$$S_i(X) = \sum_{u \in D_i} X^u$$

and

$$T_i(X) = S_i(X^2) = \sum_{u \in E_i} X^u \pmod{X^{2p} - 1}.$$

According to Equation (1), the generating polynomial of $(s_u)_{u \geq 0}$ is

$$S(X) = 2X^p + S_1(X) + 2T_0(X) + 3T_1(X). \quad (3)$$

As mentioned before, we will consider the values $S(\gamma^v)$ for a unit $\gamma \in GR^*(4^r, 4)$ of order $2p$ and $v = 0, 1, \dots, 2p-1$. According to the definitions of D_0, D_1, E_0 and E_1 , we will describe $S(\gamma^v)$ in the following lemma in terms of $S_0(\gamma)$ (or $S_1(\gamma)$) due to the fact that in the ring $GR(4^r, 4)$

$$S_0(\gamma) + S_1(\gamma) = \sum_{u \in D_0 \cup D_1} \gamma^u = \sum_{j=0}^{p-1} \gamma^{2j+1} - \gamma^p = 1. \quad (4)$$

Lemma 4. Let $\gamma \in GR^*(4^r, 4)$ be of order $2p$, and let $S(X)$ be the generating polynomial of $(s_u)_{u \geq 0}$ described in Equation (3).

(I). If $p \equiv \pm 3 \pmod{8}$, we have

$$S(\gamma^v) = \begin{cases} 1 - 2S_0(\gamma), & \text{if } v \in D_0, \\ -1 + 2S_0(\gamma), & \text{if } v \in D_1, \\ 3, & \text{if } v \in E_0 \cup E_1. \end{cases}$$

(II). If $p \equiv \pm 1 \pmod{8}$, we have

$$S(\gamma^v) = \begin{cases} 0, & \text{if } v \in D_0 \cup D_1, \\ 2 - 2S_0(\gamma), & \text{if } v \in E_0, \\ 2S_0(\gamma), & \text{if } v \in E_1. \end{cases}$$

Proof.

(I). Let $p \equiv \pm 3 \pmod{8}$. By Lemma 3(I) we first get

$$S_1(\gamma^v) = \begin{cases} 1 - S_0(\gamma), & \text{if } v \in D_0, \\ S_0(\gamma), & \text{if } v \in D_1. \end{cases}$$

Second, for any $v \in E_j$ for $j \in \{0, 1\}$, write $v = 2\bar{v}$ for $\bar{v} \in D_j$. We see that $p + 2\bar{v} \in D_{j+1}$ by Lemma 3(III) and $\gamma^v = \gamma^{2\bar{v}} = -\gamma^{p+2\bar{v}}$, by Lemma 3(I) we derive

$$\begin{aligned} S_1(\gamma^v) &= S_1(-\gamma^{p+2\bar{v}}) = - \sum_{u \in D_1} \gamma^{u(p+2\bar{v})} \\ &= \begin{cases} - \sum_{w \in D_0} \gamma^w, & \text{if } \bar{v} \in D_0, \\ - \sum_{w \in D_1} \gamma^w, & \text{if } \bar{v} \in D_1, \end{cases} \end{aligned}$$

which leads to

$$S_1(\gamma^v) = \begin{cases} -S_0(\gamma), & \text{if } v \in E_0, \\ -1 + S_0(\gamma), & \text{if } v \in E_1. \end{cases}$$

Similarly, by Lemma 3(I)-(IV), we have

$$T_0(\gamma^v) = \begin{cases} -1 + S_0(\gamma), & \text{if } v \in D_0, \\ -S_0(\gamma), & \text{if } v \in D_1, \\ S_0(\gamma), & \text{if } v \in E_0, \\ 1 - S_0(\gamma), & \text{if } v \in E_1, \end{cases}$$

and

$$T_1(\gamma^v) = \begin{cases} -S_0(\gamma), & \text{if } v \in D_0, \\ -1 + S_0(\gamma), & \text{if } v \in D_1, \\ 1 - S_0(\gamma), & \text{if } v \in E_0, \\ S_0(\gamma), & \text{if } v \in E_1. \end{cases}$$

Then putting everything together, we get the first assertion.

The second assertion of this lemma can be proved in a similar way.

So in order to determine the values of $S(\gamma^v)$, it is sufficient to calculate $S_0(\gamma)$. We need the parameter $[i, j]$ for $i, j \in \{0, 1\}$, which is the cardinality of the set $(1 + D_i) \cap E_j$, i.e.,

$$[i, j] = |(1 + D_i) \cap E_j|,$$

where $1 + D_i = \{1 + u \pmod{2p} : u \in D_i\}$.

Lemma 5. With notations as before. We have

$$[0, 0] = \begin{cases} (p-5)/4, & \text{if } p \equiv 1 \pmod{8}, \\ (p-3)/4, & \text{if } p \equiv 7 \pmod{8}, \\ (p-1)/4, & \text{if } p \equiv 5 \pmod{8}, \\ (p+1)/4, & \text{if } p \equiv 3 \pmod{8}, \end{cases}$$

and

$$[0, 1] = \begin{cases} (p-1)/4, & \text{if } p \equiv 1 \pmod{8}, \\ (p+1)/4, & \text{if } p \equiv 7 \pmod{8}, \\ (p-5)/4, & \text{if } p \equiv 5 \pmod{8}, \\ (p-3)/4, & \text{if } p \equiv 3 \pmod{8}, \end{cases}$$

Proof. Since g used above is also a primitive modulo p , we write

$$H_0 = \{g^{2n} \pmod{p} : n = 0, 1, \dots, (p-3)/2\}$$

and

$$H_1 = \{g^{1+2n} \pmod{p} : n = 0, 1, \dots, (p-3)/2\}.$$

We find that for $i = 0, 1$

$$\{u \pmod{p} : u \in D_i\} = H_i$$

and

$$\{2u \pmod{p} : u \in D_i\} = H_{i+\ell \bmod 2},$$

where $\ell = 0$ if $p \equiv \pm 1 \pmod{8}$ and $\ell = 1$ if $p \equiv \pm 3 \pmod{8}$, i.e., $\ell = 0$ if 2 is a quadratic residue modulo p , and $\ell = 1$ otherwise [14]. Therefore,

$$[i, j] = |(1 + D_i) \cap E_j| = |(1 + H_i) \cap H_{j+\ell \bmod 2}|.$$

We conclude the proof by applying the values of $|(1 + H_i) \cap H_j|$ computed in [13]. \square

With the values of $[0, 0]$ and $[0, 1]$, we prove the following statement, which is a generalization of [6, Theorem 1].

Lemma 6. Let $\gamma \in GR^*(4^r, 4)$ be of order $2p$. Then we have

$$(S_0(\gamma))^2 = S_0(\gamma) + \begin{cases} (p-1)/4, & \text{if } p \equiv 1 \pmod{8}, \\ (p+1)/4, & \text{if } p \equiv -1 \pmod{8}, \\ (p+1)/4, & \text{if } p \equiv 3 \pmod{8}, \\ (p-1)/4, & \text{if } p \equiv -3 \pmod{8}. \end{cases}$$

Proof. By the definition of $S_0(X)$ we have

$$(S_0(\gamma))^2 = \sum_{l,m=0}^{(p-3)/2} \gamma^{g^{2l}+g^{2m}} = \sum_{l,m=0}^{(p-3)/2} \gamma^{g^{2m}(g^{2(l-m)}+1)}.$$

For each fixed m , since the order of g modulo $2p$ is $p-1$, we see that $l-m$ modulo $(p-1)$ runs through the range $0, 1, \dots, (p-3)/2$ if l does. So we have

$$(S_0(\gamma))^2 = \sum_{m,n=0}^{(p-3)/2} \gamma^{g^{2m}(g^{2n}+1)}. \quad (5)$$

Since g is odd, we see that $g^{2n} + 1 \pmod{2p}$ is even for any n . That is, $g^{2n} + 1 \pmod{2p} \in E_0 \cup E_1 \cup \{0\}$. So we consider $g^{2n} + 1 \pmod{2p}$ in three different cases.

Case 1. Let

$$N_0 = \{n : 0 \leq n \leq (p-3)/2, g^{2n} + 1 \pmod{2p} \in E_0\}.$$

In fact, the cardinality $|N_0|$ of N_0 equals $[0, 0]$. For each $n \in N_0$, as the proof of Lemma 4 we obtain that by Equation (4)

$$\begin{aligned} \sum_{m=0}^{(p-3)/2} \gamma^{g^{2m}(g^{2n}+1)} &= \sum_{v \in D_0} \gamma^{2v} = S_0(\gamma^2) = S_0(-\gamma^{p+2}) \\ &= \begin{cases} -S_0(\gamma), & \text{if } p \equiv \pm 1 \pmod{8}, \\ -1 + S_0(\gamma), & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases} \end{aligned}$$

Case 2. Similar to Case 1, we let

$$N_1 = \{n : 0 \leq n \leq (p-3)/2, g^{2n} + 1 \pmod{2p} \in E_1\}.$$

Then the cardinality $|N_1|$ equals $[0, 1]$. Now for each $n \in N_1$, we obtain that

$$\begin{aligned} \sum_{m=0}^{(p-3)/2} \gamma^{g^{2m}(g^{2n}+1)} &= \sum_{v \in D_1} \gamma^{2v} = S_1(\gamma^2) = S_1(-\gamma^{p+2}) \\ &= \begin{cases} -1 + S_0(\gamma), & \text{if } p \equiv \pm 1 \pmod{8}, \\ -S_0(\gamma), & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases} \end{aligned}$$

Case 3. There is an n such that $(g^{2n} + 1) \equiv 0 \pmod{2p}$ if and only if $p \equiv 1 \pmod{4}$. In this case, we have $n = (p-1)/4$ and $\sum_{m=0}^{(p-3)/2} \gamma^{g^{2m}(g^{2n}+1)} = (p-1)/2$. Let $p \equiv 1 \pmod{8}$. Using Equation (5) we obtain that

$$(S_0(\gamma))^2 = |N_0| \cdot (-S_0(\gamma)) + |N_1| \cdot (-1 + S_0(\gamma)) + (p-1)/2.$$

Then we get the desired result by using the values of $[0, 0]$ ($=|N_0|$) and $[0, 1]$ ($=|N_1|$) in Lemma 5.

The assertions for $p \equiv -1, 3, -3 \pmod{8}$ can be obtained in a similar way. \square

With the help of Lemma 6 we now deduce the values of $S_0(\gamma)$. It is clear that $S_0(\gamma) \in GR^*(4^r, 4)$ or $S_1(\gamma) \in GR^*(4^r, 4)$ from Equation (4). Therefore, without loss of generality we always suppose that $S_0(\gamma) \in GR^*(4^r, 4)$. (Of course, if one supposes that $S_1(\gamma) \in GR^*(4^r, 4)$, then $S_1(\gamma)$ will be used in the context.)

Lemma 7. Let $\gamma \in GR^*(4^r, 4)$ be of order $2p$ with $S_0(\gamma) = \sum_{u \in D_0} \gamma^u \in GR^*(4^r, 4)$. We have

$$S_0(\gamma) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod{16}, \\ \rho, & \text{if } p \equiv \pm 5 \pmod{16}, \\ 3, & \text{if } p \equiv \pm 9 \pmod{16}, \\ 2 + \rho, & \text{if } p \equiv \pm 13 \pmod{16}, \end{cases}$$

where ρ satisfies the equation $\rho^2 + 3\rho + 3 = 0$ over \mathbb{Z}_4 .

Proof. Let $p \equiv \pm 1 \pmod{16}$. Then, by Lemma 6, we obtain that $(S_0(\gamma))^2 = S_0(\gamma)$. Under given assumptions about $S_0(\gamma)$, we have $S_0(\gamma) = 1$. The other assertions of this lemma can be proved in a similar way. \square

Lemma 8. Let $\gamma \in GR^*(4^r, 4)$ be of order $2p$ with $S_0(\gamma) = \sum_{u \in D_0} \gamma^u \in GR^*(4^r, 4)$, and let $S(X)$ be the generating polynomial of $(s_u)_{u \geq 0}$ described in Equation (3).

(I). For any odd prime p , we have

$$S(\gamma^v) = \begin{cases} p+1, & \text{if } v = 0, \\ 2, & \text{if } v = p. \end{cases}$$

(II). If $p \equiv \pm 3 \pmod{8}$, we have

$$S(\gamma^v) \in GR^*(4^r, 4), \text{ for all } v \in D_0 \cup D_1 \cup E_0 \cup E_1.$$

(III). If $p \equiv \pm 1 \pmod{8}$, we have

$$S(\gamma^v) = \begin{cases} 0, & \text{if } v \in D_0 \cup D_1 \cup E_0, \\ 2, & \text{if } v \in E_1. \end{cases}$$

Proof. (I) can be checked easily. (II) and (III) follow immediately from Lemmas 4 and 7. \square

In the following subsections, we will derive linear complexity of $(s_u)_{u \geq 0}$ in Equation (2) by considering the factorization of $S(X)$.

2.2 Linear Complexity for the Case $p \equiv \pm 3 \pmod{8}$

Theorem 1. Let $(s_u)_{u \geq 0}$ be the quaternary sequence over \mathbb{Z}_4 defined by Equation (1). Then the linear complexity of $(s_u)_{u \geq 0}$ satisfies

$$LC((s_u)_{u \geq 0}) = \begin{cases} 2p, & \text{if } p \equiv -3 \pmod{8}, \\ 2p-1, & \text{if } p \equiv 3 \pmod{8}. \end{cases}$$

Proof. With notations as before. That is, we use $S(X)$ the generating polynomial of $(s_u)_{u \geq 0}$ and let $\gamma \in GR^*(4^r, 4)$ be of order $2p$ with $S_0(\gamma) = \sum_{u \in D_0} \gamma^u \in GR^*(4^r, 4)$. Suppose that $C(X) \in \mathbb{Z}_4[X]$ is a connection polynomial of $(s_u)_{u \geq 0}$. We remark that $\min \deg(C(X)) \leq 2p$.

For $p \equiv \pm 3 \pmod{8}$, by Equation (2) and Lemma 8(II) we get

$$C(\gamma^v) = 0 \text{ for all } v \in D_0 \cup D_1 \cup E_0 \cup E_1.$$

Now we consider the values of $C(\gamma^0)$ and $C(\gamma^p)$.⁴ Let $s(X)$ and $c(X)$ be the polynomials of degree < 2 such that

$$S(X) \equiv s(X) \pmod{X^2 - 1}$$

and

$$C(X) \equiv c(X) \pmod{X^2 - 1}.$$

If $p \equiv -3 \pmod{8}$, we have $S(-1) = S(1) = 2$ by Lemma 8(I). It follows that $s(X) = 2$ or $s(X) = 2X$. So by Equation (2) again, we see that

$$c(X) \in \{0, 2, 2X, 2X + 2\}$$

⁴In fact, $C(\gamma^0) = C(1)$ and $C(\gamma^p) = C(-1)$.

and hence either $C(-1) = C(1) = 0$ or $C(-1) = C(1) = 2$.

In terms of all values of $C(\gamma^v)$ for $v = 0, 1, \dots, 2p - 1$ above, by Lemma 2(III) we have $\deg C(X) \geq 2p$. Consequently, we get $\min \deg(C(X)) = 2p$ and hence $LC((s_u)_{u \geq 0}) = 2p$ for this case.

Similarly if $p \equiv 3 \pmod{8}$, we have $S(1) = 0$ and $S(-1) = 2$ by Lemma 8(I), and hence $s(X) = 1 - X$. Then we get

$$c(X) \in \{0, 2, X + 1, 2X + 2\}$$

and hence $C(-1) = C(1) = 0$, or $C(-1) = C(1) = 2$, or $C(-1) = 0$ and $C(1) = 2$. Then by Lemma 2(III) we have $\deg C(X) \geq 2p - 1$.

On the other hand, since $s(X) = 1 - X$, we see that $S(X)$ is divisible by $X - 1$ over \mathbb{Z}_4 , from which we derive

$$S(X) \cdot \frac{X^{2p} - 1}{X - 1} \equiv 0 \pmod{X^{2p} - 1}.$$

Then $\frac{X^{2p} - 1}{X - 1}$ is a connection polynomial of $(s_u)_{u \geq 0}$. So we get $\min \deg(C(X)) = 2p - 1$, i.e., $LC((s_u)_{u \geq 0}) = 2p - 1$. \square

2.3 Linear Complexity for the Case $p \equiv \pm 1 \pmod{8}$

Due to Lemma 8(III), it is more complicated to determine the connection polynomial $C(X)$ with the smallest degree when $p \equiv \pm 1 \pmod{8}$. For $j = 0, 1$, define

$$\Gamma_j(X) = \prod_{v \in D_j} (X - \gamma^v) \text{ and } \Lambda_j(X) = \prod_{v \in E_j} (X - \gamma^v),$$

where $\gamma \in GR^*(4^r, 4)$ is of order $2p$ with $S_0(\gamma) = \sum_{u \in D_0} \gamma^u \in GR^*(4^r, 4)$. In particular, by Lemma 3(IV) we have for $j = 0, 1$,

$$\Lambda_j(X) = \prod_{v \in D_j} (X - \gamma^{v+p}).$$

Lemma 9. If $p \equiv \pm 1 \pmod{8}$, then $\Gamma_j(X)$ and $\Lambda_j(X)$ are polynomials over \mathbb{Z}_4 for $j = 0, 1$.

Proof. We only consider $\Gamma_0(X)$ here, for $\Gamma_1(X)$, $\Lambda_0(X)$ and $\Lambda_1(X)$ it can be done in a similar manner. It is sufficient to show that the coefficients of $\Gamma_0(X)$

$$a_m = (-1)^m \sum_{\substack{i_1 < i_2 < \dots < i_m \\ i_1, i_2, \dots, i_m \in D_0}} \gamma^{i_1 + i_2 + \dots + i_m} \in \mathbb{Z}_4$$

for $1 \leq m \leq (p-1)/2$.

Let γ^b be a term of the last sum and $b \equiv i_1 + i_2 + \dots + i_m \pmod{2p}$, $b \not\equiv 0 \pmod{p}$. By Lemma 3 for any $n : 0 < n < (p-1)/2$ we have that $g^{2^n} i_j \in D_0, j = 0, \dots, m$. Hence, $X - \gamma^{g^{2^n} i_j}, j = 0, \dots, m$ are the factors in the product $\prod_{v \in D_j} (X - \gamma^v)$. So, $\gamma^{g^{2^n} i_1} \dots \gamma^{g^{2^n} i_m} = \gamma^{g^{2^n} b}$ is also a term of this sum for any $n = 0, \dots, (p-3)/2$, i.e.,

$$\gamma^b + \gamma^{g^{2b}} + \dots + \gamma^{g^{p-3b}} = S_0(\gamma^b)$$

is a part of this sum. Therefore, there must exist the elements b_1, \dots, b_n such that

$$a_m = (-1)^m \sum_{i=0}^n S_0(\gamma^{b_i}) + A,$$

where

$$A = |\{a | a \equiv (i_1 + i_2 + \dots + i_m) \equiv 0 \pmod{p} \text{ and } i_1 < i_2 < \dots < i_m; i_1, i_2, \dots, i_m \in D_0\}|.$$

By Lemma 7 and the proof of Lemma 4 we have that $S_0(\gamma^{b_i}) \in \mathbb{Z}_4$. This completes the proof of Lemma 9. \square

Since γ^v is a root of $X^p + 1$ for any $v \in \{p\} \cup D_0 \cup D_1$, and $\gamma^{v_1} - \gamma^{v_2} \in GR^*(4^r, 4)$ for distinct $v_1, v_2 \in \{p\} \cup D_0 \cup D_1$, it follows that

$$X^p + 1 = (X + 1)\Gamma_0(X)\Gamma_1(X), \quad (6)$$

from Lemma 2 and the definitions on $\Gamma_0(X)$ and $\Gamma_1(X)$. Similarly, we have

$$X^p - 1 = (X - 1)\Lambda_0(X)\Lambda_1(X). \quad (7)$$

Now, let us explore the expansion of

$$S(X) = 2X^p + S_1(X) + 2T_0(X) + 3T_1(X).$$

Lemma 10. We have the polynomial factoring in the ring $\mathbb{Z}_4[X]$

$$S_1(X) + 3T_1(X) = \begin{cases} (X^p - 1)\Gamma_0(X)U_1(X), & \text{if } p \equiv \pm 1 \pmod{16}, \\ (X^p - 1)\Gamma_0(X)U_2(X) + 2(X^p + 1), & \text{if } p \equiv \pm 9 \pmod{16}, \end{cases}$$

and

$$2X^p + 2T_0(X) = \begin{cases} \Gamma_0(X)\Lambda_0(X)(X - 1)V_1(X) + 2(X^p + 1), & \text{if } p \equiv -1, -9 \pmod{16}, \\ \Gamma_0(X)\Lambda_0(X)V_2(X) + 2(X^p + 1), & \text{if } p \equiv 1, 9 \pmod{16}, \end{cases}$$

where $U_i(X), V_i(X) \in \mathbb{Z}_4[X], i = 1, 2$.

Proof. Since $p \equiv \pm 1 \pmod{8}$, by Lemma 3(V) we obtain

$$\begin{aligned} S_1(X) + 3T_1(X) &= \sum_{u \in D_1} X^u + 3 \sum_{u \in E_1} X^u \\ &= \sum_{\substack{u \in D_1 \\ u < p}} X^u + \sum_{\substack{u \in D_1 \\ u > p}} X^u + 3 \sum_{\substack{u \in D_1 \\ u < p}} X^{u+p} + 3 \sum_{\substack{u \in D_1 \\ u > p}} X^{u-p} \\ &= (X^p + 3) \left(3 \sum_{\substack{u \in D_1 \\ u < p}} X^u + \sum_{\substack{u \in D_1 \\ u > p}} X^{u-p} \right). \end{aligned}$$

Write

$$M(X) = 3 \sum_{\substack{u \in D_1 \\ u < p}} X^u + \sum_{\substack{u \in D_1 \\ u > p}} X^{u-p}.$$

With the choice of γ as before, if $v \in D_0$, we have

$$\begin{aligned} M(\gamma^v) &= 3 \sum_{\substack{u \in D_1 \\ u < p}} \gamma^{vu} + \sum_{\substack{u \in D_1 \\ u > p}} \gamma^{v(u-p)} \\ &= - \sum_{\substack{u \in D_1 \\ u < p}} \gamma^{vu} - \sum_{\substack{u \in D_1 \\ u > p}} \gamma^{vu} \\ &= -S_1(\gamma) = -1 + S_0(\gamma), \end{aligned}$$

where we use $\gamma^p = -1$ and Equation (4). So for $v \in D_0$, by Lemma 7 we get

$$M(\gamma^v) = \begin{cases} 0, & \text{if } p \equiv \pm 1 \pmod{16}, \\ 2, & \text{if } p \equiv \pm 9 \pmod{16}, \end{cases}$$

from which, and by Lemma 2, we derive

$$M(X) = \begin{cases} \Gamma_0(X)U_1(X), & \text{if } p \equiv \pm 1 \pmod{16}, \\ 2 + \Gamma_0(X)U_2(X), & \text{if } p \equiv \pm 9 \pmod{16}, \end{cases}$$

where $U_1(X), U_2(X) \in \mathbb{Z}_4[X]$. We complete the proof of the first statement.

Now, we consider the polynomial $2X^p + 2T_0(X)$. Since $2X^p + 2T_0(X) = 2(X^p + 1) + 2 + 2T_0(X)$, we only need to consider $2 + 2T_0(X)$.

We first consider the roots of $2 + 2S_0(X)$. According to the proof of Lemma 4, we see that $p + 2 \in D_0$ since $p \equiv \pm 1 \pmod{8}$. For any $v \in E_0$ with $v \equiv 2\bar{v} \pmod{2p}$, where $\bar{v} \in D_0$, we obtain by Equation (4) and Lemma 7

$$\begin{aligned} 2 + 2S_0(\gamma^v) &= 2 + 2 \sum_{u \in D_0} \gamma^{uv} = 2 + 2 \sum_{u \in D_0} \gamma^{2\bar{v}u} \\ &= 2 + 2S_0(\gamma^2) = 2 + 2S_0(-\gamma^{p+2}) \\ &= 2 - 2S_0(\gamma) = 0. \end{aligned}$$

So, by Lemma 2 we have

$$2 + 2S_0(X) = \Lambda_0(X)G(X)$$

for some $G(X) \in \mathbb{Z}_4[X]$, then we have

$$2 + 2S_0(X^2) = \Lambda_0(X^2)G(X^2).$$

Since $T_0(X) = S_0(X^2) \pmod{X^{2p} - 1}$ and

$$\begin{aligned} \Lambda_0(X^2) &= \prod_{v \in E_0} (X^2 - \gamma^v) = \prod_{u \in D_0} (X^2 - \gamma^{2u}) \\ &= \prod_{u \in D_0} (X - \gamma^u)(X + \gamma^u) \\ &= \prod_{u \in D_0} (X - \gamma^u)(X - \gamma^{u+p}) \\ &= \prod_{u \in D_0} (X - \gamma^u) \prod_{v \in D_0} (X - \gamma^{v+p}) \\ &= \Gamma_0(X)\Lambda_0(X), \end{aligned}$$

it follows that

$$2 + 2T_0(X) = 2 + 2S_0(X^2) = \Gamma_0(X)\Lambda_0(X)G(X^2).$$

On the other hand, from the fact that

$$2 + 2T_0(1) = p + 1 = \begin{cases} 0, & \text{if } p \equiv -1 \pmod{8}, \\ 2, & \text{if } p \equiv 1 \pmod{8}, \end{cases}$$

and $\Gamma_0(1)\Lambda_0(1) \in GR^*(4^r, 4)$, we write

$$G(X^2) = (X - 1)V_1(X)$$

for $p \equiv -1 \pmod{16}$ or $p \equiv -9 \pmod{16}$. Otherwise, we write $V_2(X) = G(X^2)$. Putting everything together, we complete the proof of the second statement. \square

Lemma 11. Let $S(X)$ be the generating polynomial of $(s_u)_{u \geq 0}$ described in (3). We have in the ring $\mathbb{Z}_4[X]$

$$S(X) = \begin{cases} (X - 1)\Gamma_0(X)\Gamma_1(X)W_1(X), & \text{if } p \equiv -1 \pmod{16}, \\ \Gamma_0(X)\Gamma_1(X)W_2(X), & \text{if } p \equiv 1 \pmod{16}, \\ (X - 1)\Gamma_0(X)\Gamma_1(X)\Lambda_0(X)W_3(X), & \text{if } p \equiv -9 \pmod{16}, \\ \Gamma_0(X)\Gamma_1(X)\Lambda_0(X)W_4(X), & \text{if } p \equiv 9 \pmod{16}, \end{cases}$$

where $W_i(\gamma^v) \neq 0, i = 1, 2$ for $v \in E_0 \cup E_1$ and $W_i(\gamma^v) \neq 0, i = 3, 4$ for $v \in E_1$.

Proof. Let $p \equiv -1 \pmod{16}$. By (6) we have

$$2(X^p + 1) = 2(X + 1)\Gamma_0(X)\Gamma_1(X) = 2(X - 1)\Gamma_0(X)\Gamma_1(X).$$

Then according to Lemma 10, we write

$$S(X) = (X - 1)\Gamma_0(X)H(X),$$

where

$$H(X) = U_1(X)(X^p - 1)/(X - 1) + \Lambda_0(X)V_1(X) + 2\Gamma_1(X).$$

We check that

$$H(\gamma^v) \begin{cases} = 0, & \text{if } v \in D_1, \\ \neq 0, & \text{if } v \in E_0, \\ \neq 0, & \text{if } v \in E_1. \end{cases}$$

For $v \in D_1$, we have $S(\gamma^v) = 0$ by Lemma 8. Since $(\gamma^v - 1)\Gamma_0(\gamma^v) \in GR^*(4^r, 4)$, we have $H(\gamma^v) = 0$ by Lemma 1.

For $v \in E_0$, we have $((\gamma^v)^p - 1)/(\gamma^v - 1) = 0$ and $\Lambda_0(\gamma^v) = 0$, so that $H(\gamma^v) = 2\Gamma_1(\gamma^v) \neq 0$;

For $v \in E_1$, since $S(\gamma^v) = 2$ by Lemma 8, we have $H(\gamma^v) \neq 0$.

So we have by Lemma 1

$$H(X) = \Gamma_1(X)W_1(X)$$

for some $W_1(X) \in \mathbb{Z}_4[X]$ and $W_1(\gamma^v) \neq 0$ for $v \in E_0 \cup E_1$. Then we get the factorization of $S(X)$ for $p \equiv -1 \pmod{16}$.

Another assertions of this lemma can be proved in a similar way. \square

Theorem 2. Let $(s_u)_{u \geq 0}$ be the quaternary sequence over \mathbb{Z}_4 defined by Equation (1). Then the linear complexity of $(s_u)_{u \geq 0}$ satisfies

$$LC((s_u)_{u \geq 0}) = \begin{cases} p, & \text{if } p \equiv -1 \pmod{16}, \\ p+1, & \text{if } p \equiv 1 \pmod{16}. \end{cases}$$

Proof. Let $p \equiv -1 \pmod{16}$. Since

$$S(X) = (X-1)\Gamma_0(X)\Gamma_1(X)W_1(X)$$

by Lemma 11, together with Lemma 8(I) we have $W_1(\gamma^v) \neq 0$ for $v \in E_0 \cup E_1 \cup \{p\}$. Then we see that

$$S(X)(X+1)\Lambda_0(X)\Lambda_1(X) \equiv 0 \pmod{X^{2p}-1}.$$

That is, $(X+1)\Lambda_0(X)\Lambda_1(X)$ is a connection polynomial of degree p of $(s_u)_{u \geq 0}$. So the minimal degree of connection polynomials of $(s_u)_{u \geq 0}$ is $\leq p$.

Let $C(X) \in \mathbb{Z}_4[X]$ be a connection polynomial of $(s_u)_{u \geq 0}$. Due to

$$\gcd((X-1)\Gamma_0(X)\Gamma_1(X), (X+1)\Lambda_0(X)\Lambda_1(X)) = 1,$$

we have

$$W_1(X)C(X) \equiv 0 \pmod{(X+1)\Lambda_0(X)\Lambda_1(X)}$$

by Equations (2), (6), (7) and Lemma 11. So we deduce

$$W_1(\gamma^v)C(\gamma^v) = 0 \text{ for } v \in E_0 \cup E_1 \cup \{p\}.$$

Since $W_1(\gamma^v) \neq 0$ for $v \in E_0 \cup E_1 \cup \{p\}$, if $W_1(\gamma^v) \in GR^*(4^r, 4)$ then we get $C(\gamma^v) = 0$, and if $W_1(\gamma^v) = 2\eta, \eta \in GR^*(4^r, 4)$, then we have either $C(\gamma^v) = 0$ or $C(\gamma^v) = 2$. I.e., $2C(\gamma^v) = 0$ for $v \in E_0 \cup E_1 \cup \{p\}$.

By the definition of $C(X) = 1 + c_1X + \dots$, i.e., $2C(x)$ is non-constant, then by Lemma 1 we have that $2C(x)$ is divisible by $(X+1)\Lambda_0(X)\Lambda_1(X)$, i.e., $\deg C(X) \geq p$ and hence $LC((s_u)_{u \geq 0}) = p$ for this case. We prove the first statement.

Let $p \equiv 1 \pmod{16}$. From that

$$S(X)(X^2-1)\Lambda_0(X)\Lambda_1(X) \equiv 0 \pmod{(X^{2p}-1)},$$

we see that $(X^2-1)\Lambda_0(X)\Lambda_1(X)$ is a connection polynomial of $(s_u)_{u \geq 0}$ of degree $p+1$.

For any connection polynomial $C(X)$ of $(s_u)_{u \geq 0}$, a similar way presented above gives

$$W_2(X)C(X) \equiv 0 \pmod{(X^2-1)\Lambda_0(X)\Lambda_1(X)}.$$

As in the proof of Theorem 1, denote by $s(X)$ and $c(X)$ the polynomials of degree < 2 such that

$$S(X) \equiv s(X) \pmod{X^2-1}$$

and

$$C(X) \equiv c(X) \pmod{X^2-1}.$$

As earlier, we can obtain that $c(X) \in \{0, 2, 2X, 2X+2\}$, hence $2c(X) = 0$ and $2C(X) = (X^2-1)M(X)$ for some $M(X) \in \mathbb{Z}_4[X]$. Since by Lemma 11 $W_2(\gamma^v) \neq 0$ for $v \in E_0 \cup E_1$, it follows that $2C(\gamma^v) = 0$ and $M(\gamma^v) = 0$ for $v \in E_0 \cup E_1$. Therefore, $M(X)$ is divisible by $\Lambda_0(X)\Lambda_1(X)$ by Lemma 1, i.e., $\deg C(X) \geq p+1$ and hence $LC((s_u)_{u \geq 0}) = p+1$ for this case. \square

Theorem 3. Let $(s_u)_{u \geq 0}$ be the quaternary sequence defined by Equation (1). Then the linear complexity of $(s_u)_{u \geq 0}$ satisfies

$$LC((s_u)_{u \geq 0}) = \begin{cases} (p+1)/2, & \text{if } p \equiv -9 \pmod{16}, \\ (p+3)/2, & \text{if } p \equiv 9 \pmod{16}. \end{cases}$$

Proof. The proof can follow that of Theorem 2 in a similar way. Here we give a sketch.

Let $p \equiv -9 \pmod{16}$. On the one hand, $(X+1)\Lambda_1(X)$ is a connection polynomial of $(s_u)_{u \geq 0}$ of degree $(p+1)/2$ by Equation (2).

On the other hand, for any connection polynomial $C(X)$ of $(s_u)_{u \geq 0}$, we have

$$W_3(X)C(X) \equiv 0 \pmod{(X+1)\Lambda_1(X)}.$$

Now since $W_3(\gamma^v) \neq 0$ for $v \in E_1 \cup \{p\}$, it follows that $2C(\gamma^v) = 0$ for $v \in E_1 \cup \{p\}$. Therefore, by Lemma 2 again $2C(x)$ is divisible by $(X+1)\Lambda_1(X)$, i.e., $\deg C(X) \geq (p+1)/2$ and hence $LC((s_u)_{u \geq 0}) = (p+1)/2$ for this case.

The case of $p \equiv 9 \pmod{16}$ follows the way of $p \equiv 1 \pmod{16}$ in Theorem 2 and we omit it. \square

3 Final Remarks and Conclusions

We determined the exact values of the linear complexity of $2p$ -periodic quaternary sequences over \mathbb{Z}_4 defined from the generalized cyclotomic classes modulo $2p$ by considering the factorization of the generating polynomial $S(X)$ in $\mathbb{Z}_4[X]$. It is more complicated to study this problem than that in finite fields. Besides the autocorrelation considered in [17], this is another cryptographic feature of the quaternary cyclotomic sequences of period $2p$.

A direct computing of the linear complexity has been done for $3 \leq p \leq 1000$ by the Berlekamp-Massey algorithm adapted by Reeds and Sloane in [20] for the residue class ring to confirm our theorems. Below we list some experimental data.

1. $p = 3$, $(s_u)_{u \geq 0} = (0, 0, 2, 2, 3, 1)$, then $C(X) = 1 + X + X^2 + X^3 + X^4 + X^5$ and $LC((s_u)_{u \geq 0}) = 5 (= 2p-1)$.

2. $p = 5$, $(s_u)_{u \geq 0} = (0, 0, 2, 1, 3, 2, 3, 1, 2, 0)$, then $C(X) = 1 + 3X^{10}$ and $LC((s_u)_{u \geq 0}) = 10 (= 2p)$.

3. $p = 7$, $(s_u)_{u \geq 0} = (0, 0, 2, 1, 2, 1, 3, 2, 2, 0, 3, 0, 3, 1)$, then $C(X) = 1 + X^2 + X^3 + 3X^4$ and $LC((s_u)_{u \geq 0}) = 4 (= (p+1)/2)$.

4. $p = 17$, $C(X) = 1 + X + 3X^{17} + 3X^{18}$, $LC((s_u)_{u \geq 0}) = 18 (= p+1)$.

5. $p = 31$, $C(X) = 1 + 3X^{31}$, $LC((s_u)_{u \geq 0}) = 31 (= p)$.

6. $p = 41$, $C(X) = 1 + 2X^2 + 3X^3 + 2X^5 + 2X^6 + 3X^7 + 3X^8 + 3X^9 + X^{10} + 2X^{11} + 3X^{12} + X^{13} + X^{14} + X^{15} + 2X^{16} + 2X^{17} + X^{19} + 2X^{20} + 3X^{22}$, $LC((s_u)_{u \geq 0}) = 22 (= (p+3)/2)$.

We hope that the procedures in this paper used to derive the linear complexity can be extended to quaternary cyclotomic sequences with larger period (for example, $2p^n$).

We finally remark that it is interesting to consider the k -error linear complexity of the sequences in this work.

From [18], it is also possible to use the sequences to define quaternary interleaved sequences of larger period.

Acknowledgements

The authors wish to thank the referees for their valuable comments and to thank Prof. Xiaoni Du for many suggestions. Parts of this work were written during a very pleasant visit of Z. Chen to the Hong Kong University of Science and Technology in Feb., 2016. He wishes to thank Prof. Cunsheng Ding for the hospitality and financial support.

Z.X.C. was partially supported by the National Natural Science Foundation of China under grant No. 61373140, the Natural Science Foundation of Fujian Province under grant No.2015J01662 and the Foundation of Putian Univ. under grant No. 2016074.

V.A.E. was supported by the Ministry of Education and Science of Russia as a part of state-sponsored project No. 1.949.2014/K.

References

- [1] Z. L. Chang, D. D. Li, "On the linear complexity of quaternary cyclotomic sequences with the period $2pq$," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E97-A, no. 2, pp. 679–684, 2014.
- [2] Z. X. Chen, "Linear complexity and trace representation of quaternary sequences over \mathbb{Z}_4 based on generalized cyclotomic classes modulo pq ," *Cryptography Communications*, 2016. (DOI 10.1007/s12095-016-0185-6)
- [3] T. W. Cusick, C. Ding, A. Renvall, *Stream Ciphers and Number Theory*, Elsevier, Amsterdam, 1998.
- [4] C. Ding, T. Hellesteth, H. Martinsen, "New families of binary sequences with optimal three-level autocorrelation," *IEEE Transactions on Information Theory*, vol. 47, no. 1, pp. 428–433, 2001.
- [5] X. N. Du, Z. X. Chen, "Linear complexity of quaternary sequences generated using generalized cyclotomic classes modulo $2p$," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E94-A, no. 5, pp. 1214–1217, 2011.
- [6] V. A. Edemskiy, "On the linear complexity of binary sequences on the basis of biquadratic and sextic residue classes," *Discrete Mathematics and Applications*, vol. 20, no. 1, pp. 75–84, 2010.
- [7] V. A. Edemskiy, O. Antonova, "The linear complexity of generalized cyclotomic sequences with period $2p^n$," *Applicable Algebra in Engineering, Communication and Computing*, vol. 25, no. 3, pp. 213–223, 2014.
- [8] V. A. Edemskiy, A. Ivanov, "Autocorrelation and linear complexity of quaternary sequences of period $2p$ based on cyclotomic classes of order four," in *Proceedings of the 2013 IEEE International Symposium on Information Theory (ISIT'13)*, pp. 3120–3124, Istanbul, Turkey, 2013.
- [9] V. A. Edemskiy, A. Ivanov, "Linear complexity of quaternary sequences of length pq with low autocorrelation," *Journal of Computational and Applied Mathematics*, vol. 259, pp. 555–560, 2014.
- [10] V. A. Edemskiy, A. Ivanov, "The linear complexity of balanced quaternary sequences with optimal autocorrelation value," *Cryptography and Communications*, vol. 7, no. 4, pp. 485–496, 2015.
- [11] V. A. Edemskiy, A. Palvinskiy, "The linear complexity of binary sequences of length $2p$ with optimal three-level autocorrelation," *Information Processing Letters*, vol. 116, no. 2, pp. 153–156, 2016.
- [12] S. W. Golomb, G. Gong, *Signal Design for Good Correlation: For Wireless Communications, Cryptography and Radar Applications*, Cambridge University Press, Cambridge, 2005.
- [13] M. Hall, *Combinatorial Theory*, Wiley, New York, 1975.
- [14] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, 1982.
- [15] P. Ke, Z. Yang, J. Zhang, "On the autocorrelation and linear complexity of some $2p$ periodic quaternary cyclotomic sequences over \mathbb{F}_4 ," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. EA94-A, no. 11, pp. 2472–2477, 2011.
- [16] P. Ke, S. Zhang, "New classes of quaternary cyclotomic sequence of length $2p^m$ with high linear complexity," *Information Processing Letters*, vol. 112, pp. 646–650, 2012.
- [17] Y.-J. Kim, Y.-P. Hong, H. Y. Song, "Autocorrelation of some quaternary cyclotomic sequences of length $2p$," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E91-A, no. 12, pp. 3679–3684, 2008.
- [18] X. Ma, T. J. Yan, D. D. Zhang, Y. Y. Liu, "Linear complexity of some binary interleaved sequences of period $4N$," *International Journal of Network Security*, vol. 18, no. 2, pp. 244–249, 2016.
- [19] B. R. McDonald, *Finite Rings With Identity*, New York. Marcel Dekker, 1974.
- [20] J. A. Reeds, N. J. A. Sloane, "Shift-register synthesis modulo m ," *SIAM Journal on Computing*, vol. 14, pp. 505–513, 1985.
- [21] P. Udaya, M. U. Siddiqi, "Optimal biphasic sequences with large linear complexity derived from sequences over \mathbb{Z}_4 ," *IEEE Transactions on Information Theory*, vol. 42, pp. 206–216, 1996.
- [22] P. Udaya, M. U. Siddiqi, "Optimal and suboptimal quadriphase sequences derived from maximal length sequences over \mathbb{Z}_4 ," *Applicable Algebra in Engineering, Communication and Computing*, vol. 9, pp. 161–191, 1998.

- [23] P. Udaya, M. U. Siddiqi, "Generalized GMW quadriphase sequences satisfying the Welch bound with equality," *Applicable Algebra in Engineering, Communication and Computing*, vol. 10, pp. 203-225, 2000.
- [24] Z. X. Wan, *Finite Fields and Galois Rings*, Singapore, World Scientific Publisher, 2003.
- [25] C. H. Wu, "Trace representation of cyclotomic generator of order r ," *International Journal of Computer Mathematics: Computer Systems Theory*, vol. 1, no. 1, pp. 3-13, 2016.
- [26] J. Zhang, C. A. Zhao, "The linear complexity of a class of binary sequences with period $2p$," *Applicable Algebra in Engineering, Communication and Computing*, vol. 26, no. 5, pp. 475-491, 2015.

$Q(X)(X^p + 1)/(X + 1)$, $Q(X) \in \mathbb{Z}_4[X]$ and $2Q(X) \neq 0$. Since $P(-1) = 2$ it follows that $Q(-1) = 2$ and $Q(X) = (X + 1)F(X) + 2$, $F(X) \in \mathbb{Z}_4[X]$ or

$$P(X) = (X^p + 1)F(X) + 2(X^p + 1)/(X + 1).$$

From the last equality and conditions of this lemma we obtain $2F(\gamma^v) = 0$ for $v \in E_0 \cup E_1 \cup \{0\}$, therefore $2F(x)$ is divisible by $x^p - 1$ and $\deg P(X) \geq 2p$.

Remark 1. The polynomial $P(X)$ is not obliged to be divisible by $X^{2p} - 1$ when $P(\gamma^j) = 0$ for $j = 0, 1, \dots, 2p - 1$. For example, $P(X) = X^{2p} - 1 + 2(X^p + 1)$.

Appendix

Proof of Lemma 1.

It is well known that if $\xi \in GR(4^r, 4)$ is a root of the polynomial $P(X) \in \mathbb{Z}_4[X]$ then $P(X) = (X - \xi)Q_1(X)$ for some polynomial $Q_1(X) \in GR(4^r, 4)[X]$. Let η be another root of $P(X)$ and $\xi - \eta \in GR^*(4^r, 4)$, then we have $(\xi - \eta)Q_1(\eta) = 0$, i.e., $Q_1(\eta) = 0$. So, $Q_1(X) = (X - \eta)Q_2(X)$ holds for some polynomial $Q_2(X) \in GR(4^r, 4)[X]$ and we derive $P(X) = (X - \xi)(X - \eta)Q_2(X)$.

Proof of Lemma 2.

(I). By the choice of γ we have an expansion $(X^p - 1)/(X - 1) = \prod_{j=1}^{p-1} (X - \gamma^{2j})$, hence $p = \prod_{j=1}^{p-1} (1 - \gamma^j)(1 + \gamma^j)$. So, $\gamma^j - \gamma^n \in GR^*(4^r, 4)$ when $j, n \in \{0, \dots, 2p - 1\}$ and $j \not\equiv n \pmod{p}$. Therefore, if $P(\gamma^j) = 0$ for all $j \in D_i$ or for all $j \in E_i, i = 0, 1$, then $P(X)$ is divisible by $\prod_{j \in D_i} (X - \gamma^j)$ or $\prod_{j \in E_i} (X - \gamma^j)$ by Lemma 1. The first assertion of Lemma 2 is proved.

(II). This assertion follows from (I).

(III). We consider two cases.

Let $P(1) = 0$ or $P(-1) = 0$. Suppose $P(-1) = 0$, in this case by (II) we have that

$$P(X) = (X^p + 1)P_3(X)$$

and $2P_3(X) \neq 0$ since $P(0) = 1$. From the equality $P(X) = (X^p + 1)P_3(X)$ for $X = \gamma^v$, $v \in E_0 \cup E_1$ we deduce $2P_3(\gamma^v) = 0$, therefore $2P_3(X)$ is divisible by $(X^p - 1)/(X - 1)$ and $\deg P(X) \geq 2p - 1$. Furthermore, if $P(1) = 0$ then $2P_3(X)$ is divisible by $(X^p - 1)$ and $\deg P(X) \geq 2p$.

Let $P(1) \neq 0$ and $P(-1) \neq 0$. Then, we derive $P(1) = 2$, $P(-1) = 2$ and $P(\gamma^j) = 0$ for all $j \in D_0 \cup D_1$. By (I) we have $P(X) =$

Biography

Zhixiong Chen was born in 1972. He received the M.S degree in Mathematics from Fujian Normal University in 1999 and Ph.D. degree in Cryptography from Xidian University in 2006, respectively. Now he is a professor of Putian University. He worked as a visiting scholar supervised by Prof. Arne Winterhof in Austrian Academy of Sciences (Linz) in 2013 and by Prof. Andrew Klapper in University of Kentucky (Lexington) during 2014-2015, respectively. His research interests include stream cipher, elliptic curve cryptography and digital signatures.

Vladimir Edemskiy finished Leningrad University in Mathematics and he received the Ph.D. degree in Algebra and Number Theory from Leningrad University in 1990. In 2010 he received the D. Sc. degree from Novgorod State University. Now he is a professor of Novgorod State University. His research interests include pseudorandom sequences, design sequences and cryptography.

A Key-insulated Proxy Re-encryption Scheme for Data Sharing in a Cloud Environment

Yilei Wang¹, Dongjie Yan¹, Fagen Li¹ and Hu Xiong¹

(Corresponding author: Hu Xiong)

School of Information and Software Engineering, University of Electronic Science and Technology of China¹

No. 4, North Jianshe Road, Chenghua District, chengdu, Sichuan 610054, China

(Email: xionghu.uestc@gmail.com)

(Received Apr. 16, 2016; revised and accepted June 28 & July 19, 2016)

Abstract

Proxy re-encryption (PRE) enables a semi-trusted proxy to delegate the decryption right by re-encrypting the ciphertext under the delegator's public key to an encryption under the public key of delegatee. Fueled by the translation ability, PRE is regarded as a promising candidate to secure data sharing in a cloud environment. However, the security of the PRE will be totally destroyed in case the secret key of the delegator or the delegatee has been exposed. Despite the key exposure seems inevitable, the PRE scheme with resistance against secret key leakage has never been presented before. To deal with this intractable problem, we propose a key-insulated proxy re-encryption (KIPRE) scheme by incorporating the mechanisms of PRE and key-insulated cryptosystem. In the proposed scheme, the lifetime of the secret key associated with the user, i.e., the delegator or the delegatee, has been divided into several periods. In each time period, the user can interact with his/her physically-secure but computation-limited helper to update his/her temporary secret key. On the contrary, the public keys of the users remained unchanged during the whole lifetime of the system. We then apply our KIPRE scheme to construct a practical solution to the problem of sharing sensitive information in public clouds with resilience to the key exposure. The performance evaluation and the security analysis demonstrate that our scheme is efficient and practical.

Keywords: Cloud Environment; Key Insulation; KIPRE; PRE; Secret Key Exposure.

1 Introduction

In 1998, Blaze et al. [2] introduced the conception called *atomic proxy re-encryption*, in which a semi-trusted proxy is deployed to transform the ciphertext encapsulated under Alice's public key into the one that can be decrypted with Bob's secret key.

In such an environment, Alice can delegate her decryption right to Bob without making him access her secret key (That is to say, Alice and Bob respectively perform as the delegator and the delegatee during the communication), meanwhile, the proxy is unable to see the underlying plaintext.

In the present decade, proxy re-encryption (PRE) has attracted much attention of many researchers [3, 4, 7, 18, 22, 27] and has been introduced to be applied in a number of interesting environments such as secure file systems [1, 24], multicast [20], email forwarding [13] and law enforcement [12].

PRE is also deemed as a promising technique to ensure data confidentiality and fine-access control in cloud computing environment [14, 15, 26, 27, 28] which is an emerging computing paradigm drawing extensive attention from both academia and industry. In such an environment, the cloud service provider (CSP) plays the role of the proxy, and the users respectively act as the delegator (Alice) and the delegatee (Bob). Despite that PRE has various of inspiring applications, the security behind it relies on the basic precondition that the user's secret key in PRE settings is kept insulated from the attacker. That is to say, the security of user's sensitive data will no longer exist if the user's secret key is compromised.

Exposure of a secret key. We consider that it is reasonable for an attacker to compromise the legal user's secret key in a normal asymmetric cryptosystem (including PRE in cloud computing environment), in which a single secret key is bound to a public key or an identity. The secret key is the only necessity for a user to decrypt a ciphertext. In general, it is repositied in either a personal computer or a fully trusted server, and even protected by some naive approach such as a password. This protection method is valid and high-efficient if the computer or the server is absolutely isolated from an opening network. Unfortunately, this assumption is too strong and it is unlikely to be met in reality. (1) Threats from the Internet: the device holding the secret key may suffer from numerous attacks from network hackers with various in-

trusion capacities, meanwhile the key owner may be unaware about it. (2) Physical threats: the computer/server may be accessed by some other ill-disposed users when the original user (i.e. the key owner) leaves without locking it. In these cases, the malicious users or the network attackers can compromise the secret key to gain the access of its owner's personal data stored in the cloud system. Consequently, it is particularly imperative to tackle the compromise of user's secret key in public key settings.

To address the intractable key exposure problem mentioned above, broad research has been made to minimize the damage caused by key exposure rather than to prevent the attacker from getting access to the secret key (because the secret key is used frequently in decryption in public key settings). An effective and practical approach is to utilize key-insulated encryption (KIE) which was introduced by Dodis et al. [5] in 2002. In KIE environment, the core idea is that the user's secret key is made up of two parts, one of which is controlled by the user and the other is evolved by the helper (i.e. a physically-secure but computation-limited device). The system lifetime is divided into several distinct time periods, in which the user's secret key is diverse from each other. However, the corresponding public key remains unchanged through the whole system lifetime. By utilizing the technic of key-insulation, the user interacts with the physically-secure helper at the beginning of each time period to yield a temporary secret key which is valid in decryption during that time period. In KIE, the key exposure in a certain time period only threatens the security during that time period rather than the others. In other words, KIE captures the forward security and the backward security simultaneously.

Our contribution. Inspired by [1] and [5], we present a new scheme called key-insulated proxy re-encryption (KIPRE) for data sharing in a cloud environment to enjoy the benefits of KIE in PRE settings, using a practical helper. The helper is actually a proper device which satisfies the following conditions: (1) its computation capacity may be limited, because it should be portable enough; and (2) it is physically secure and should not be eavesdropped, i.e. the secret information reserved in it cannot be accessed by any invalid user. In this paper, we introduce key-insulation to the PRE environment to cope with the exposure of user's private keys. More importantly, our scheme, for the first time, addresses the secret key exposure in PRE for data sharing in a cloud environment. Furthermore, we give our concrete construction of KIPRE as well as the security and efficiency analysis of our proposed scheme.

2 Related Work

In this section, we inspect some related works involving proxy re-encryption cryptosystems (which suffers from the exposure of user's secret key) and cryptosystems with key insulation.

2.1 Proxy Re-encryption Cryptosystems

The idea that the decryption right can be delegated from one legal user to another was introduced by Mambo and Okamoto [19] in 1997. Then Blaze et al. [2] introduced the conception of *atomic proxy re-encryption* as well as a concrete scheme which was based on ElGamal system. However, it was unfortunately bidirectional. (i.e. The corrupted proxy could re-encrypt the original ciphertexts from Alice to Bob and vice versa.) With some improvement, Ateniese et al. [1] showed their pairing-based unidirectional proxy re-encryption schemes in 2006. In their schemes, the proxy cannot collude with the delegatee to reveal the delegator's private key and their schemes are semantically secure based on the Decisional Bilinear Diffie-Hellman problem. In 2007, Canetti and Hohenberger [3] firstly defined the security against chosen ciphertext attacks (CCA) in PRE system and gave a concrete construction capturing the security they defined. Since then, varieties of PRE schemes [17, 21, 27] which satisfied different properties were proposed. In particular, Sur et al. [21] introduced the conception of certificate-less proxy re-encryption (CL-PRE) as well as its security definitions. Moreover, they also constructed a CCA secure scheme, the security of which was proved in the random oracle model. In 2014, Liu et al. [17] presented a time-based proxy re-encryption scheme (TimePRE) for secure data sharing in a cloud environment, in which a user's access right to the re-encrypted data stored in the proxy could expire automatically by embedding a predetermined time period in user's private key, i.e. the delegatee could be revoked even if the delegator was not online. In the following year, Xu et al. [27] proposed an efficient Conditional Identity-based Broadcast proxy re-encryption scheme (CIBPRE) which was considered appropriate to be applied into secure cloud email system with more advantages than the existing secure email systems.

Despite that there are plenty of schemes which have been proposed with various properties, none of them focus on the exposure of user's secret key. We argue that the message (either the original ciphertext of the re-encrypted ciphertext) transferred in the PRE settings can be decrypted by the attackers if either the delegator's or the delegatee's private key is leaked.

2.2 Cryptosystems with Key Insulation

In 2002, Dodis et al. [5] firstly introduced the notion of key-insulated security as well as the first (t, N) -key-insulated encryption scheme based on any (standard) public key encryption scheme. Then, Hanaoka et al. [10] constructed an unconditionally secure key-insulated encryption scheme. Additionally, they also extended the model of key-insulated encryption (KIE) to dynamic and mutual key-insulated encryption (DMKIE) which could be constructed from broadcast encryption schemes or key pre-distribution schemes. In 2006, Hanaoka et al. [8] pre-

sented a new paradigm called parallel key-insulated encryption scheme (PKIE), in which more than one helper was employed to interact with the user to update the temporary secret key. They tried to address the increasing probability of the key leakage caused by frequent update of the temporary secret key. In [9], Hanaoka et al. firstly proposed a new primitive called one time forward-secure public key encryption (OTFS-PKE), which could be constructed from either ordinary identity-based encryption (IBE) or hierarchical identity-based encryption (HIBE). Then they also introduced how to extend a OTFS-PKE scheme to a parallel key-insulated encryption (PKIE) scheme. Recently, Hong and Sun [11] firstly presented a pairing-free key insulated attribute-based encryption scheme which is high efficient and provably secure. Their scheme combined the advantages of both key insulation and attribute-based encryption. Moreover, they also argued that their scheme was much more suitable to be applied in data sharing network systems, particularly those with limitation in computation such as mobile communication system and wireless sensor networks. The advantage of key insulated mechanism can also be combined into PRE to tackle key exposure problems in PRE settings and it is necessary to propose a KIPRE scheme with efficiency and security.

3 Preliminary

3.1 Mathematical Background

Bilinear Maps. \mathbb{G}, \mathbb{G}_T are two groups with the same prime order q . g is the generator of \mathbb{G} , and e is a function, $e: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$, such that:

- 1) **Bilinear:** $e(g^a, g^b) = e(g, g)^{ab}$, for $\forall a, b \in \mathbb{Z}_q^*$.
- 2) **Non-degenerate:** There exists some $g \in \mathbb{G}$ such that $e(g, g) \neq 1$.
- 3) **Computable:** There exists an efficient algorithm to compute $e(g^a, g^b)$, for $\forall a, b \in \mathbb{Z}_q^*$.

3.2 Assumption

q -weak Decisional Bilinear Diffie-Hellman Inversion (q -wDBDHI) Assumption. we assume the intractability of a variant of the q -Decisional Bilinear Diffie-Hellman Inversion (q -DBDHI) problem [6]. For an algorithm \mathcal{A} , define its advantage as $\text{Adv}_{\mathcal{A}}^{q\text{-wDBDHI}}(k) = |\Pr[\mathcal{A}(g, g^a, \dots, g^{(a^q)}, g^b, e(g, g)^{b/a}) = 1] - \Pr[\mathcal{A}(g, g^a, \dots, g^{(a^q)}, g^b, \Gamma) = 1]|$, where $g \leftarrow \mathbb{G}$, $a, b \in \mathbb{Z}_q^*$ and $\Gamma \in \mathbb{G}_T$. We say the q -wDBDHI assumption holds, if for any probabilistic polynomial-time (PPT) algorithm \mathcal{A} , $\text{Adv}_{\mathcal{A}}^{q\text{-wDBDHI}}(k)$ is negligible in security parameter k . We argue that the q -wDBDHI assumption is slightly weaker than the q -DBDHI assumption defined in [6], which is to recognize $e(g, g)^{1/a}$ given $(g, g^a, \dots, g^{(a^q)}) \in \mathbb{G}^{q+1}$ and Dodis and Yampolskiy showed that it was indeed hard in generic groups.

4 System Model

In our system, we assume that the cloud server is a semi-trusted party which may correctly execute the corresponding delegation algorithms with curiosity on the underlying data. It may try to decrypt the ciphertext reserved in the cloud server. Furthermore, we assume that the helper is some proper device which is physically-secure (e.g. it is isolated from the opening network and well protected by its owner.) and may be computation-limited (in order to capture some other properties such as portability). To guarantee the consistency of the time periods among all the entities, we also assume that there is a global time flowing through the whole system lifetime. Actually, a global time is not quite easy to achieve in a cloud computing environment. However, we can utilize the techniques introduced in [16] to achieve this goal. In addition, we also suggest that our scheme is much more appropriate for the cloud environment where a coarse-grained time accuracy for the division of time periods is satisfactory.

Before giving the concrete construction of our proposed scheme, we show an intuition on it and further illustrate our mechanism's framework in Figure 1. In our system, there are four entities which are described as follows:

- **Cloud Service Provider (CSP):** The CSP maintains the cloud infrastructures including the bandwidth, storage devices and many cloud servers with powerful computation capability. We assume that the storage and the computation ability of the CSP are flexibly extensible. Therefore, it owns high reliability and efficiency far beyond the personal computers. In our system, the CSP mainly provides two kinds of services: data storage and re-encryption. After receiving the encrypted data from the delegator (Alice), the CSP stores the data on the cloud storage devices. After obtaining the re-encryption key sent from Alice, the CSP will correctly execute the re-encryption algorithm to transfer the original ciphertext to the re-encrypted ciphertext and sent it to the delegatee (Bob).
- **Delegator (Alice):** She is the delegator (or the data owner) and she is responsible for sending the ciphertext encrypted with her own public key to the CSP and generating re-encryption key which will be delivered to the CSP in an appropriate time period.
- **Delegatee (Bob):** He is the delegatee (the receiver) and he can issue a request for the data Alice outsourced in the cloud. Then the CSP send the re-encrypted data to him. He can decrypt the re-encrypted data utilizing his own secret key in the corresponding time period.
- **Physically-Secure Device (Helper):** It is a physically-secure but computation-limited device which is deployed to help the system user (i.e. the delegator and the delegatee) to update their secret keys (Each

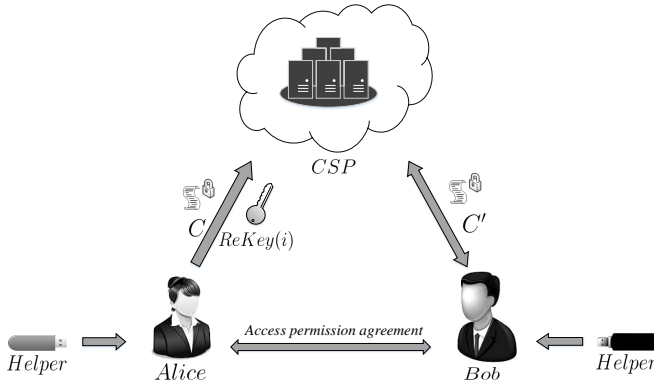


Figure 1: Key insulated proxy re-encryption framework

user owns a distinct temporary secret key in each time period).

On account of the local storage and computation limitation of personal computer, Alice prefers to outsource her data (which is encrypted before uploading) on the remote cloud server. To share her data stored in the CSP without reveal to the public, the system performs as follows:

- 1) **Upload encrypted data.** Before uploading the outsourced data to the CSP, Alice encrypts the data with her public key and current time period i . Since the decryption requires Alice's secret key which is properly protected by key-insulation mechanism, the data stored on the cloud server is well safeguarded.
- 2) **Access request.** To get the access permission from Alice, Bob needs to send an access request to Alice. Then Alice decides whether he is allowed to get access to the corresponding data. That is to say, Alice makes access control by herself.
- 3) **Access permission.** If Alice permits Bob's request, she will respond a permission (may be some material such as a signature representing Alice's confirmation) to Bob and executes the $ReKey(i)$ generation. Otherwise, she refuses Bob's request.
- 4) **ReKey(i) generation.** In this phase, Alice executes $ReKeyGen$ algorithm to generate the re-encryption key $ReKey(i)$ for time period i and sends it to the CSP.
- 5) **Re-encrypted data response.** When the CSP receives the $ReKey(i)$ from Alice, it honestly re-encrypts the original ciphertext and sends the re-encrypted ciphertext to Bob. Though the CSP is always curious during the whole system runtime, it cannot get any underlying information except the source address and the destination.
- 6) **Decryption of the re-encrypted ciphertext.** After receiving the re-encrypted ciphertext from the

CSP, Bob can run the Dec algorithm with his own secret key for time period i to obtain the underlying data.

5 Our Construction

In this section, we will give the concrete construction of our proposed KIPRE scheme which involves septuple algorithms: $KeyGen$, $Update^*$, $Update$, $ReKeyGen$, Enc , $ReEnc$, Dec . Compared to the traditional PRE scheme, our scheme includes two additional algorithms $Update^*$ and $Update$, which make user's secret key evolve with time periods. Therefore, it can correctly capture key insulation in PRE settings and mitigate the damage caused by key exposure. In our system, we consider the two users Alice and Bob as the delegator and the delegatee respectively. The detail of the algorithms mentioned above are described as follows. (Note that the keys corresponding to Bob perform as the same as those of Alice in the algorithms $Update^*$ and $Update$. For simplicity, we omit them.)

- **KeyGen:** On input the security parameter 1^k , this algorithm randomly selects a prime q . Let \mathbb{G}, \mathbb{G}_T be two groups of the same prime order q and g is a generator of \mathbb{G} . For Alice, this algorithm chooses $x_{A,0}^*, \dots, x_{A,t}^* \leftarrow \mathbb{Z}_q^*$, where $t \in \mathbb{Z}_q^*$ is the total number of the time periods which the system life-time is divided into. The system public parameters are $g, \mathbb{G}, \mathbb{G}_T, e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$, where e is a bilinear map. Alice's public key is $PK_A = \{g^{x_{A,0}^*}, \dots, g^{x_{A,t}^*}\}$. The master key of Alice's helper is $SK_A^* = (x_{A,1}^*, \dots, x_{A,t}^*)$. The initial key of Alice is $SK_{A,0} = x_{A,0}^*$. Bob's initial keys including $PK_B, SK_B^*, SK_{B,0}$ can be generated in a similar way and we omit it here.
- **Update*:** At the end of time period $i-1 \in \{0, 1, \dots, t-1\}$, Alice's helper executes algorithm $Update^*$ to generate the helper key $SK'_{A,i} = x'_{A,i}$ for period $i \in \{1, 2, \dots, t\}$, where $x'_{A,i} = \sum_{j=1}^t x_{A,j}^* (i^j - (i-1)^j)$.
- **Update:** Given the helper key $SK'_{A,i}$ for period i , Alice runs this algorithm to compute $x_{A,i} = x_{A,i-1} + x'_{A,i} = \sum_{j=0}^t (x_{A,j}^* (i-1)^j) + \sum_{j=1}^t x_{A,j}^* (i^j - (i-1)^j) = \sum_{j=0}^t (x_{A,j}^* \cdot i^j)$. Then output $SK_{A,i} = x_{A,i}$ for period i .
- **ReKeyGen:** This algorithm takes Bob's public key $PK_B = \{g^{x_{B,0}^*}, \dots, g^{x_{B,t}^*}\}$ and time period i as input. Compute $rk_{A \rightarrow B,1} = \prod_{j=0}^t (g^{x_{B,j}^*})^{i^j} = g^{x_{B,i}}$. Then Alice uses her secret key $SK_{A,i}$ to compute $rk_{A \rightarrow B,2} = rk_{A \rightarrow B,1}^{1/x_{A,i}} = g^{x_{B,i}/x_{A,i}}$ and sends $rk_{A \rightarrow B,2}$ to the CSP.
- **Enc:** Given Alice's public key $PK_{A,i}$, this algorithm randomly selects $r \leftarrow \mathbb{Z}_q^*$ and computes the

original ciphertext $C = (C_1, C_2)$, where $C_1 = (\prod_{j=0}^t (g^{x_{A,j}^*})^{i^j})^r = (g^{\sum_{j=0}^t (x_{A,j}^* \cdot i^j)})^r = (g^{x_{A,i}})^r$ and $C_2 = e(g, g)^r \cdot M$.

- **ReEnc:** On input the re-encryption key $rk_{A \rightarrow B, 2}$ and the original ciphertext (C_1, C_2) for period i , this algorithm computes $C'_1 = e(C_1, rk_{A \rightarrow B, 2}) = e(g^{r x_{A,i}}, g^{x_{B,i}/x_{A,i}})$. Then output the re-encrypted ciphertext as $C' = (C'_1, C_2)$.
- **Dec:** For a original ciphertext $C = (C_1, C_2)$, Alice can compute $M = \frac{C_2}{e(g, C_1)^{1/x_{A,i}}}$. Receiving the re-encrypted ciphertext $C' = (C'_1, C_2)$, Bob executes the algorithm Dec with input $SK_{B,i}$ to recover the plaintext $M = \frac{C_2}{(C'_1)^{1/x_{B,i}}}$.

6 System Evaluation

6.1 Discussion

Privacy of user's secret key. In our proposed scheme, we import the key-insulated mechanism to protect user's secret key from being exposed. Our construction supports key-insulated security which is captured by key update in each time period with the assistance of the helper, i.e. the secret keys for both previous and following time periods are safe even if the secret key for the current time period is exposed.

Time period consistency. To guarantee the time period consistency among all the related entities in our system, we should pre-defined a global time which can be achieved by utilizing some other techniques such as [16]. We further argue that it is reasonable and available to be achieved, since the time period consistency is the basic condition for all of the previous key-insulated schemes [5, 11, 23, 25] and some other time-based schemes [16, 17].

Time-release delegation. In ReKeyGen of our proposed scheme, we consider the sharing data should be outsourced in the same time period that Bob's data request is issued. That is to say, Alice's data outsourcing and Bob's data requirement are occurred in the same time period. Actually, we argue that our scheme is also suitable for time-release delegation. (Alice uploads her sharing data to the CSP in time period i , and Bob sends Alice a data request in arbitrary time period j , where $i < j$.) Specifically, when Alice uploads the encrypted data to the CSP, she can make a record on the map of the data message (some characteristics, e.g. hash value of the data) and the current time period i as $\langle \text{data}, i \rangle$, and add the record to a list stored locally. Since the computation and storage cost of this record is quite cheap, it is acceptable to a personal computer. When Alice receives a data request from Bob, she first generates $rk_{A \rightarrow B, 1}$ with Bob's public key PK_B in the same way as the above scheme. Then Alice search corresponding

record from her list and get the time period i^* . She continues to compute SK_{A,i^*} with her helper (since our scheme supports random access key update which is defined in Section 6.2.1), rather than $SK_{A,i}$ which is the secret key for the current time period i . Finally, Alice computes $rk_{A \rightarrow B, 2} = rk_{A \rightarrow B, 1}^{1/x_{A,i^*}} = g^{x_{B,i}/x_{A,i^*}}$ and sends $rk_{A \rightarrow B, 2}$ to the CSP. Thus, the data outsourced in previous time periods can also be correctly delegated in the following time periods.

6.2 Security Analysis

6.2.1 Key-insulation

In our scheme, the system lifetime is divided into a number of time periods and the user's secret key is not wholly preserved by himself but updated with his/her helper's help in each time period. For each time period, the user's secret key is generated with the previous secret key and the assistance of his unique physically-secure helper. When a legal user is intruded by an attacker, he can only decrypt the ciphertext encrypted for the current time period, since the user's secret key for each time period is distinct. Particularly, in an original PRE scheme, the attacker can decrypt all the ciphertext through the whole system lifetime if he compromises the secret keys of the delegator and the delegatee. However, our scheme enjoys the advantage of key insulation. The attacker cannot get the whole secret keys for any other time periods, even if he captures the temporary secret keys for several time periods, since he cannot get access to the helper. Moreover, our scheme satisfies the following properties: secure key update and random-access key update.

Secure key update. Similar to [5], we define secure key update as follows: A scheme satisfies secure key update if a *key-update exposure* in period i is equivalent to key exposures in both period $i - 1$ and period i . The *key-update exposure* in period i denotes that the key exposure happens while the key update from SK_{i-1} to SK_i is taking place. (i.e. the attacker can get SK_{i-1} , SK'_i and SK_i .) We argue that our scheme has secure key update, since the attacker who makes key exposures in period $i - 1$ and i can obviously get SK_{i-1} and SK_i . Then he can further compute $SK'_i = SK_i - SK_{i-1}$. That is the same as *key-update exposure* in period i .

Random access key update. *Random access key update* denotes that the temporary secret key can be updated to any other one for arbitrary time period instead of the next one. Obviously, our scheme enjoys the advantage of *random access key update*. In particular, the helper can compute the helper key as $SK'_{A,i+\Delta} = x'_{A,i+\Delta} = \sum_{j=1}^t x_{A,j}^* ((i+\Delta)^j - i^j)$, and the user can further compute $SK_{A,i+\Delta} = x_{A,i} + x'_{A,i+\Delta} = \sum_{j=0}^t (x_{A,j}^* i^j) + \sum_{j=1}^t x_{A,j}^* ((i+\Delta)^j - i^j) = \sum_{j=0}^t (x_{A,j}^* (i+\Delta)^j)$. It correctly performs the *random access key update* from time period i to $i + \Delta$, where Δ is the time period distance.

Table 1: Property comparison

Schemes	PRE	Unidirectional	Temporary delegation	Time-release delegation	Key insulation	Key update	Trusted server free	Helper requirement
[1]-2	✓	✓	×	×	×	×	✓	×
[1]-3	✓	✓	×	×	×	×	✓	×
[1]-4	✓	✓	✓	×	×	×	×	×
Our scheme	✓	✓	✓	✓	✓	✓	✓	✓

6.2.2 Semantic Security

Since key-insulated mechanism has well addressed the exposure of user's secret key, we then analyze the semantic security of our scheme. Actually, this scheme has many attractive properties such as efficient unidirectional, non-interactive, proxy invisible and nontransitive.

The security of our scheme is based on the q -wDBDHI assumption defined in Section 3.2, and we set $q = t + 1$. Think of g^b as g^{ak} for some $k \in \mathbb{Z}_q^*$, and we consider the original ciphertext $C = (g^b, M \cdot \Gamma)$ which is encrypted for public key g^a (actually may be $g^{\sum_{j=0}^t (x_{u,j}^* \cdot i^j)}$, where u denotes a valid user.) and message M . Check $\Gamma \stackrel{?}{=} e(g, g)^k$, where $e(g, g)^k = e(g, g)^{b/a} = e(g, g)^{ak/a}$. If it is true, C is a correct ciphertext of M , otherwise, it is a ciphertext of some other message $M' \neq M$. Therefore, the semantic security of our scheme can be easily broken by the adversary that can solve the q -wDBDHI problem (which is indeed proven hard in the generic group by Dodis and Yampolskiy [6]). Moreover, the security of our scheme is also based on the assumption that a cannot be figured out given a tuple (g, g^a) , where $g \in \mathbb{G}$ and $a \in \mathbb{Z}_q^*$.

6.3 Comparison to Existing Works

In this section, we show some attractive properties of our scheme compared to Ateniese et al's schemes [1], which is very similar to our scheme in system time division and temporary delegation.

In fact, there are four schemes proposed in [1]. However, the first scheme (we omit it in Table 1) cannot be seen as a pure proxy re-encryption scheme, since it is actually a special encryption scheme which has two decryption approaches rather than has a ciphertext transformation between users. The second and third schemes are much more like normal proxy re-encryption schemes with unidirectionality, non-interactivity, collusion-resilience and non-transitivity, unfortunately, they are ordinary versions without temporary delegation and the protection of user's secret key. Ateniese et al's fourth scheme, which can be deemed as an improvement of the previous three schemes, is very attractive with the properties of temporary delegation. Its system lifetime is also divided into several time periods to ensure a temporary delegation in period i , which is similar to our proposed scheme. They deployed a trusted server which broadcasted a random value $h_i \in \mathbb{G}_1$ in each time period for all users to see. Obviously, it is an efficient approach to enable Alice to temporarily delegate her decryption right to Bob for some period i . However, we consider that there are some drawbacks in reality. (1) To guarantee the honesty of a server on opening network

is not quite easy. (2) It does not support time-release delegation which is very useful and flexible. (3) Most importantly, it suffers the problem of key exposure, i.e. if an adversary comprises Alice's and Bob's secret keys (h_i can be seen for all users), he will be able to decrypt all the ciphertexts, which is disastrous.

We argue that our scheme is very exciting. We deploy a physically-secure device named "helper" rather than a trusted server to achieve temporary delegation. Note that the helper is much more practical in reality compared to the trusted server, since it is isolated from the opening network and may be brought with the user. (In some sense, it is controlled by its owner rather than someone else.) Instead of broadcasting a random value h_i for every user, in our scheme, the user interacts with his own unique helper to update his temporary secret key for each time period i . Meanwhile, our scheme also supports time-release delegation which we explained in Section 6.1. In addition, since user's temporary key for each time period is distinct and can only be derived by interacting with the corresponding helper, the adversary can only compromise the temporary key for period i rather than the whole system lifetime, even if he makes a key exposure in period i . Thus, our KIPRE scheme enjoys the advantage of key insulation and mitigates the damage caused by key exposure.

Furthermore, we also provide the theoretical and experimental comparison with Ateniese et al's schemes [1] as follows.

Theoretical comparison. We show the theoretical comparison with Ateniese et al's schemes [1] in Table 1, Table 2 and Table 3 for property, communication and computation complexity, respectively. Since [1]-4 can be seen as an improvement of the previous three schemes in [1] and it is much more similar to our proposed scheme, we only give the efficiency comparison between our scheme and [1]-4 in Table 2 and Table 3. We define the notations we used in tables as follows: $|\mathbb{G}|$, $|\mathbb{G}_T|$ and $|\mathbb{Z}_q^*|$ respectively denote the bit-length of an element in \mathbb{G} , \mathbb{G}_T and \mathbb{Z}_q^* . C_p , C_{e_T} and C_e denote the computation cost of a bilinear pairing, an exponentiation in \mathbb{G}_T and an exponentiation in \mathbb{G} , respectively. t is the total number of the time periods that the system lifetime is divided into. We assume that the corresponding schemes share the same security parameter. Note by \perp we mean non-applicable.

Experimental comparison. In addition, we provide an experimental evaluation of our proposed scheme and show the performance comparison with [1]-4. Our experiment is simulated on the PC equipped with an Intel Core i5-4460 Processor running at 3.2 GHz with 8G memory. The programming language is C and the operations in bilin-

Table 2: Communication comparison

Schemes	[1]-4	Ours
Secret key size	$2 \mathbb{Z}_q^* $	$ \mathbb{Z}_q^* $
Helper key size	\perp	$t \mathbb{Z}_q^* $
Original ciphertext size	$2 \mathbb{G}_T $	$ \mathbb{G} + \mathbb{G}_T $
Re-encrypted ciphertext size	$2 \mathbb{G}_T $	$ \mathbb{G} + \mathbb{G}_T $

Table 3: Computation comparison

Schemes	[1]-4	Ours
Initial keys generation	$2C_e$	$(t+1)C_e$
ReKey generation	C_e	C_e
Secret key update	\perp	tC_e
Original ciphertext generation	$2C_p + 2C_{e_T}$	$C_p + C_{e_T} + C_e$
Re-encrypted ciphertext generation	$2C_p + C_{e_T} + C_e$	C_p
Decryption (original ciphertext)	C_{e_T}	$C_p + C_{e_T}$
Decryption (re-encrypted ciphertext)	$C_p + 2C_{e_T}$	C_{e_T}

ear groups are implemented by using the stanford PBC library 0.5.14 (available at <https://crypto.stanford.edu/pbc/>). In our experimentation, we use PBC Type A pairing which is constructed on the curve $y^2 \equiv x^3 + x \pmod p$ for some prime $p \equiv 3 \pmod 4$ and the embedding degree is 2. We choose the 80-bit security level. The sizes of p, q are 512 bits and 160 bits respectively. The size of an element in group \mathbb{G} is 1024 bits. With the above settings, we learn that an exponentiation operation in \mathbb{G} costs 8.31 ms, an exponentiation operation in \mathbb{G}_T costs 1.98 ms and a pairing operation costs 16.67 ms. Furthermore, we choose the number of time periods $t = 5$ and pellucidly describe the output results for each algorithms as well as the time consumption comparison with [1]-4 in Figure 2.

7 Conclusions

In this paper, we proposed a novel KIPRE scheme to achieve both key insulation and decryption right delegation in a cloud environment. Our scheme, for the first

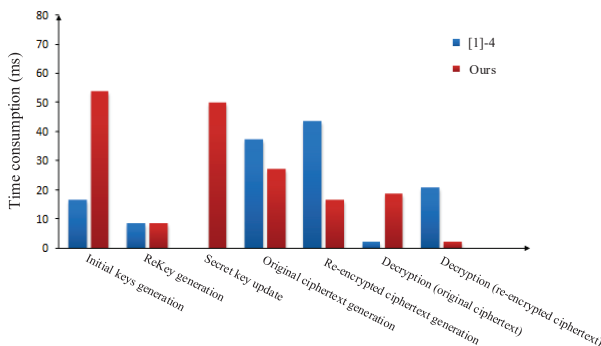


Figure 2: Time consumption comparison

time, addressed the key exposure problem in PRE settings. Meanwhile, it not only supported temporary delegation, but also satisfied time-release delegation (we defined in Section 6.1). The main advantage of our scheme is that it can mitigate the damage caused by user's secret key leakage for data sharing in a cloud environment. Moreover, we also showed the acceptability of our scheme on security and efficiency.

Acknowledgments

This work was supported in part by the National Science Foundation of China (No. 61370026, No. 61602096 and No. 61370026), the National High Technology Research and Development Program of China (No. 2015AA016007), Science and Technology Project of Guangdong Province (No. 2016A010101002).

References

- [1] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," *ACM Transactions on Information and System Security*, vol. 9, no. 1, pp. 1–30, 2006.
- [2] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in *International Conference on the Theory and Application of Cryptography*, pp. 127–144, Springer, 1998.
- [3] R. Canetti and S. Hohenberger, "Chosen-ciphertext secure proxy re-encryption," in *14th ACM Conference on Computer and Communications Security*, pp. 185–194, 2007.
- [4] P. S. Chung, C. W. Liu, and M. S. Hwang, "A study of attribute-based proxy re-encryption scheme in cloud environments," *International Journal of Network Security*, vol. 16, no. 1, pp. 1–13, 2014.
- [5] Y. Dodis, J. Katz, S. Xu, and M. Yung, "Key-insulated public key cryptosystems," in *International Conference on the Theory and Applications of Cryptographic Techniques Amsterdam*, pp. 65–82, 2002.
- [6] Y. Dodis and A. Yampolskiy, "A verifiable random function with short proofs and keys," in *8th International Workshop on Theory and Practice in Public Key Cryptography*, pp. 416–431, 2005.
- [7] X. Fu, "Unidirectional proxy re-encryption for access structure transformation in attribute-based encryption schemes," *International Journal of Network Security*, vol.17, no.2, PP. 142–149, Mar. 2015.
- [8] G. Hanaoka, Y. Hanaoka, and H. Imai, "Parallel key-insulated public key encryption," in *9th International Conference on Theory and Practice in Public-Key Cryptography*, pp. 105–122, 2006.
- [9] G. Hanaoka and J. Weng, "Generic constructions of parallel key-insulated encryption," in *7th International Conference on Security and Cryptography for Networks*, pp. 36–53, 2010.

- [10] Y. Hanaoka, G. Hanaoka, J. Shikata, and H. Imai, "Unconditionally secure key insulated cryptosystems: models, bounds and constructions," in *4th International Conference on Information and Communications Security*, pp. 85–96, 2002.
- [11] H. Hong and Z. Sun, "High efficient key-insulated attribute based encryption scheme without bilinear pairing operations," *SpringerPlus*, vol. 5, no. 1, pp. 1–12, 2016.
- [12] A. Ivan and Y. Dodis, "Proxy cryptography revisited," in *Annual Network and Distributed System Security Symposium*, pp. 1–20, 2003.
- [13] H. Khurana, A. Slagell, and R. Bonilla, "Sels: a secure e-mail list service," in *Proceedings of the 2005 ACM Symposium on Applied Computing*, pp. 306–313, 2005.
- [14] C. Liu, W. Hsien, C. Yang, and M. Hwang, "A survey of attribute-based access control with user revocation in cloud data storage," *International Journal of Network Security*, vol. 18, no. 5, pp. 900–916, 2016.
- [15] C. Liu, W. Hsien, C. Yang, and M. Hwang, "A survey of public auditing for shared data storage with user revocation in cloud computing," *International Journal of Network Security*, vol. 18, no. 4, pp. 650–666, 2016.
- [16] Q. Liu, C. Tan, J. Wu, and G. Wang, "Reliable re-encryption in unreliable clouds," in *IEEE Global Telecommunications Conference (GLOBECOM'11)*, pp. 1–5, 2011.
- [17] Q. Liu, G. Wang, and J. Wu, "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment," *Information Sciences*, vol. 258, pp. 355–370, 2014.
- [18] E. J. L. Lu, M. S. Hwang, C. J. Huang, "A new proxy signature scheme with revocation," *Applied mathematics and Computation*, vol. 161, no. 3, pp. 799–806, 2005.
- [19] M. Mambo and E. Okamoto, "Proxy cryptosystems: Delegation of the power to decrypt ciphertexts," *IEEE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 80, no. 1, pp. 54–63, 1997.
- [20] R. Mukherjee and J. Atwood, "Proxy encryptions for secure multicast key management," in *28th Annual IEEE International Conference on Local Computer Networks*, pp. 377–384, 2003.
- [21] C. Sur, C. Jung, Y. Park, and K. Rhee, "Chosen-ciphertext secure certificateless proxy re-encryption," in *IFIP International Conference on Communications and Multimedia Security*, pp. 214–232, 2010.
- [22] X. Tian, X. Wang, and A. Zhou, "Dsp re-encryption based access control enforcement management mechanism in daas," *International Journal of Network Security*, vol. 15, no. 1, pp. 28–41, 2013.
- [23] Z. Wan, J. Li, and X. Hong, "Parallel key-insulated signature scheme without random oracles," *Journal of Communications and Networks*, vol. 15, no. 3, pp. 252–257, 2013.
- [24] Z. Wang, Y. Lu, G. Sun, "A policy-based deduplication mechanism for securing cloud storage," *International Journal of Electronics and Information Engineering*, vol. 2, no. 2, pp. 70–79, 2015.
- [25] T. Wu, Y. Tseng, and C. Yu, "Id-based key-insulated signature scheme with batch verifications and its novel application," *International Journal of Innovative Computing, Information and Control*, vol. 8, no. 7, 2012.
- [26] Q. Xie, S. Jiang, L. Wang, and C. Chang, "Composable secure roaming authentication protocol for cloud-assisted body sensor networks," *International Journal of Network Security*, vol. 18, no. 5, pp. 816–831, 2016.
- [27] P. Xu, T. Jiao, Q. Wu, W. Wang, and H. Jin, "Conditional identity-based broadcast proxy re-encryption and its application to cloud email," *IEEE Transactions on Computers*, vol. 65, no. 1, pp. 66–79, 2016.
- [28] M. Zareapoor, P. Shamsolmoali, and M. A. Alam, "Establishing safe cloud: Ensuring data security and performance evaluation," *International Journal of Electronics and Information Engineering*, vol. 1, no. 2, pp. 88–99, 2014.

Biography

Yilei Wang is pursuing his Ph.D. degree in the School of Information and Software Engineering, University of Electronic Science and Technology of China (UESTC). He received his B.S. degree from School of Communication and Information, UESTC, in 2008. He received his M.S. from Faculty of Engineering, Lund University of Sweden, in 2011. His research interests include security and application of mobile network data.

Dongjie Yan received his B.S. degree from University of Electronic Science and Technology of China (UESTC) in 2014. He is currently pursuing his M.S. degree in the School of Information and Software Engineering, UESTC. His research interests include cryptographic protocols and network security.

Fagen Li received his Ph.D. degree in Cryptography from Xidian University, Xi'an, P.R. China in 2007. He is now a associate professor in the School of Computer Science and Engineering, University of Electronic Science and Technology of China (UESTC). His recent research interests include cryptography and network security.

Hu Xiong is an associate Professor at University of Electronic Science and Technology of China (UESTC). He received his Ph.D. degree from UESTC in 2009. His research interests include cryptographic protocols and network security.

An Improved Key-Management Scheme for Hierarchical Access Control

Wan-Yu Chao¹, Cheng-Yi Tsai², Min-Shiang Hwang^{2,3}

(Corresponding author: Min-Shiang Hwang)

Department of Management Information Systems, National Chung Hsing University¹

Department of Computer Science and Information Engineering, Asia University²

No. 500, Lioufeng Raod, Wufeng Shiang, Taichung 41354, Taiwan

Department of Medical Research, China Medical University Hospital, China Medical University³

No.91, Hsueh-Shih Road, Taichung 40402, Taiwan

(Email: mshwang@asia.edu.tw)

(Received Aug. 27, 2016; revised and accepted Oct. 9, 2016)

Abstract

Now, most institutions share the data through the Internet. With the rapid development of the Internet and the cloud storage, data-sharing becomes so easy that the data was stolen or destroyed easier than before. Therefore, accessing data should strictly control to avoid unauthorized access. In this paper, we propose the more efficient key management scheme for hierarchical access control than Odelu et al.'s scheme.

Keywords: Access Control; Hierarchical Access Control; Key Management

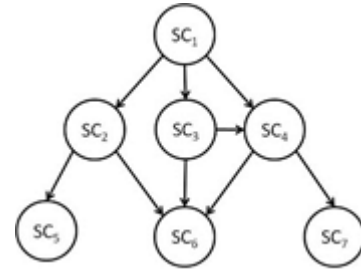


Figure 1: An example of user hierarchy system [16]

1 Introduction

The user hierarchy system is represented by a set of disjoint security class SC_i ($i = 1, 2, \dots, N$) and a partially ordered set (POSET) (SC, \leq) , where \leq (i.e. $<$ or $=$) is a binary partially ordered relationship in a user set [10, 11, 12]. Generally, this hierarchy system is managed by a trusted central authority (CA). CA distributes the secret key (SK_i) to each security class (SC_i) and announces the corresponding public information in a public domain. $SC_j < SC_i$ denotes that SC_i is a predecessor of SC_j , and SC_j is a successor of SC_i ; and a predecessor security class can derive its successors' secret keys (SK_j). We take a user hierarchy system as an example in Figure 1 [5, 7, 13]. When $SC_2 \leq SC_1$, we can know that SC_2 is a successor of SC_1 . If SC_2 encrypts files using its secret key (SK_2), SC_1 derives SC_2 's secret key to access the files which are encrypted by SC_2 .

In 1983, Akl and Taylor [1] proposed the cryptographic solution to the problem of access control, the first concept of the cryptographic key assignment scheme in an arbitrary POSET hierarchy. A lot of related works have been proposed to solve access control prob-

lems [2, 3, 4, 6, 8, 9, 14, 15, 17, 18, 19]. In 2013, Odelu et al. [16] proposed an efficient and secure access control scheme only based on symmetric-key cryptosystems and one-way hash functions.

2 Review of Odelu et al.'s Schemes

In this section, we briefly introduce Odelu et al.'s scheme [16]. In Table 1, we show the notations' meaning in this paper. We just describe two phases in this scheme: key generation phase and key derivation phase.

2.1 Key Generation Phase

Firstly, CA builds the hierarchical structure for controlling access among the security classes. Let two security classes be $SC_i, SC_j \in SC$ and $SC_j \leq SC_i$ ($1 \leq i \leq N$ and $1 \leq j \leq N$).

Step 1: CA chooses $(H(\cdot), \Omega)$ and publishes them. Then CA selects randomly its own secret key (k_{CA})

Table 1: Notations' meanings used in this paper

Notation	Meaning
$H(\cdot)$	A one-way hash function
$E_k(\cdot)/D_k(\cdot)$	AES encryption/decryption with key k
Ω	A symmetric-key cryptosystem
$ $	Concatenation
\oplus	Exclusive-OR
CA	The trusted central authority
ID_{CA}	An identity of CA
$ID(SC_i)$	An identity of SC_i
T_{SHA1}	Time for hashing 512 bits message block using SHA-1
T_{AES}	Time for encrypting/decrypting 128 bits message block using AES with a 128 bits key.

and also calculates its own private key $K = H(ID_{CA}||k_{CA})$.

Step 2: CA selects randomly the secret key (SK_i), and sub-secret key (d_i) for each security class ($SC_i, 1 \leq i \leq N$) in the hierarchical structure.

Step 3: For each security class SC_i , CA computes the encryption key $EK_i = H(ID_{CA}||k_{CA}||d_i)$ and the private key $K_i = H(ID_{CA}||d_i)$.

Step 4: CA computes the following public parameters:

- 1) For each security class $SC_j \leq SC_i$, computes $M_{ij} = E_{EK_i}(SK_j)$.
- 2) For SC_i , computes $R_i = E_{K_i}(EK_i)$ and the signature $Sign_i = H(ID_{CA}||SK_i)$.
- 3) CA encrypts K_i as $S_i = E_K(K_i)$.

Step 5: CA finally sends d_i to each SC_i via the secure channel.

2.2 Key Derivation Phase

This phase introduces how the security class (SC_i) derives the corresponding successor security classes' (SC_j) secret key (SK_j) from the public parameters available in the public domain.

Step 1: SC_i uses its own sub-secret key to compute its private key, $K_i = H(ID_{CA}||d_i)$ and then decrypts R_i for the encryption key, $EK_i = D_{K_i}(R_i)$.

Step 2: SC_i decrypts M_{ij} to obtain the secret keys $SK_j = D_{EK_i}(M_{ij})$.

Step 3: SC_i computes the signature $Sign_j^* = H(ID_{CA}||SK_j)$ and then verifies whether $Sign_j^* = Sign_j$ or not. If yes, the derived secret key (SK_j) is legitimate.

3 The Proposed Scheme

We propose our scheme based on a hybrid cryptosystem utilizing a symmetric-key cryptosystem and a one-way hash function. At First, we present the key generation phase and key derivation phase. Finally, we show the dynamic key management.

3.1 Key Generation Phase

Like Odelu et al.'s scheme, CA builds the hierarchical structure for access control. Let two security classes be $SC_i, SC_j \in SC$ and $SC_j \leq SC_i$ ($1 \leq i \leq N$ and $1 \leq j \leq N$).

Step 1: CA selects ($H(\cdot), \Omega$) and declares them publicly. Then CA chooses its own secret key (k_{CA}) randomly.

Step 2: CA selects randomly the secret key (SK_i), sub-secret key (d_i) for each security class ($SC_i, 1 \leq i \leq N$) in the hierarchical structure.

Step 3: CA calculates the encryption key (EK_i) for each security class as $EK_i = H(k_{CA}||ID(SC_i))$.

Step 4: CA computes the public parameters (M_{ij}, R_i) for each security class as $M_{ij} = E_{EK_i}(SK_j \oplus ID_{CA})$, and $R_i = E_{d_i}(EK_i)$.

Step 5: At last, CA sends d_i to each SC_i securely and clears all keys (SK_i, d_i, EK_i).

3.2 Key Derivation Phase

For $SC_j \leq SC_i$, we show how the security class (SC_i) derives the secret keys (SK_j) of all its successors (SC_j) and its own secret key from the public parameters, and verifies that secret key is legitimate.

Step 1: SC_i uses its sub-secret key to decrypt R_i as $EK_i = D_{d_i}(R_i)$.

Step 2: SC_i decrypts M_{ij} to obtain $SK_j \oplus ID_{CA} = D_{EK_i}(M_{ij})$.

Table 2: The storage space requirement in the hierarchy shown in Figure 1

CA (Private Domain)	Public Domain		SC _i (Private Domain)	
k_{CA}	R_1	$M_{11}, M_{12}, M_{13}, M_{14}, M_{15}, M_{16}, M_{17}$	d_1	SC_1
	R_2	M_{22}, M_{25}, M_{26}	d_2	SC_2
	R_3	$M_{33}, M_{34}, M_{36}, M_{37}$	d_3	SC_3
	R_4	M_{44}, M_{46}, M_{47}	d_4	SC_4
	R_5	M_{55}	d_5	SC_5
	R_6	M_{66}	d_6	SC_6
	R_7	M_{77}	d_7	SC_7

Step 3: If M_{ij} does not change by the attacker, we can get $SK_j = (SK_j \oplus ID_{CA}) \oplus ID_{CA}$. If not, SC_i will notify CA that M_{ij} is wrong.

3.3 Dynamic Key Management

3.3.1 Insert a New Security Class into the Existing Hierarchical Structure

Assume that a security class (SC_x) with the relationships $SC_j \leq SC_x \leq SC_i$ was inserted into an existing hierarchical structure. CA executes the following steps to manage the accessing priority:

Step 1: CA randomly selects a secret key (SK_x), a sub-secret key (d_x) for the security class (SC_x).

Step 2: For SC_x , CA calculates the encryption key (EK_x) as $EK_x = H(k_{CA} || ID(SC_x))$, and then computes $R_x = E_{(d_x)}(EK_x)$.

Step 3: CA computes the public parameters corresponding to SC_x 's predecessors and successors including itself and declares publicly as follows:

- 1) For all $SC_x \leq SC_i$, CA calculates $EK_i = H(k_{CA} || ID(SC_i))$ and public parameters as $M_{ix} = E_{(EK_i)}(SK_x \oplus ID_{CA})$.
- 2) For all $SC_j \leq SC_x$, CA computes $SK_j = D_{(EK_j)}(M_{jj}) \oplus ID_{CA}$. If it is valid, the CA computes the public parameters as $M_{xj} = E_{(EK_x)}(SK_j \oplus ID_{CA})$.

Step 4: CA sends d_x to SC_x securely.

3.3.2 Delete a Security Class from the Existing Hierarchical Structure

Suppose that an existing security class (SC_x) was deleted from the existing user hierarchical structure ($SC_j \leq SC_x \leq SC_i$). In order to assure the forward security, SC_x does not have permission to access all the information which was authorized originally after being deleted from the user hierarchy system. CA performs the following steps to manage the authority to access:

Step 1: CA removes all the parameters corresponding to SC_x .

Step 2: For all the successors SC_j ($SC_j \leq SC_x$), CA renews the secret key as SK_j^* .

Step 3: For all the relationships $SC_j \leq SC_i$, CA renews the parameter $M_{ij}^* = E_{(EK_i)}(SK_j^* \oplus ID_{CA})$.

4 Analysis of the Proposed Scheme

In this section, we provide the analysis of security, storage and computational overheads required in our scheme. We assume that there are N security classes in the hierarchy system which forms a set $SC = \{SC_1, SC_2, \dots, SC_N\}$, and each security class SC_i has v_i number of predecessors.

4.1 Storage Complexity

In Table 2, we show the storage space of private and public domains of CA and security classes for the hierarchy as shown in Figure 1. In our scheme, each key (k_{CA} , SK_i , d_i , EK_i) uses 128 bits, so CA and SC_i 's private domain need 128 bits storage space. And considering the public domain for storage complexity, CA requires to store public parameters in the public domain: ID_{CA} requires 128 bits, and $NID(SC_i)$ need 128N bits; NR_i require 128N bits, and finally M_{ij} need $128(\sum_{i=1}^N (v_i + 1))$ bits. The total storage complexity required for the public domain is $128(\sum_{i=1}^N (v_i + 1) + 2N + 1)$ bits. We present the comparison of the storage space between our scheme and Odelu et al.'s scheme [16] in Table 3.

4.2 Computational Complexity

For analysis of the computational complexity, because exclusive-OR operation requires very few computations, we neglect considering its computational cost in this paper. CA computes the NEK_i which require NT_{SHA1} operations, NR_i which need NT_{AES} operations, and finally M_{ij} which need $\sum_{i=1}^N (v_i + 1)T_{AES}$ operations. And during the key derivation phase, all security classes SC_i in the hierarchy need to compute the followings: decrypting R_i requires NT_{AES} operations, and decrypting M_{ij} needs $\sum_{i=1}^N (v_i + 1)T_{AES}$ operations. Therefore,

Table 3: Comparison of the storage space

Schemes	Private Domain		Public Domain
	CA	SC_i	
Odelu et al. [16]	128	128	$128(\sum_{i=1}^N (v_i + 1) + 3N + 1)$
Ours	128	128	$128(\sum_{i=1}^N (v_i + 1) + 2N + 1)$

Table 4: Comparison of computational costs

Schemes	Time complexity
Odelu et al. [16]	$(3N + 2 \sum_{i=1}^N (v_i + 1))T_{AES} + (5N + 1)T_{SHA1}$
Ours	$(2N + 2 \sum_{i=1}^N (v_i + 1))T_{AES} + NT_{SHA1}$

the total computational complexity for the key generation and derivation phases becomes $(2N + 2 \sum_{i=1}^N (v_i + 1))T_{AES} + NT_{SHA1}$. We also present the comparison of computational costs between our scheme and Odelu et al.'s scheme [16] in Table 4.

4.3 Security Analysis

Then we show that our scheme can resist three attacks which often occur in the user hierarchy system.

- 1) Contrary attack: In this attack, SC_i is a predecessor security class of a successor SC_j ($SC_j < SC_x$). The attacker SC_j attempts to derive the secret key (SK_i) of SC_i from the public parameters available in the public domain. SC_j has $M_{ii} = E_{(EK_i)}(SK_i \oplus ID_{CA})$ and $R_i = E_{(d_i)}(EK_i)$. Because d_i is the sub-secret key only known to SC_i , SC_j cannot decrypt R_i to know EK_i . Therefore, SC_j cannot decrypt M_{ii} without EK_i . In a word, it is infeasible that SC_j derives SK_i of SC_i . Our proposed scheme can resist the contrary attack.
- 2) Collaborative attack: Suppose that several users in security classes (SC_j, SC_x) collaborate to derive illegally the secret key (SK_i) of their predecessor (SC_i), where $SC_j, SC_x < SC_i$. The attackers cannot use their sub-secret keys (d_j, d_x) and public parameters ($M_{ii}, M_{ij}, M_{ix}, R_i$) to compute EK_i , because d_i is the sub-secret key only known to SC_i . As a result, SC_j and SC_x cannot get SK_i through collaborative attack.
- 3) Forward security of successors: When we delete a security class (SC_x) from the existing hierarchical structure ($SC_j < SC_x < SC_i$), CA replaces the secret key (SK_j) of SC_j with the renewed secret key SK_j^* and the related public parameters. Therefore, SC_x will not have chance to get the new secret key SK_j^* .

5 Conclusion

In this paper, we have proposed an improved key management scheme to solve a dynamic access problem in a user hierarchy by utilizing a symmetric-key cryptosystem and a one-way hash function. Compared with Odelu et al.'s scheme [16], both the time complexity and storage space are reduced in our scheme. Our scheme is more efficient and suitable for the hierarchy system.

References

- [1] S. G. Akl and P. D. Taylor, "Cryptographic solution to a problem of access control in a hierarchy," *ACM Transactions on Computer Systems*, vol. 1, no. 3, pp. 239–248, July 1983.
- [2] B. J. Cacic and R. Wei, "Improving indirect key management scheme of access hierarchies," *International Journal of Network Security*, vol. 4, no. 2, pp. 128–137, 2007.
- [3] D. Giri and P. D. Srivastava, "A cryptographic key assignment scheme for access control in poset ordered hierarchies with enhanced security," *International Journal of Network Security*, vol. 7, no. 2, pp. 223–234, 2008.
- [4] D. Giri and P. D. Srivastava, "An asymmetric cryptographic key assignment scheme for access control in tree structural hierarchies," *International Journal of Network Security*, vol. 4, no. 3, pp. 348–354, 2007.
- [5] M. S. Hwang, "A cryptographic key assignment scheme in a hierarchy for access control," *Mathematical and Computer Modelling*, vol. 26, no. 2, pp. 27–31, 1997.
- [6] M. S. Hwang, "Extension of CHW cryptographic key assignment scheme in a hierarchy," *IEEE Proceedings Computers and Digital Techniques*, vol. 146, no. 4, pp. 219, 1999.
- [7] M. S. Hwang, "An improvement of novel cryptographic key assignment scheme for dynamic access control in a hierarchy," *IEICE Transactions on*

Fundamentals Of Electronics, Communications and Computer Sciences, vol. 82-A, no. 3, pp. 548–550, 1999.

- [8] M. S. Hwang, “A new dynamic cryptographic key generation scheme in a hierarchy,” *Nordic Journal of Computing*, vol. 6, no. 4, pp. 363–371, 1999.
- [9] M. S. Hwang, “An asymmetric cryptographic scheme for a totally-ordered hierarchy,” *International Journal of Computer Mathematics*, vol. 73, pp. 463–468, 2000.
- [10] M. S. Hwang, “Cryptanalysis of YCN key assignment scheme in a hierarchy,” *Information Processing Letters*, vol. 73, no. 3, pp. 97–101, 2000.
- [11] M. S. Hwang and W.P. Yang, “Controlling access in large partially ordered hierarchies using cryptographic keys,” *Journal of Systems and Software*, vol. 67, no. 2, pp. 99–107, 2003.
- [12] Iuon-Chung Lin, Min-Shiang Hwang, and Chin-Chen Chang, “A new key assignment scheme for enforcing complicated access control policies in hierarchy,” *Future Generation Computer Systems*, vol. 19, no. 4, pp. 457–462, 2003.
- [13] Iuon-Chung Lin, H. H. Ou, and Min-Shiang Hwang, “Efficient access control and key management schemes for mobile agents,” *Computer Standards & Interfaces*, vol. 26, no. 5, pp. 423–433, 2004.
- [14] X. Liu, J. Ma, J. Xiong, and G. Liu, “Ciphertext-policy hierarchical attribute-based encryption for fine-grained access control of encryption data,” *International Journal of Network Security*, vol. 16, no. 6, pp. 437–443, 2014.
- [15] J. W. Lo, M. S. Hwang, and C. H. Liu, “An efficient key assignment scheme for access control in a large leaf class hierarchy,” *Information Sciences*, vol. 181, no. 4, pp. 917–925, 2011.
- [16] V. Odelu, A. K. Das, and A. Goswami, “An effective and secure key-management scheme for hierarchical access control in e-medicine system,” *Journal of Medical Systems*, vol. 37, no. 2, 2013. (doi: 10.1007/s10916-012-9920-5)
- [17] S. F. Tzeng, C. C. Lee, and T. C. Lin, “A novel key management scheme for dynamic access control in a hierarchy,” *International Journal of Network Security*, vol. 12, no. 3, pp. 178–180, 2011.
- [18] Q. Zhang, Y. Wang, and J. P. Jue, “A key management scheme for hierarchical access control in group communication,” *International Journal of Network Security*, vol. 7, no. 3, pp. 323–334, 2008.
- [19] R. Zhou, C. Xu, W. Li, and J. Zhao, “An id-based hierarchical access control scheme with constant size public parameter,” *International Journal of Network Security*, vol. 18, no. 5, pp. 960–968, 2016.

Management Information Systems from National Chung Hsing University. Her current research interests include applied cryptography, cloud computing, and mobile communications.

Cheng-Yi Tsai received the B.S. degree in Department of Business Administration from Chaoyang University of Technology (CYUT), Taichung, Taiwan, in 2001; the M.S. degree in Computer Science & Information Engineering from Asia University, Taichung, Taiwan, in 2005. He is currently pursuing his PHD degree in Graduate Institute of Computer Science & Information Engineering from Asia University. His current research interests include applied cryptography and mobile communications.

Min-Shiang Hwang Min-Shiang Hwang received the B.S. in Electronic Engineering from the National Taipei Institute of Technology, Taipei, Taiwan, in 1980; the M.S. in Industrial Engineering from the National Tsing Hua University, Taiwan, in 1988; and a Ph.D. in Computer and Information Science from the National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at the National Cheng Kung University, Taiwan, from 1984-1986. Dr. Hwang passed the National Higher Examination in field “Electronic Engineer” in 1988. He also passed the National Telecommunication Special Examination in field “Information Engineering”, qualified as advanced technician the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications. He was also the chairman of the Department of Information Management, Chaoyang University of Technology (CYUT), Taiwan, during 1999-2002. He was a professor and chairman of the Graduate Institute of Networking and Communications, CYUT, during 2002-2003. He was a professor and chairman of the Department of Management Information Systems, National Chung Hsing University (NCHU), during 2003-2009. He was also a visiting professor of UC. Riverside and UC. Davis (USA) during 2009-2010. He was a distinguished professor of the department of Management Information Systems, NCHU, during 2007-2011. He obtained the 1997, 1998, 1999, 2000, and 2001 Excellent Research Award of National Science Council (Taiwan). He was a dean of College of Computer Science, Asia University (AU). He is currently a Chair Professor of the department of Computer Science & Information Engineering, AU. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include information security, electronic commerce, database and data security, cryptography, image compression, and mobile computing. Dr. Hwang has published over 200+ articles on the above research fields in international journals.

Biography

Wan-Yu Chao received the B.S. degree in Information Management from Central Police University, Taiwan, Republic of China; the M.S. degree in Graduate Institute of

NFC Communications-based Mutual Authentication Scheme for the Internet of Things

Yanna Ma

(Corresponding author: Yanna Ma)

Zhejiang University of Water Resources and Electric Power, Zhejiang 310000, China

(Email: helenmayanna@163.com.)

(Received May 10, 2016; revised and accepted Sept. 3 & Sept. 25, 2016)

Abstract

The integration of Near Field Communication (NFC) into consumer electronics devices has opened up opportunities for the internet of things applications such as electronic payment, electronic ticketing and sharing contacts, etc.. Meanwhile, various security risks should not be ignored. Therefore, all kinds of different protocols have been released with the purposing of securing NFC communications. Lately, a pseudonym-based NFC protocol for the consumer Internet of things was presented. They claimed that their scheme could withstand man-in-the-middle attack headed from their scheme could provide mutual authentication. This study presents a security analysis on their scheme and finds that their scheme is not really secure against man-in-the-middle attack. Subsequently, this paper proposes an enhancement for purpose of thwarting this security attack. The security and performance analyses show that the enhancement is secure and efficient while keeping privacy preserving.

Keywords: Authentication; Key Establishment; Smart Cards; Wireless Communications

1 Introduction

Several wireless communications techniques and protocols are available in the market, such as Bluetooth, ZigBee, RFID, Wi-Fi and Infrared, which have different working frequencies and ranges. A more recent technology for short-range wireless (up to 10 cm) is the Near Field Communication (NFC) [16] that enables an easy, fast and secure communication between two devices in proximity. Its communication occurs with 13.56 MHz operating frequency while providing a high-level safety than other well-known wireless technologies, e.g. Bluetooth [3, 6]. The primary characteristic of NFC, leading to its widespread use and popularity is the advent of touch-less transactions, which leads to no cards, no coins and no laborious connections and network setup [2]. NFC thus enables the long awaited Internet-of-Things (IoT) [13], changing the interactions with the world in subtle but pervasive

ways while providing digitally immersive experience. Although the communication range of NFC is limited to a few centimeters, NFC alone does not ensure secure communications, especially authentication between the sender and the recipient. One of the most important properties for data communication is mutual authentication which is defined as the ability that both communicating parties can authenticate with each other, thus preventing man-in-the-middle attack and replay attack [11, 14, 17]. In order to be secure NFC, the NFC security standards have been proposed in order to define data exchange format, tag types, and security protocols, e.g., a key agreement protocol [8, 9, 10]. In the process of key agreement, Certificate Authority (CA) as the Trusted Third Party (TTP) is in charge of generating the public key of the correspondents.

Recently, Eun et al. [5] proposed an authentication scheme for NFC communications to prevent replay and man-in-the-middle attack by providing mutual authentication based on a trusted service manager. The scheme was based on asymmetric cryptography and hash functions. By using an asymmetric cryptographic system, it was possible to address several security threats such as an evil twin attack, hotspot or captive portal eavesdropping, and even man-in-the-middle attacks [15]. However, He et al. [7] found that the scheme of Eun et al. could not resist impersonation attack. As a counter measure to these sufferings, He et al. presented a modified authentication NFC protocol to amend aforementioned security weaknesses. Unfortunately, this study showed that He et al.'s modification was not secure against the man-in-the-middle attack. As a result, a secure NFC mutual authentication scheme with privacy preservation for the Internet of things was designed in this paper.

The remainder of the paper is arranged as follows. In Section 2, a brief review of He et al.'s security protocol. In Section 3, man-in-the-middle attack is developed to analyze Eun et al.'s protocol. In Section 4, the proposed NFC communication-based protocol. Security and performance analyses results are given in Sections 5 and 6, respectively. Section 7 concludes this paper.

2 Review of He et al.'s Scheme

This part concisely review the NFC mutual authentication scheme by He et al. in 2014. For ease of presentation, Table I shows some intuitive abbreviations and notations.

Table 1: Notations

ID_X	the identity of the user X
TSM	a trusted service manager
G	the base point of the elliptic curve
KDF	a key derivation function
d_X	the private key of the user X
Q_X	the public key of the user X , where $Q_X = d_X G$
SK	exclusive-or operation
$E_K(m)$	symmetric encryption of using the key K
$h(\cdot), f(\cdot)$	hash functions
$Sig_K(m)$	signature of m using the key K

Once receiving the user A 's request, the TSM generates n pseudonyms and delivers them to A via a private channel. The TSM also stores the user A 's identity and pseudonyms into its database. Next, the TSM computes $PN_A^i = \{Q_A^i, E_{d_{TSM}}(ID_A, Q_A^i), ID_{TSM}, S_{TSM}^i\}$ and $S_{TSM}^i = Sig_{d_{TSM}}(Q_A^i, E_{d_{TSM}}(ID_A, Q_A^i), ID_{TSM})$, where $Q_A^i = q_A^i G$ is the public key of A , $d_A^i = q_A^i + h(ID_{TSM}, PN_A^i)d_{TSM}$ is A 's private key, and S_{TSM}^i is the TSM 's signature on the i th message.

The users A and B execute the establishment of the session key in the following manner:

Step 1: A computes $Q'_A = r_A G$ and sends the message $\{PN_A^i, Q'_A, N_A\}$ to B , where r_A and N_A are the random numbers generated by A , PN_A^i is a pseudonym selected by A .

Step 2: B computes $Q'_B = r_B G$ and sends back the message $\{PN_B^j, Q'_B, N_B\}$ to A , where r_B and N_B are the random numbers generated by B and PN_B^j is a pseudonym selected by B .

Step 3: After receiving the message, A computes $Z_A^1 = r_A Q'_B$, $Z_A^2 = d_A^i(Q_B^j + h(ID_{TSM}, PN_B^j)Q_{TSM})$, $SK = KDF(N_A, N_B, ID_A, ID_B, Z_A^1, Z_A^2)$ and $MacTag_A = f(SK, ID_A, ID_B, Q'_A, Q_A^2)$. Subsequently, A sends the message $\{MacTag_A\}$ to B .

Step 4: When receiving the message, B computes $Z_B^1 = r_B Q'_A$, $Z_B^2 = d_B^j(Q_A^i + h(ID_{TSM}, PN_A^i)Q_{TSM})$, $SK = KDF(N_A, N_B, ID_A, ID_B, Z_B^1, Z_B^2)$ and verifies $f(SK, ID_A, ID_B, Q'_A, Q'_B) \stackrel{?}{=} MacTag_A$. If it holds, B computes $MacTag_B = f(SK, ID_A, ID_B, Q'_A, Q'_B)$ and sets SK as the session key. Finally, B transmits the message $\{MacTag_B\}$ to A .

Step 5: Once receiving the message, A computes:

$$\begin{aligned}
 Z_A^1 &= r_A Q'_B = r_A r_B G \\
 &= r_B r_A G = r_B Q'_A, \\
 Z_A^2 &= d_A^i(Q_B^j + h(ID_{TSM}, PN_B^j)Q_{TSM}) \\
 &= (q_A^i + h(ID_{TSM}, PN_A^i)d_{TSM}) \\
 &\quad (q_B^j + h(ID_{TSM}, PN_B^j)d_{TSM})G \\
 &= (q_B^j + h(ID_{TSM}, PN_B^j)d_{TSM}) \\
 &\quad (q_A^i + h(ID_{TSM}, PN_A^i)d_{TSM})G \\
 &= (q_B^j + h(ID_{TSM}, PN_B^j)d_{TSM}) \\
 &\quad (q_A^i G + h(ID_{TSM}, PN_A^i)d_{TSM}G) \\
 &= d_B^j(Q_B^j + h(ID_{TSM}, PN_B^j)Q_{TSM}).
 \end{aligned}$$

A computes SK and $f(SK, ID_A, ID_B, Q'_A, Q'_B)$, then, A checks the correctness of the value $MacTag_B$. If it does not hold, A stops the session; Otherwise, A agrees on the session key SK with B .

3 Weaknesses of He et al.'s Scheme

He et al. declared that their improvements could resist the man-in-the-middle-attack due to their proposed scheme could provide the mutual authentication between A and B . Actually, a notable question is that A and B are unable to confirm the real identity of the other entity because of the absence of TSM during the execution of their scheme, thus giving a perfect opportunity for an adversary \mathbb{A} to launch the man-in-the-middle attack.

The man-in-the-middle attack is a form of active eavesdropping in which \mathbb{A} makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, while in fact the entire conversation is controlled by \mathbb{A} .

Let's describe the details of the attack as follows.

Step 1: When the message $M_1 = \{Q'_A, PN_A^j, N_A\}$ is sent from A to B , \mathbb{A} intercepts the message and computes $Q_A^* = r_{\mathbb{A}}^1 G$, and sends the forged message $M_1 = \{Q_A^*, PN_A^j, N_{\mathbb{A}}^1\}$ to B , where $r_{\mathbb{A}}^1$ and $N_{\mathbb{A}}^1$ are the random numbers of \mathbb{A} .

Step 2: When receiving the message, B computes $Q'_B = r_B G$ and sends the message $M_2 = \{Q'_B, PN_B^j, N_B\}$ to A .

Step 3: \mathbb{A} intercepts the message M_2 and computes $Q_B^* = r_{\mathbb{A}}^2 G$ and sends the forged message $M_2 = \{Q_B^*, PN_B^j, N_{\mathbb{A}}^2\}$ to A , where $r_{\mathbb{A}}^2$ and $N_{\mathbb{A}}^2$ are the random numbers of \mathbb{A} .

Step 4: After receiving the message, A computes $Z_A^2 = d_A^i(Q_B^* + h(ID_{TSM}, PN_B^j)Q_{TSM})$, $Z_A^1 = r_A Q'_B$, and the session key $SK = KDF(N_A, N_{\mathbb{A}}^2, ID_A, ID_B, Z_A^1, Z_A^2)$ and $MacTag_A =$

$f(SK, ID_A, ID_B, Q'_A, Q_B^*)$. Next, A sends the message $M_3 = \{MacTag_A\}$ to B .

Step 5: \mathbb{A} eavesdrops this message and computes $Z_A^2 = d_A^1(Q'_B + h(ID_{TSM}, PN_B^j)Q_{TSM})$, $Z_A^1 = r_A^1 Q'_B$, and the session key $SK = KDF(N_B, N_A^1, ID_A, ID_B, Z_A^1, Z_A^2)$ and $MacTag_A = f(SK, ID_A, ID_B, Q_A^*, Q'_B)$. After that, \mathbb{A} sends the forged message $M_3 = \{MacTag_A\}$ to B .

Step 6: When receiving the message M_3 , B computes $Z_B^1 = r_B Q_A^*$, $Z_B^2 = d_B^1(Q_A^* + h(ID_{TSM}, PN_B^j)Q_{TSM})$ and $SK = KDF(N_B, N_A^1, ID_A, ID_B, Z_B^1, Z_B^2)$. B verifies whether $f(SK, ID_A, ID_B, Q_A^*, Q'_B) \stackrel{?}{=} MacTag_A$ and it is obvious that the equation is true, because:

$$\begin{aligned} Z_B^1 &= r_B Q_A^* = r_B r_A^1 G \\ &= r_A^1 Q'_B = Z_A^1, \\ Z_B^2 &= d_B^1(Q_A^* + h(ID_{TSM}, PN_B^j)Q_{TSM}) \\ &= (q_A^j + h(ID_{TSM}, PN_B^j)d_{TSM}) \\ &\quad (q_A^i G + h(ID_{TSM}, PN_B^j)d_{TSM})G \\ &= (q_A^i + h(ID_{TSM}, PN_B^j)d_{TSM}) \\ &\quad (q_B^j + h(ID_{TSM}, PN_A^i)d_{TSM})G \\ &= d_A^1(Q'_B + h(ID_{TSM}, PN_B^j)Q_{TSM}) \\ &= Z_A^2. \end{aligned}$$

B computes $MacTag_B = f(SK, ID_A, ID_B, Q_A^*, Q'_B)$ and sends the message $M_4 = \{MacTag_B\}$ to A .

Step 7: \mathbb{A} receives the message M_4 from B to A , \mathbb{A} computes $Z_B^2 = d_A^i(Q'_A + h(ID_{TSM}, PN_B^j)Q_{TSM})$, $Z_B^1 = r_A^2 Q'_A$ and the session key $SK = KDF(N_A, N_A^2, ID_A, ID_B, Z_B^1, Z_B^2)$ and $MacTag_B = f(SK, ID_A, ID_B, Q'_A, Q_B^*)$. After that, \mathbb{A} sends the forged message $M_4 = \{MacTag_B\}$ to A .

Step 8: When receiving the message, A checks the validity of $MacTag_B$ and it is sure that the equation will be equal to $f(SK, ID_A, ID_B, Q'_A, Q_B^*)$. Therefore, A agrees on the session key SK as the common key aiming at encrypting the communication messages.

In this way, \mathbb{A} is successfully authenticated by A and B , respectively. That is, \mathbb{A} shares a session key $SK = KDF(N_A, N_A^2, ID_A, ID_B, Z_B^1, Z_B^2)$ with A , at the same time, he shares a session key $SK = KDF(N_B, N_A^1, ID_A, ID_B, Z_A^1, Z_A^2)$ with B . However, both of A and B do not know that they are communicating with an attacker at all. They believe they successfully have finished the handshake agreement with each other.

4 The Proposed Scheme

This section will present the proposed scheme as Figure 1.

After receiving the user A 's request for pseudonyms, the TSM generates n pseudonyms and sends them to

A via a secret channel. The TSM also stores the user A 's identity and pseudonyms into its database. There are four parties in a pseudonym PN_A^i : the A 's public key, A 's private key, the TSM 's identity and the TSM 's signature.

$$\begin{aligned} PN_A^i &= \{Q_A^i, Enc(\{ID_A, Q_A^i\}, d_{TSM}), ID_{TSM}, S_{TSM}^i\}, \\ S_{TSM}^i &= Sig(d_{TSM}, Q_A^i, Enc(Q_A^i, d_{TSM}), ID_{TSM}), \\ d_A^i &= d_{TSM} + h(ID_A, r_{S-A})h(ID_A, PN_A^i). \end{aligned}$$

As the same method, the user B could get its pseudonyms and corresponding private key $d_B^j = d_{TSM} + h(ID_B, r_{S-B})h(ID_B, PN_B^j)$ and public key $d_B^j G$.

4.1 Establishment of the Session Key

When A and B attempts to establish the handshake, they perform as follows:

Step 1: A computes $Q'_A = r_A G$, $Q''_A = r_A d_B^j G$, where r_A is a nonce generated by A . Then, A sends $\{Q'_A, Q''_A\}$ to B .

Step 2: When receiving the message, B computes $(d_B^j)^{-1}Q''_A = Q'_A$, $Q'_B = r_B G$, and $Q''_B = r_B d_A^i G$, where $d_A^i G$ is the public key of A . Finally, B returns $\{Q'_B, Q''_B\}$ to A .

Step 3: Once receiving the message, A computes $(d_A^i)^{-1}Q''_B = Q'_B$, $Z'_A = r_A Q'_B$, $Z''_A = d_A^i(Q_{TSM} + h(ID_B, PN_B^j)Q_A^i)$, $SK = KDF(ID_A, ID_B, Z'_A, Z''_A)$ and $MacTag_A = f(ID_A, ID_B, SK, Q'_B)$. At last, A sends back the message $\{MacTag_A\}$ to B .

Step 4: When receiving the messages, B computes $Z'_B = r_B Q'_A$, $Z''_B = d_B^j(Q_{TSM} + h(ID_A, PN_A^i)Q_B^j)$, $SK = KDF(ID_A, ID_B, Z'_B, Z''_B)$ and verifies whether $f(ID_A, ID_B, SK, Q'_B) \stackrel{?}{=} MacTag_A$. If it is equal, B sets SK as the session key and computes $MacTag_B = f(ID_A, ID_B, SK, Q'_A)$. After that, B delivers back the message $\{MacTag_B\}$ to A .

Step 5: When receiving the message, A checks whether $f(ID_A, ID_B, SK, Q'_A) \stackrel{?}{=} MacTag_B$. If it holds, A successfully negotiates the session key SK with B .

5 Security Analysis

This section analyze the security of the proposed scheme, which includes achieving users' anonymity, mutual authentication, perfect forward session key security, and withstanding relay attack, impersonation attack. The details describe below.

5.1 Users' Anonymity

In the proposed scheme, the users' identities ID_A and ID_B are respectively implied in $MacTag_{A(B)} =$

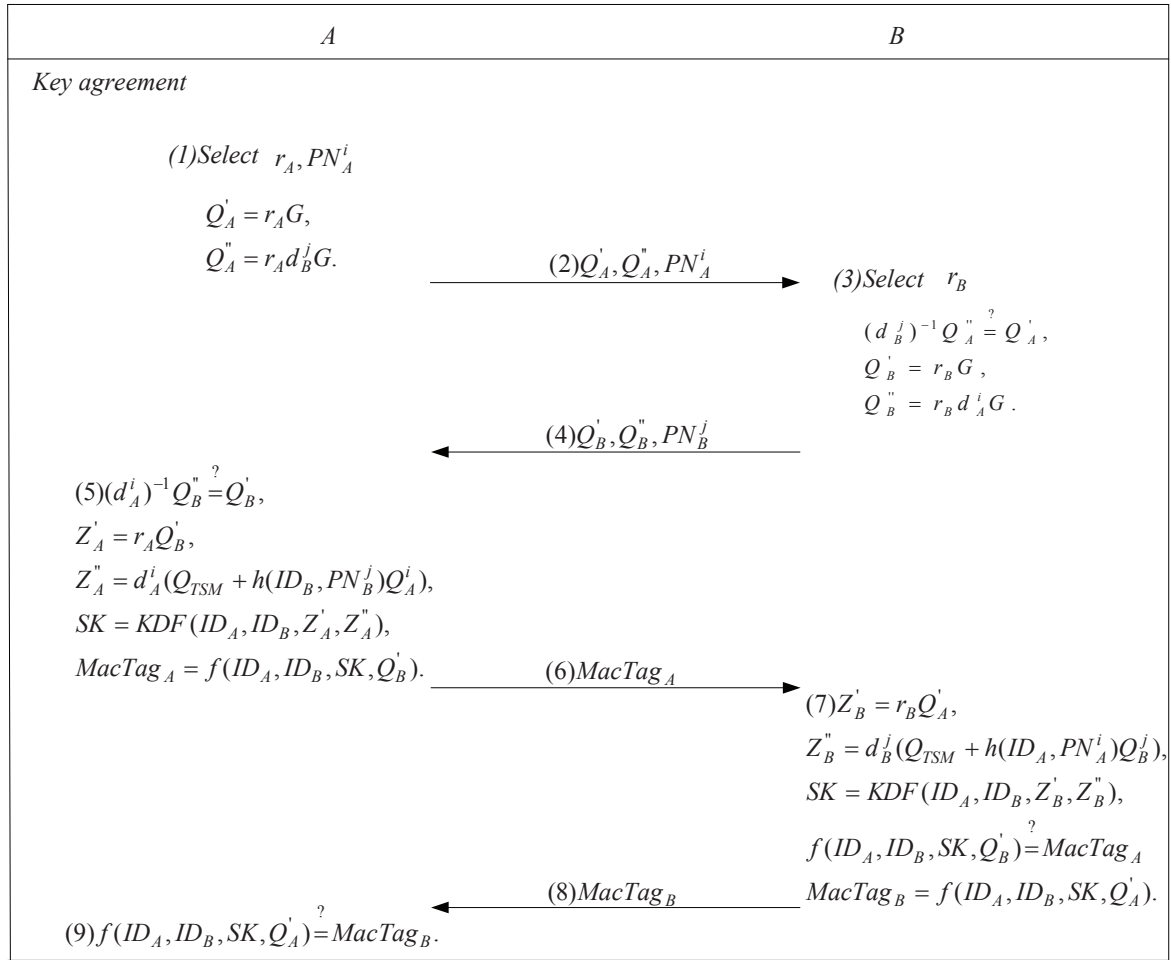


Figure 1: Mutual authentication and key agreement of our scheme

$f(ID_A, ID_B, SK, Q_{B(A)}')$, where SK is the session key, $Q_{B(A)}' = r_{B(A)} d_{A(B)}^{i(j)} G$, $r_{B(A)}$ and $d_{A(B)}^{i(j)}$ are the random numbers and the private keys. Therefore, ID_A is not able to be derived from Z_A'' without knowing the users' private key, owing to the one-way property of the hash function. Therefore, the proposed scheme preserves identity privacy.

5.2 Mutual Authentication

In the proposed scheme, A authenticates A by checking $Q_A' = (d_B^j)^{-1} Q_A''$ and $MacTag_A = f(ID_A, ID_B, SK, Q_B')$, where $SK = KDF(ID_A, ID_B, r_B Q_A', d_B^j d_A^i G)$. Additionally, A authenticates B by verifying whether $Q_B' = (d_A^i)^{-1} Q_B''$ and $MacTag_B = f(ID_A, ID_B, SK, Q_A')$, where $SK = KDF(ID_A, ID_B, r_A Q_B', d_A^i d_B^j G)$.

5.3 Perfect Forward Security of the Session Key

Given Q_A', Q_A'', Q_B', Q_B'' and $d_A^i d_B^j$, the session key $SK = KDF(ID_A, ID_B, r_A Q_B', d_A^i d_B^j G)$ cannot be cal-

culated without the knowledge of r_A and r_B , owing to the Diffie-Hellman problem. Additionally, given $MacTag_A = f(ID_A, ID_B, SK, Q_B')$ and $MacTag_B = f(ID_A, ID_B, SK, Q_A')$, SK cannot be determined due to the one-way property of the hash function and no knowledge of users' identities. Therefore, the session key cannot be derived from the revealed messages in the proposed scheme.

5.4 Known Session Key Security

In the proposed scheme, the session key is computed as $SK = KDF(ID_A, ID_B, r_A r_B G, d_A^i d_B^j G)$, which does not give any useful information for computing the next session keys because r_A and r_B are randomly generated in different runs and are independent of each other among scheme executions. Therefore, the proposed scheme has the property of known-key security.

5.5 Resistance to relay attack

Relay Attack is also popularly known as “man in the middle attack” in network security. An attacker acts as a middleman between two NFC devices to intercept the data

Table 2: Computational cost comparison

	Eun et al. [5]	He et al. [7]	The Proposal
A	$3T_{ecm} + 1T_{eca} + 2T_h + 2T_{mm} + 1T_{kdf}$ ≈ 0.6552	$4T_{ecm} + 1T_{eca} + 2T_h + 1T_{kdf}$ ≈ 0.2214	$4T_{ecm} + 1T_{mi} + 2T_h + 1T_{kdf}$ ≈ 0.2391
B	$3T_{ecm} + 1T_{eca} + 2T_h + 2T_{mm} + 1T_{kdf}$ ≈ 0.2583	$4T_{ecm} + 1T_{eca} + 3T_h + 1T_{kdf}$ ≈ 0.1845	$4T_{ecm} + 1T_{mi} + 2T_h + 1T_{kdf}$ ≈ 0.1107
Total	$6T_{ecm} + 2T_{eca} + 4T_h + 4T_{mm} + 2T_{kdf}$ ≈ 0.6921	$8T_{ecm} + 2T_{eca} + 5T_h + 2T_{kdf}$ ≈ 0.369	$8T_{ecm} + 2T_{mi} + 4T_h + 2T_{kdf}$ ≈ 0.3498

without the knowledge of the two NFC devices. The attacker either reads and records or manipulates the data before relaying it to the receiving device [18]. If an adversary intends to impersonate as a legal user to cheat A and B , he cannot accomplish his well as he wished. Because A and B each hold the data which is only verified by the other side, any forgery data will be detected by the receiver. Specifically, A sends $Z_A'' = d_A^i d_B^j G$ which is concealed in the session key and $Q_A'' = r_A d_B^j G$ to B , where $d_B^j G$ is a secret value of B . After verifying the correctness of the two values, B judges whether the sender is the real A . Similarly, A can also authenticate the validity of B by checking $Z_B'' = d_B^j d_A^i G$ and $Q_B'' = r_B d_A^i G$.

5.6 Resistance to Impersonation Attack

In the establishment of the session key, A transmits $Q_A'' = r_A d_B^j G$ to B , where d_B^j is the secret key of B , only B knows d_B^j . Others are impossible to know the value of $d_B^j G$ and cannot compute Z_A'' . Without the value of Z_A'' , an adversary cannot pass the authentication of B . Meanwhile, B also sends back the value $d_A^i G$ which is hidden in $Q_B'' = r_B d_A^i G$, where $d_A^i G$ is the secret information only known by of A and B , and only A knows d_A^i . That is, any unauthorized user cannot compute the correct Z_B'' and hence cannot be verified by A without the value of $d_A^i G$. In this way, the proposed scheme can withstand the impersonation attack.

5.7 No Key Control

In the proposed scheme, both A and B jointly compute the session key $SK = KDF(ID_A, ID_B, r_A r_B G, d_A^i d_B^j G)$ and therefore, A fails to predetermine a session key since SK contains r_B and d_B^j , where r_B and d_B^j are the secret values of B and independent among scheme executions. In other word, A or B cannot determine a session key alone and hence, the proposed scheme provides the no key control property.

5.8 Verification Using Scyther Tool

Scyther is a tool for the automatic verification of security protocols. In this part, we use Scyther-w32-v1.1.3 [4] to analyze the proposed scheme. Figure 1 shows a summary

of the claims in the proposed scheme. The verification result (Figuer 2) shows our scheme is correct.

6 Performance Comparisons

This section will evaluate the performance of the proposed scheme, and compare it with other related schemes [5, 7] for performance and functionality aspects. In order to facilitate the analysis of the performance, some notations was defined as below:

- T_{ecm} : the time consumption for an elliptic curve point multiplication operation;
- T_h : the time consumption for a hash function operation;
- T_{eca} : the time consumption for an elliptic curve point addition operation;
- T_{kdf} : the time consumption for a key derivation function operation;
- T_{mm} : the time consumption for a modular multiplication operation;
- T_{mi} : The time consumption for a modular inversion operation.

Generally, T_{mm} is far greater than T_{ecm} , T_{eca} and T_h . According to [1], under the environment of 2.2 GHz CPU and 2.0GB RAM, T_{ecm} and T_{eca} are 2.226 and 0.0288 ms, T_{mi} , T_{mm} and T_h are 5.565, 1.855 and 2.3 μs , respectively.

Table 2 demonstrates that the proposed scheme has less computational efficiency as compared with He et al. [7] but a slighter higher than Eun et al. [5] schemes, where the computational cost for executing the scheme once is only half of the time needed for other related scheme due to the proposed scheme needs more elliptic curve point multiplication computation than Eun et al.'s scheme, and employ modular inversion computation instead of elliptic curve point addition computation.

Table 3 shows the functionality analysis of the proposed scheme with Eun et al.'s [5] and He et al.'s [7] schemes. It is observed that the proposed scheme outperforms as compared to He et al.'s and Eun et al.'s schemes as the proposed scheme supports extra features listed in

```

hashfunction H;hashfunction KDF;

const Add: Function;const Mul: Function;

usertype String;const IDa, IDb: String;
protocol lu(A,B)
{
  role A{
    fresh Ra, G, PNa, PNb, Qtsm: Nonce;

    var Qa1, Qa2, Qb1, Qb2, Za1, Za2: Nonce;

    var SK, MacTaga, MacTagb: Nonce;

    match(Qa1,Mul(Ra, G));match(Qa2,Mul(Ra,pk(B)));

    send_!1(A,B,Qa1,Qa2,PNa);recv_!2(B,A,Qb1,Qb2,PNb);

    match(Za1,Mul(Ra,Qb1));match(Za2,{Add(Mul(H(IDb,PNb),Qa1),Qtsm)}sk(A));

    match(SK,KDF(IDa, IDb, Za1, Za2));

    match(MacTaga,H(IDa, IDb, SK, Qb1));send_!3(A,B,MacTaga);
    recv_!4(B,A,MacTagb);claim_A1(A,Secret,MacTaga);claim_A2(A,Secret,Qa1);

    claim_A3(A,Secret,Qa2);claim_A4(A,Secret,Qb1);

    claim_A5(A,Secret,Qb1);claim_A6(A,Alive);

    claim_A7(A,Weakagree);claim_A8(A,Niagree);

    claim_A9(A,Nisynch);}
  role B{
    fresh Rb, G, PNa, PNb, Qtsm: Nonce;

    var Qa1, Qa2, Qb1, Qb2, Zb1, Zb2: Nonce;

    var SK, MacTaga, MacTagb: Nonce;

    recv_!1(A,B,Qa1,Qa2,PNa);match(Qb1,Mul(Rb, G));

    match(Qb2,Mul(Rb,pk(A)));send_!2(B,A,Qb1,Qb2,PNb);

    recv_!3(A,B,MacTaga);match(Zb1,Mul(Rb,Qa1));

    match(Zb2,{Add(Mul(H(IDa,PNb),Qb1),Qtsm)}sk(B));

    match(SK,KDF(IDa, IDb, Zb1, Zb2));

    match(MacTagb,H(IDa, IDb, SK, Qa1));

    send_!4(B,A,MacTagb);claim_B1(B,Secret,MacTagb);

    claim_B2(B,Secret,Qa1);claim_B3(B,Secret,Qa2);

    claim_B4(B,Secret,Qb1);claim_B5(B,Secret,Qb1);

    claim_B6(B,Alive);claim_B7(B,Weakagree);

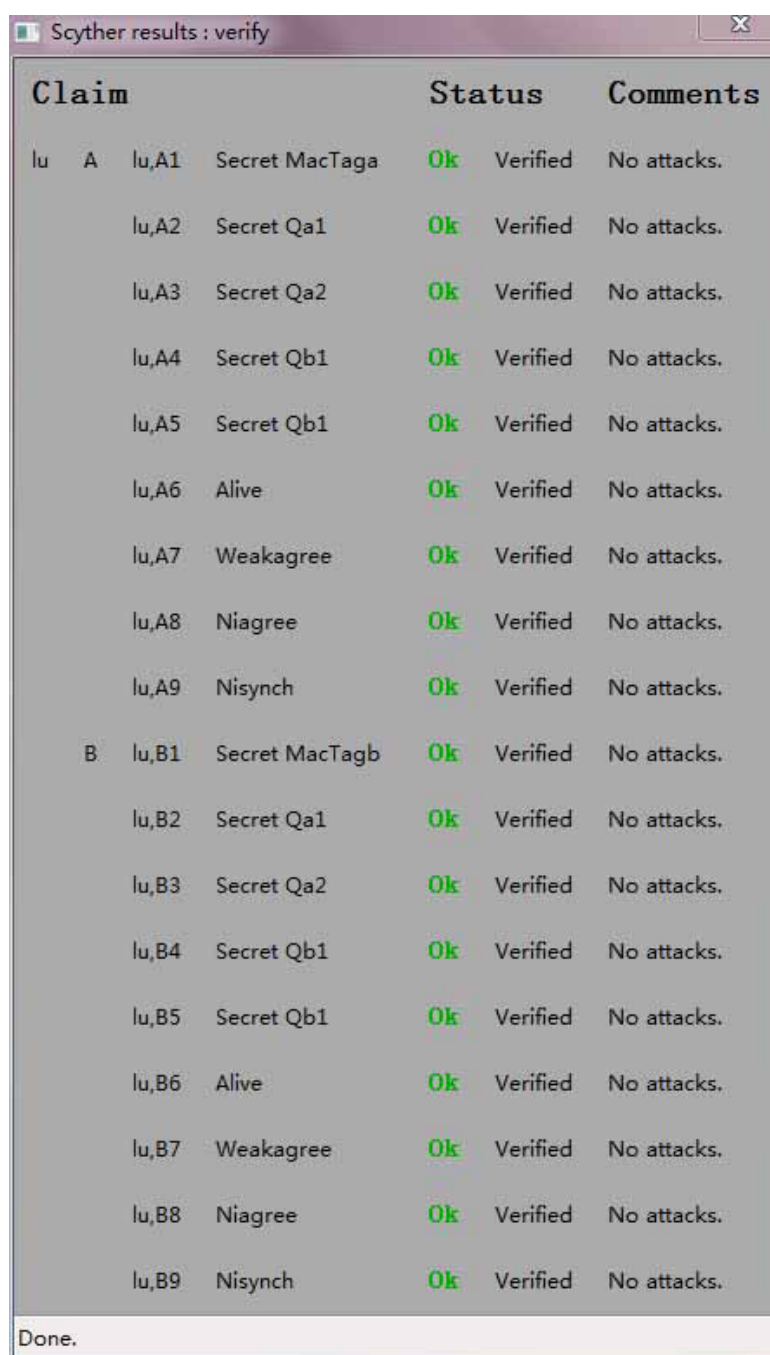
    claim_B8(B,Niagree);claim_B9(B,Nisynch);}}

```

Figure 2: The scheme description

Table 3: Comparison of functionality features

	Eun et al. [5]	He et al. [7]	The Proposal
Mutual authentication	Yes	Yes	Yes
User anonymity	Yes	Yes	Yes
No key control	Yes	Yes	Yes
Known session key security	Yes	Yes	Yes
Impersonation attack	No	Yes	Yes
Perfect forward security of the session key	-	-	Yes
Relay attack	-	No	Yes



Scyther results : verify

Claim				Status	Comments
lu	A	lu,A1	Secret MacTaga	Ok Verified	No attacks.
		lu,A2	Secret Qa1	Ok Verified	No attacks.
		lu,A3	Secret Qa2	Ok Verified	No attacks.
		lu,A4	Secret Qb1	Ok Verified	No attacks.
		lu,A5	Secret Qb1	Ok Verified	No attacks.
		lu,A6	Alive	Ok Verified	No attacks.
		lu,A7	Weakagree	Ok Verified	No attacks.
		lu,A8	Niagree	Ok Verified	No attacks.
		lu,A9	Nisynch	Ok Verified	No attacks.
	B	lu,B1	Secret MacTagb	Ok Verified	No attacks.
		lu,B2	Secret Qa1	Ok Verified	No attacks.
		lu,B3	Secret Qa2	Ok Verified	No attacks.
		lu,B4	Secret Qb1	Ok Verified	No attacks.
		lu,B5	Secret Qb1	Ok Verified	No attacks.
		lu,B6	Alive	Ok Verified	No attacks.
		lu,B7	Weakagree	Ok Verified	No attacks.
		lu,B8	Niagree	Ok Verified	No attacks.
		lu,B9	Nisynch	Ok Verified	No attacks.

Done.

Figure 3: Test result.

this table and is also more secure than He et al.'s scheme. As a result, the proposed scheme is much suitable for practical applications as compared to the recently proposed He et al.'s scheme.

7 Conclusion

This paper have investigated the NFC communications-based mutual authentication scheme presented by He et al.. By cryptanalyzing studies, a fatal security weakness in He et al.'s scheme have been found. In order to remedy this flaw, an enhancement based on He et al.'s scheme

have been presented. Based on the security analysis, the proposed scheme has been demonstrated to be satisfied both the verifiability and privacy of attributes. According to the performance comparison results, the efficiency and feasibility of the proposed scheme under different privacy requirements for the IOT have been shown.

References

- [1] H. Arshad, and M. Nikooghadam, "An efficient and secure authentication and key agreement scheme for ses-

- sion initiation protocol using ECC,” *Multimedia Tools and Applications*, vol. 75, no. 1, pp. 181–197, 2016.
- [2] G. Broll, S. Siorpaes, E. Rukzio, M. Paolucci, J. Hamard, M. Wagner and A. Schmidt, “Supporting mobile service usage through physical mobile interaction,” in *5th Annual IEEE International Conference on Pervasive Computing and Communications*, White Plains, NY, USA. 2007.
 - [3] V. Coskun, K. Ok, and B. Ozdenizci, *Near Field Communication (NFC): From Theory to Practice*, London, Wiley, February, 2012.
 - [4] C. Cremers, *The Scyther Tool*, Apr. 4, 2014. (<https://www.cs.ox.ac.uk/people/cas.cremers/scyther/>)
 - [5] H. Eun, H. Lee, and H. Oh, “Conditional privacy preserving security protocol for NFC applications,” *IEEE Transaction on Consumer Electronics*, vol. 59, no. 1, pp. 153–160, 2013.
 - [6] E. Hasoo, L. Hoonjung, S. Junggab, K. Sangjin, and O. Heekuck, “Conditional privacy preserving security protocol for NFC applications,” in *IEEE International Conference on Consumer Electronics*, pp.380–381, 2012.
 - [7] D. He, N. Kumar, and J. H. Lee, “Secure pseudonym-based near field communication protocol for the consumer internet of things,” *IEEE Transactions on Consumer Electronics*, vol. 61, no. 1, pp. 56–62, 2015.
 - [8] ISO/IEC, *Information Technology-Security Methods-Cryptographic Methods Based on Elliptic Curves - Part 1: General*, ISO/IEC 15946-1, Apr. 2008.
 - [9] ISO/IEC, *Information Technology Telecommunications and Information Exchange Between Systems-NFC Security - Part 1: NFC-SEC NFCIP-1 Security Service and Protocol*, ISO/IEC 13157-1: 2010, May 2010.
 - [10] ISO/IEC, *Information Technology Telecommunications and Information Exchange Between Systems-NFC Security - Part 2: NFC-SEC Cryptography Standard Using ECDH and AES*, ISO/IEC 13157-2: 2010, May 2010.
 - [11] P. Kumar, A. Gurtov, J. Iinatti, and S. G. Lee, “Delegation-based robust authentication model for wireless roaming using portable communication devices,” *IEEE Transaction on Consumer Electronics*, vol. 60, no.4, pp. 668–674, 2014.
 - [12] Y. Lu, X. Wu, X. Yang, “A secure anonymous authentication scheme for wireless communications using smart cards,” *International Journal of Network Security*, vol. 17, no. 3, pp. 237–245, 2015.
 - [13] W. Lumpkins, and M. Joyce, “Near-field communication: It pays: Mobile payment systems explained and explored,” *IEEE Consumer Electronics Magazine*, vol. 4, no. 2, pp. 49–53, 2015.
 - [14] G. Madlmayr, J. Langer, and C. Kantner, “NFC devices: Security and privacy,” in *3th Annual IEEE International Conference on Availability, Reliability and Security*, pp. 642–647, 2008.
 - [15] A. Matos, D. Romao, and P. Trezentos, “Secure hotspot authentication through a near field communication side-channel,” in *2012 IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications*, pp. 807–814, Oct. 2012.
 - [16] K. F. Warnick, R. B. Gottula, S. Shrestha, and J. Smith, “Optimizing power transfer efficiency and bandwidth for near field communication systems,” *IEEE Transaction on Antennas and Propagation*, vol. 61, no. 2, pp. 927–933, 2013.
 - [17] T. Sunil, B. Rabin, and M. Sangman, “NFC and its application to mobile payment: Overview and comparison,” in *2012 8th IEEE International Conference on Information Science and Digital Content Technology*, pp. 203–206, 2012.
 - [18] C. Thammarat, R. Chokngamwong, C. Techapanupreeda, and S. Kungpisdan, “A secure lightweight protocol for NFC communications with mutual authentication based on limited-use of session keys,” in *Proceedings of 2015 IEEE International Conference on Information Networking*, pp. 133–138, 2015.

Biography

Yan-Na Ma received the B.S. degree in electrical engineering from Dalian University (DUT) of Technology, Dalian, China, in 2009 and the M.S. and Ph.D. degree in communications and integrated system from Tokyo Institute of Technology, Tokyo, Japan, in 2011 and 2014, respectively. Currently, she is a faculty member with School of Information Engineering and Art Design, Zhejiang University of Water Resources and Electric Power, China. Her research interests are speech signal processing, noise reduction, near field communication and their applications to communication devices.

Security on a Knapsack-Type Encryption Scheme Based upon Hybrid-Model Assumption

Zhengping Jin¹, Hong Zhang², and Zhongxian Li³

(Corresponding author: Zhengping Jin)

State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications¹
Beijing 100876, China

National Computer Network Emergency Response Technical Team Coordination Center of China²
Beijing 100029, China

National Cybernet Security Limited, Tianjin 300384, China³
(Email: zhpjin@bupt.edu.cn)

(Received Apr. 17, 2016; revised and accepted June 16 & July 19, 2016)

Abstract

Provable security is a reduction that breaking the scheme is usually reduced to solving some basic hard problems, thus the foundation of the scheme's security is the assumption that it is hard to solve the based problems. Due to most existing schemes are founded on single assumption, some encryption schemes, whose security are based on multiple assumptions, have been proposed. Recently, Su and Tsai constructed a knapsack-type encryption scheme based on hybrid-model, and proved it should be more secure than schemes based on single assumption. In this paper, we find that this scheme actually cannot reach the security as claimed. By launching the known message attack, we show Su and Tsai's encryption scheme cannot provide confidentiality, for the adversary could decrypt any ciphertext in this cryptosystem if one of the assumptions does not hold.

Keywords: Confidentiality; Hybrid Problems; Knapsack Cryptosystem; Provable Security

1 Introduction

Provable security was first introduced by Goldwasser and Micali [4] in the particular context of asymmetric encryption. Its main idea comes from proofs by contradiction in Mathematics, which is a reduction as follows [14]. At first, take some goal for a scheme, such as achieving privacy via encryption. Then, make a formal adversarial model according to the adversary's ability, and define what it means for a scheme to be secure.

With this in hand, a particular scheme, based on some particular atomic primitive, can be analyzed from the point of view of meeting the definition. Eventually, one shows that the scheme works via a reduction. The reduction shows that the only way to defeat the scheme is to

break the underlying atomic primitive [1, 7]. Therefore, the atomic primitive, which may be some basic mathematical problem, is the foundation of the security for intended scheme.

Since the concept of provable security was proposed, a large number of works have been made, including many delicate encryption designed and proved in formal security model [6, 8]. However, the security of most existing schemes is founded on just one cryptographic assumption, such as factoring, discrete logarithm (DL) problem [11], elliptic curve discrete logarithm problem (ECDLP) [12], etc. Though these assumptions appear reliable now, it is possible that efficient algorithms will be sooner or later developed to break one or more of them. It is unlikely that multiple cryptographic assumptions would simultaneously become easy to be solved. Thus, several cryptographic systems' security is reduced to solving multiple hard problems at the same time.

In 1994, Harn [5] first developed a public key cryptosystem based on multiple cryptographic assumptions, intractability of factoring [3] and DL problems [10]. Recently, Su and Tsai [13] presented an encryption scheme based on the linearly shift knapsack and elliptic curve cryptosystem, and claimed that it is secure based on the hardness of the linearly shifting knapsack problem and ECDLP, for one possible hope to break the proposed system might be to solve both of the problems.

In this paper, we cryptanalyze Su and Tsai's knapsack-type encryption scheme, and find it is not really secure as claimed. Concretely, with one pair of message and ciphertext in hands, the adversary could decrypt any ciphertext in this cryptosystem, if one of the assumptions, i.e. the linearly shifting knapsack problem is hard, does not hold, which consequently breaks its security based on multiple assumptions.

The rest of this paper is organized as follows. Some

preliminary works are given in Section 2. Then, Su and Tsai's knapsack-type encryption scheme is recalled and our attack on its security is described in Section 3. Finally, some conclusions are drawn in Section 4.

2 Preliminaries

In this section, we briefly review some basic concepts used in this paper, including bilinear pairings, the knapsack problem, the linearly shift knapsack algorithm and the computational knapsack Diffie-Hellman problem.

2.1 Bilinear Pairings

Let \mathbb{G} and \mathbb{G}_T be groups of prime order q and P be a generator of \mathbb{G} . The map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is said to be an admissible bilinear pairing if the following three conditions hold true:

- 1) Bilinearity: for all $a, b \in \mathbb{Z}_q$, we have $e(aP, bP) = e(P, P)^{ab}$.
- 2) Non-degeneracy: $e(P, P) \neq 1_{\mathbb{G}_T}$.
- 3) Computability: e is efficiently computable.

It is noted that the map e is symmetric since $e(aP, bP) = e(P, P)^{ab} = e(bP, aP)$ and we refer reader to [2] for more details on the construction of such pairings.

2.2 Knapsack Problem

The knapsack problem is a typical problem of combinatorial optimization, and 0/1 knapsack problem is one of the most basic cases, which is presented as follows [13].

- Problem instance:
 $K = (k_1, k_2, \dots, k_n, t)$, where k_1, k_2, \dots, k_n and t are positive integers. k_1, k_2, \dots, k_n are called sizes and t is called the target sum.

- Question:
Is there a 0-1 vector $S = (x_1, x_2, \dots, x_n)$ such that $\sum_{i=1}^n x_i k_i = t$?

It is easy to solve the knapsack problem when (k_1, k_2, \dots, k_n) is a superincreasing sequence, in which the next term of the sequence is greater than the sum of all preceding terms. However, it is assumed that the knapsack problem for the general case cannot be solved in probabilistic polynomial time (PPT).

2.3 Linearly Shift Knapsack Cryptosystem

Based on Lai et al's method [9], Su and Tsai [13] proposed the high density knapsack algorithm and the linearly shift knapsack algorithm described as follows, which are used to generate the system parameters of their encryption scheme.

- High density knapsack algorithm:

Step 1: Let $\bar{a} = (a_1, a_2, \dots, a_n)$ be a superincreasing sequence, and select two integers w, m satisfying $\gcd(w, m) = 1$, where $m > \sum_{i=1}^n a_i$.

Step 2: Calculate the original enciphering keys $b_i \equiv a_i \times w \pmod{m}$ for all i .

Step 3: Compute the high density sequence $\bar{b}' = (b'_1, b'_2, \dots, b'_n)$, where $b'_i \equiv b_i \pmod{w}$, then $b'_i < w$ for all i .

Step 4: Calculate $\bar{c} = (c_1, c_2, \dots, c_n)$, where $c_i = \lfloor b_i/w \rfloor$, then $0 \leq c_i \leq v$, and compute the deciphering keys $a'_i = a_i - c_i$, where $v = \lfloor m/w \rfloor$ (here $\lfloor x \rfloor$ is a floor function, representing the largest integer value smaller than x).

- Linearly shift knapsack algorithm:

Step 5: As high density knapsack algorithm, calculate a high density knapsack sequence $\bar{b}' = (b'_1, b'_2, \dots, b'_n)$.

Step 6: Choose a random binary sequence $\bar{t} = (t_1, t_2, \dots, t_n)$, and an integer k with $0 < k < \min\{b'_i\}$ for $t_i = 1$. Then b'_i are linearly shifted by performing $e_i = b'_i - kt_i$ and $\bar{e} = (e_1, e_2, \dots, e_n)$ which is published as the public enciphering key.

3 Chosen Plaintext Attack on Su and Tsai's Encryption Scheme

To analyze the security of Su and Tsai's encryption scheme [13], we first recall their descriptions as follows.

System setup:

The receiver Alice selects the domain parameters which are comprised of:

- The field order q .
- Two coefficients $a, b \in F_q$ that define the equation of the elliptic curve E over F_q .
- The number of points in $E(F_q)$, denoted as $\#E(F_q)$.
- Two field elements x_P and y_P in F_q that define a finite point $P = (x_P, y_P)$. P has a prime order q' and is called the base point.
- A one-way hash function $f(\cdot)$.
- Parameters (w, m, k, r_A, \bar{a}) as his private keys, where $m < q', r_A \in \mathbb{Z}_q^*$.
- A random binary sequence \bar{t} .
- Public keys $\bar{e} = (e_1, e_2, \dots, e_n)$ and $Q_A = r_A P$.

Encryption:

To encrypt the message \bar{x} to Alice, Bob picks up his secret key r_B , publishes his public key $Q_B = r_B P$ and computes the ciphertext pair message \bar{x} using Alice's public keys $\bar{e} = (e_1, e_2, \dots, e_n)$ and Q_A . The encryption phase is as follows:

- Bob encodes the plaintext message

$$\bar{x} = (x_1, \dots, x_n),$$

where $x_i = 0$ or 1 , for $i = 1, 2, \dots, n$.

- Produces the ciphertext

$$E(\bar{x}) = ((k_1, k_2) + r_B Q_A),$$

where $k_1 = \sum_{i=1}^n x_i e_i$, $k_2 = f(Q_A, Q_B)$.

- Sends $E(\bar{x}) = ((k_1, k_2) + r_B Q_A)$ to Alice.

Decryption:

To receive the ciphertext $E(\bar{x})$, Alice computes with his secret key r_A and Bob's public information Q_B . To decrypt the knapsack value, Alice multiplies the Bob's public point using his secret key r_A and subtracts the result from $E(\bar{x})$:

$$D(E(\bar{x})) = (k_1, k_2) + r_B Q_A - r_A Q_B.$$

Before computing the knapsack value, Alice needs to verify whether k_2 is sent from Bob by checking $k_2 \stackrel{?}{=} f(Q_A, Q_B)$ and computing k_1 which should be the plaintext point, corresponding to the message bit is 1.

Once Alice, knowing the private key w^{-1} , can remove $k_1 = \sum_{i=1}^n x_i e_i$ from the ciphertext, and hence retrieve the plaintext information \bar{x} :

Since

$$\begin{aligned} s \times w^{-1} &\equiv \left(\sum_{i=1}^n b'_i x_i \right) \times w^{-1} \pmod{m} \\ &\equiv \sum_{i=1}^n (e_i + k t_i) x_i \times w^{-1} \\ &\equiv k_1 \times w^{-1} + k w^{-1} \times \sum_{i=1}^n t_i x_i \pmod{m} \end{aligned}$$

and $0 \leq \sum_{i=1}^n t_i x_i \leq \sum_{i=1}^n t_i \leq n$, Alice can obtain the correct $s \times w^{-1} \pmod{m}$ at most $y + 1 \leq n + 1$ times and get \bar{x} from $s \times w^{-1}$ by his superincreasing sequence $\bar{a} = (a_1, a_2, \dots, a_n)$, for $s \times w^{-1} = \sum_{i=1}^n a_i x_i$. The correctness can be easily verified through normal enciphering procedures with the corresponding retrieved \bar{x} by checking $\sum_{i=1}^n x_i e_i \stackrel{?}{=} k_1$, as it is assumed that the system is one-to-one.

Su and Tsai [13] heuristically analyzed the security of their encryption scheme, and claimed that, one possible

hope to break their cryptosystem might be to solve the linearly shifting knapsack problem and the elliptic curve cryptography system simultaneously, which is computationally infeasible for the opponents.

However, we will show that, if one adversary could only solve the linearly shifting knapsack problem but not the ECDLP, it might endanger the security of their scheme, which means it's not really secure based on hybrid-model assumption. Su and Tsai [13] defined the security of a cryptosystem that is evaluated by the amount of time needed to break it, where breaking a cryptosystem means finding the private key used to encrypt a message. However, it is also a fatal destruction for some flawed encryption schemes that any adversary can obtain the plaintext or parts of plaintext from ciphertext without the help of the private key. So what is a secure encryption scheme? It is not an easy question to answer. In fact, a widely accepted security property for encryption is the ciphertext indistinguishability [8], which is very important for maintaining the confidentiality of encrypted communications. Intuitively, if a cryptosystem possesses the property of indistinguishability, then an adversary will be unable to distinguish pairs of ciphertexts based on the message they encrypt. Furthermore, according to the adversary's capability, the security property for encryption can be divided into indistinguishability under chosen plaintext attack (IND-CPA), chosen ciphertext attack (IND-CCA1) and adaptive chosen ciphertext attack (IND-CCA2). IND-CPA is considered a basic requirement for most provably secure public key cryptosystems, though some schemes also provide stronger security that are IND-CCA1 and IND-CCA2. In the following, we show that Su and Tsai's scheme cannot provide the property of IND-CPA, to say nothing of IND-CCA1 or IND-CCA2. More exactly, with an assumed algorithm that can solve the linearly shifting knapsack problem, the adversary can decrypt any ciphertext from Bob to Alice if he successfully gets a corresponding ciphertext to his chosen message, which contradicts Su and Tsai's claim.

Once the adversary got the ciphertext for some message $\bar{x} = (x_1, \dots, x_n)$, denoted as σ , he could calculate

$$r_B Q_A = \sigma - (k_1, k_2),$$

where $k_1 = \sum_{i=1}^n x_i e_i$, $k_2 = f(Q_A, Q_B)$. Then, for arbitrary ciphertext σ^* from Bob to Alice, the adversary could compute

$$D(E(\bar{x}^*)) = \sigma^* - r_B Q_A = (k_1^*, k_2^*)$$

without any part of Alice or Bob's secret key r_A or r_B , where $\bar{x}^* = (x_1^*, \dots, x_n^*)$ is the intended plaintext and $k_1^* = \sum_{i=1}^n x_i^* e_i$ is its corresponding knapsack sum. Consequently, the adversary could get the plaintext \bar{x}^* from k_1^* according to the assumed algorithm of solving the linearly shifting knapsack problem.

During the whole attacking process above, no algorithm concerning the ECDLP is needed, but the value

related to Alice's secret key r_A is leaked in a sense. Therefore, their proposal is actually not a secure encryption scheme that couldn't be broken unless the linearly shifting knapsack problem and the ECDLP were solved simultaneously. In other words, its security is only based on the hardness of the linearly shifting knapsack problem.

4 Conclusions

We have made the cryptanalysis of Su and Tsai's knapsack-type encryption scheme based on hybrid-model problems, and launched a chosen plaintext attack to show it does not satisfy the enhanced security depends on the computational complexity of multiple assumptions. Therefore, to the best of our knowledge, it remains on its way to construct really secure encryption scheme based on hybrid-model problems.

Acknowledgments

This work is supported by NSFC (Grant Nos. 61502044, 61300181), the Fundamental Research Funds for the Central Universities (Grant No. 2015RC23).

References

- [1] M. Bellare, "Practice-oriented provable-security," *Lectures on Data Security*, vol. 1561 of LNCS, pp. 1–15, 2003.
- [2] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology (Crypto'01)*, vol. 2139 of LNCS, pp. 213–229, Springer-Verlag, Berlin, 2001.
- [3] C. C. Chang, M. S. Hwang, "Parallel computation of the generating keys for RSA cryptosystems," *Electronics Letters*, vol. 32, no.15, pp. 1365–1366, 1996.
- [4] S. Goldwasser and S. Micali, "Probabilistic encryption," *Journal of Computer and System*, vol. 28, no. 2, pp. 270–299, 1984.
- [5] L. Harn, "Public-key cryptosystem design based on factoring and discrete logarithms," *IEE Proceedings - Computers and Digital Techniques*, vol. 141, pp. 193–195, 1994.
- [6] Z. P. Jin, Q. Y. Wen, and H. Z. Du, "An improved semantically-secure identity-based signcryption scheme in the standard model," *Computers & Electrical Engineering*, vol. 36, no. 3, pp. 545–552, 2010.
- [7] A. Kartit, H. K. Idrissi, and M. Belkhouraf, "Improved methods and principles for designing and analyzing security protocols," *International Journal of Network Security*, vol. 18, no. 3, pp. 523–528, 2016.
- [8] J. Katz and Y. Lindell, *Introduction to Modern Cryptography: Principles and Protocols*, Chapman & Hall/CRC, 2007.

- [9] C. S. Lai, J. Y. Lee, L. Harn, and Y. K. Su, "Linearly shift knapsack public-key cryptosystem," *IEEE Journal of Selected Areas in Communications*, vol. 7, no. 4, pp. 534–539, 1989.
- [10] C. C. Lee, M. S. Hwang, L. H. Li, "A new key authentication scheme based on discrete logarithms," *Applied Mathematics and Computation*, vol. 139, no. 2, pp. 343–349, 2003.
- [11] L. H. Li, S. F. Tzeng, M. S. Hwang, "Generalization of proxy signature-based on discrete logarithms," *Computers & Security*, vol. 22, no. 3, pp. 245–255, 2003.
- [12] L. Liu and Z. Cao, "A note on efficient algorithms for secure outsourcing of bilinear pairings," *International Journal of Electronics and Information Engineering*, vol. 5, no. 1, pp. 30–36, 2016.
- [13] P. C. Su and C. H. Tsai, "New cryptosystems design based on hybrid-mode problems," *Computers & Electrical Engineering*, vol. 35, no. 3, pp. 478–484, 2009.
- [14] Y. Zhang, H. Li, X. Li, and H. Zhu, "Subliminal-free Variant of Schnorr Signature with Provable Security," *International Journal of Electronics and Information Engineering*, vol. 3, no. 1, pp. 19–30, 2015.

Biography

Zhengping Jin, received his B.S. degree in Mathematics and Applied Mathematics and his M.S. degree in Applied Mathematics from Anhui Normal University, Wuhu, Anhui, China, in 2004 and 2007, respectively, and his Ph.D. degree in Cryptography from Beijing University of Posts and Telecommunications, Beijing, China, in 2010. Currently, he is an associate professor in the State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications. His research interests include design and analysis of cryptographic protocols, and security in cloud computing.

Hong Zhang, received his B.S. degree in Automatic Control and his M.S. degree in System Engineering from Xian Jiaotong University, Xian, Shaanxi, China, in 1998 and 2001, respectively, and his Ph.D. degree in Computer Network from Institute of Computing Technology, Chinese Academy of Science, Beijing, China, in 2004. Currently, he is a senior engineer in CNCERT/CC. His research interests include cloud computing, software engineering and network security.

Zhongxian Li, received his B.S. degree in Mathematics and his M.S. degree in Number Theory from Zhengzhou University in 1984 and 1987, respectively, and his Ph.D. degree in Signal and Information Processing from Beijing University of Posts and Telecommunications, Beijing, China, in 1999. Currently, his research interests include network and information security, virtual desktop and security in cloud computing.

Comments on a Secure Authentication Scheme for IoT and Cloud Servers

Wei-Liang Tai¹ and Ya-Fen Chang²

(Corresponding author: Ya-Fen Chang)

Department of Information Communications, Chinese Culture University¹

55, Hwa-Kang Road, Yang-Ming-Shan, Taipei, Taiwan

Department of Computer Science and Information Engineering, National Taichung University of Science and Technology²

No. 129, Sec. 3, Sanmin Rd., North Dist., Taichung, Taiwan

(Email: cyf@nutc.edu.tw)

(Received May 22, 2016; revised and accepted Aug. 5 & Sept. 2, 2016)

Abstract

Recently, Kalra and Sood proposed an authentication scheme based on Elliptic Curve Cryptography (ECC) to have embedded devices and cloud servers communicate securely using HTTP cookies. After analyzing their scheme, it is found that there are five issues that are not properly addressed. In this paper, the details and further discussions are given.

Keywords: Cloud Computing; ECC; Elliptic Curve Cryptography; IoT

1 Introduction

In 2015, Kalra and Sood proposed an ECC-based authentication scheme [7]. They claimed that their scheme could ensure the security of communications between embedded devices and cloud servers. In their scheme, HTTP cookies are used for mutual authentication, and a session key will be negotiated by the embedded device and the cloud server to protect communications. This technique makes Kalra and Sood's authentication scheme different from other authentication schemes [1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 12].

However, after analyzing Kalra and Sood's scheme, it is found that there are five issues that are not properly addressed.

- 1) An embedded system is a machine instead of a real person. Allowing an embedded system to register at the cloud server might damage the cloud server.
- 2) An embedded system cannot be authenticated by the cloud server because an important parameter is not issued by the cloud server.
- 3) Some computational operations do not comply with the definitions of ECC.

- 4) The session key can be computed by neither the embedded device nor the cloud server.
- 5) When updating or setting a cookie, the request is not verified.

Because of the above five issues, Kalra and Sood's authentication scheme cannot ensure the security of communications between embedded devices and cloud servers as claimed. The rest of this paper is organized as follows. Section 2 briefly reviews Kalra and Sood's authentication scheme for IoT and cloud servers. Section 3 implicitly shows the found issues and makes further discussions. Some conclusions are drawn in Section 4.

2 Review of Kalra and Sood's Authentication Scheme for IoT and Cloud Servers

Kalra and Sood's authentication scheme is composed of three phases, registration phase, pre-computation and login phase, and authentication phase. The notations used in Kalra and Sood's scheme are listed in Table 1. Before all phases, the cloud server S chooses an elliptic curve equation $y^2 = x^3 + ax + b$ in Z_p , where $a, b \in Z_p$ and $4a^3 + 27b^2 \bmod p \neq 0$. The order of this elliptic curve is a prime n , where $n > 2^{160}$, and O is an infinite point such that $n \times G = O$. And, the server S chooses X as its private key. The details are as follows.

2.1 Registration Phase

When a new embedded device D_i wants to access S , it needs to register at S at first. The details of this phase are as follows:

Step 1: D_i sends its unique identity ID_i to S as a registration request.

Table 1: Notations used in Kalra and Sood's authentication scheme

Symbol	Definition
D_i	An embedded device
S	The cloud server
ID_i	D_i 's identity
P_i	D_i 's password
R_i	A random number generated by S for D_i
N_1, N_2	Random numbers generated for ECC
$H()$	One-way hash function
X	S 's private key
Z_p	A finite field
p	A prime greater than 2^{160}
G	A generator point of prime order n
CK	Cookie
EXP_TIME	CK 's expiration time
\parallel	A concatenation operator
\oplus	An XOR operator

Step 2: After getting the registration request, S generates D_i 's dedicated password P_i and a unique random number R_i . S computes cookie $CK = H(R_i \parallel X \parallel \text{EXP_TIME} \parallel ID_i)$, $CK' = CK \times G$, $T_i = R_i \oplus H(X)$, and $A_i = H(R_i \oplus H(X) \oplus P_i \oplus CK')$, where CK' is an ECC point and is stored in D_i as the cookie information. Then, S stores ID_i , $A_i' = A_i \times G$, T_i , and the cookie expiration time EXP_TIME for D_i . When the cookie expires, the expiration time will be updated to EXP_TIME', and the cookie CK will be updated to $H(R_i \parallel X \parallel \text{EXP_TIME}' \parallel ID_i)$.

Step 3: S sends CK' to D_i .

2.2 Pre-computation and Login Phase

Step 1: Before each login, D_i chooses a random number N_1 , computes the corresponding ECC point $P_1 = N_1 \times G$, and stores the information in its memory.

Step 2: When D_i wants to login to S , D_i computes $P_2 = H(N_1 \times CK')$ and sends $\{P_1, P_2, ID_i\}$ to S .

2.3 Authentication Phase

After getting D_i 's login request $\{P_1, P_2, ID_i\}$, authentication phase is executed as follows:

Step 1: S computes $R_i = T_i \oplus H(X)$, $CK = H(R_i \parallel X \parallel \text{EXP_TIME} \parallel ID_i)$, and $P_2' = H(P_1 \times CK)$. Then S checks whether P_2 and P_2' are equal or not. If they are equal, this phase proceeds.

Step 2: S chooses a random number N_2 and computes $P_3 = N_2 \times G$ and $P_4 = N_2 \times A_i'$. Then S sends $\{P_3, P_4, T_i\}$ to D_i .

Step 3: After receiving $\{P_3, P_4, T_i\}$, D_i computes $A_i = H(T_i \oplus P_i \oplus CK')$ and $P_4' = P_3 \times A_i$. Then D_i checks whether P_4 and P_4' are equal or not. If they are equal, this phase proceeds.

Step 4: D_i computes $V_i = H((N_1 \times CK') \parallel P_4')$ and sends $\{V_i\}$ to S .

Step 5: After receiving $\{V_i\}$, S computes $V_i' = H((P_1 \times CK) \parallel P_4)$ and checks whether V_i and V_i' are equal or not. If they are equal, D_i and S authenticate each other successfully, and they can obtain the session key $SK = H(X \parallel ID_i \parallel N_1 \parallel N_2)$.

3 The Found Five Issues and Further Discussions

In this section, the details of the found issues are given, and further discussions are made.

3.1 The Found Issues

After analyzing Kalra and Sood's authentication scheme, it is found that it cannot ensure the security of communications between embedded devices and cloud servers as claimed because of the following five issues.

Issue 1: An embedded system is a machine instead of a real person. Allowing an embedded system to register at the cloud server might damage the cloud server.

When allowing an embedded system to register at a server, it denotes that a machine even a robot can register at will. An attacker can easily mount a DoS (denial-of-service) attack by registering at the server with plenty of distinct device identities to get a number of cookies and accessing the cloud server with these registered identities to consume the system resources.

Issue 2: An embedded system cannot be authenticated by the cloud server because an important parameter is not issued by the cloud server.

In registration phase, after the cloud server gets D_i 's registration request, S generates a dedicated password P_i and a unique random number R_i for D_i . Then S computes the corresponding parameters CK, CK', T_i, A_i , and A_i' , and S sends CK' to D_i . In authentication phase, D_i needs to compute $A_i = H(T_i \oplus P_i \oplus CK')$ and $P_4' = P_3 \times A_i$ to authenticate the cloud server S , and D_i needs to compute $V_i = H((N_1 \times CK') \parallel P_4')$ to have S authenticate it. However, D_i does not know P_i because P_i is chosen by S and is not issued to D_i in registration phase. That is, D_i is not capable of computing A_i, P_4' , and V_i , and the embedded system D_i will never be authenticated successfully.

Issue 3: Some computational operations do not comply with the definitions of ECC.

In ECC, a multiplication operation is defined as $B = \alpha \times Q$, where Q and B are ECC points and α is an integer. In Kalra and Sood's scheme, computing $P'_2 = H(P_1 \times CK)$, $P'_4 = P_3 \times A_i$, and $V'_i = H((P_1 \times CK) \parallel P_4)$ violates the definitions of ECC.

Issue 4: The session key can be computed by neither the embedded device nor the cloud server.

In Kalra and Sood's scheme, a session key $SK = H(X \parallel ID_i \parallel N_1 \parallel N_2)$ is negotiated after mutual authentication. According to Elliptic Curve Discrete Logarithm Problem (ECDLP), it is computationally infeasible to retrieve α when Q and B are known, where $B = \alpha \times Q$, Q and B are ECC points and α is an integer. Consequently, D_i only knows the random number N_1 generated by itself because it cannot retrieve N_2 from P_3 , and S only knows the random number N_2 generated by itself because it cannot retrieve N_1 from P_1 , where $P_3 = N_2 \times G$ and $P_1 = N_1 \times G$. Moreover, only S knows the private key X . That is, it is impossible for both D_i and S to obtain the session key $SK = H(X \parallel ID_i \parallel N_1 \parallel N_2)$.

Issue 5: When updating or setting a cookie, the request is not verified.

Kalra and Sood's scheme uses HTTP cookies for mutual authentication. But updating or setting a cookie is not verified such that an attacker can maliciously modify the cookie stored in the embedded device D_i to make it unable to be authenticated.

3.2 Further Discussions

To remedy the found issues, some modifications should be made. First, a user instead of an embedded device can register at the cloud server to prevent an attacker from registering at the server with distinct device identities and consuming the system resources. Second, no matter who chooses the password P_i , both the embedded device D_i and the cloud server S need to know P_i , and the party choosing P_i should transmit P_i to the other via a secure channel. Third, P'_2, P'_4 , and V'_i should be computed as $P'_2 = H(CK \times P_1)$, $P'_4 = A_i \times P_3$, and $V'_i = H((CK \times P_1) \parallel P_4)$, respectively. Forth, the session key SK can be $H(ID_i \parallel N_1 N_2 \times G)$, where D_i computes $N_1 \times P_3 = N_1 N_2 \times G$ and S computes $N_2 \times P_1 = N_1 N_2 \times G$. Fifth, the path of setting the cookie should be dedicated to the embedded device to prevent an attacker from modifying the cookie stored in the embedded device.

4 Conclusions

After analyzing Kalra and Sood's scheme, it is found that five issues are not well addressed. In this paper, the details of these issues are shown with further discussions

to remedy them. With these modifications, Kalra and Sood's scheme can be improved to ensure the security of communications between embedded devices and cloud servers.

Acknowledgments

This work was supported in part by Ministry of Science and Technology under the Grants MOST 104-2221-E-034-004-, MOST 104-2221-E-025-006-, and MOST 105-2221-E-034-014-.

References

- [1] C. C. Chang, W. Y. Hsueh, and T. F. Cheng, "An advanced anonymous and biometrics-based multi-server authentication scheme using smart cards," *International Journal of Network Security*, vol. 18, no. 6, pp. 1010–1021, 2016.
- [2] T. Y. Chang, W. P. Yang, and M. S. Hwang, "Simple authenticated key agreement and protected password change protocol," *Computers & Mathematics with Applications*, vol. 49, no. 5, pp. 703–714, 2001.
- [3] Y. F. Chang, "Flexible access control over verifiable cloud computing services with provable security," *Informatica*, vol. 26, no. 2, pp. 181–198, 2015.
- [4] Y. F. Chang, W. L. Tai, and H. C. Chang, "Untraceable dynamic-identity-based remote user authentication scheme with verifiable password update," *International Journal of Communication Systems*, vol. 27, no. 11, pp. 3430–3440, 2014.
- [5] M. S. Hwang, C. C. Lee, and Y. L. Tang, "An improvement of SPLICE/AS in WIDE against guessing attack," *International Journal of Informatica*, vol. 12, no. 2, pp. 297–302, 2001.
- [6] Q. Jiang, J. Ma, G. Li, and L. Yang, "Robust two-factor authentication and key agreement preserving user privacy," *International Journal of Network Security*, vol. 16, no. 3, pp. 229–240, 2014.
- [7] S. Kalra and S. K. Sood, "Secure authentication scheme for iot and cloud servers," *Pervasive and Mobile Computing*, vol. 24, pp. 210–223, 2015.
- [8] C. W. Lin and M. S. Hwang C. S. Tsai, "A new strong-password authentication scheme using one-way hash functions," *International Journal of Computer and Systems Sciences*, vol. 45, no. 4, pp. 623–626, 2006.
- [9] C. H. Ling, C. C. Lee, C. C. Yang, and M. S. Hwang, "A secure and efficient one-time password authentication scheme for WSN," *International Journal of Network Security*, vol. 19, no. 2, pp. 177–181, 2017.
- [10] P. K. Thandra, J. Rajan, and S. A. V. S. Murty, "Cryptanalysis of an efficient password authentication scheme," *International Journal of Network Security*, vol. 18, no. 2, pp. 362–368, 2016.
- [11] C. S. Tsai, C. C. Lee, and M. S. Hwang, "Password authentication schemes: Current status and

key issues,” *International Journal of Network Security*, vol. 3, no. 2, pp. 101–115, 2006.

- [12] J. Wei, W. Liu, and X. Hu, “Secure and efficient smart card based remote user password authentication scheme,” *International Journal of Network Security*, vol. 18, no. 4, pp. 782–792, 2016.

Biography

Wei-Liang Tai biography. Wei-Liang Tai received the M.S. degree in computer science and information engineering from National Chung Cheng University, Taiwan, in 2004 and the Ph.D. degree in computer science and information engineering from National Chung Cheng University, Taiwan, in 2008. He is currently Associate Professor, Department of Information Communications, Chinese Culture University. His main interests are in information security and forensics and multimedia signal processing. He is currently an Editor of KSII Transactions on Internet and Information Systems.

Ya-Fen Chang biography. Ya-Fen Chang is a professor of Department of Computer Science and Information Engineering at National Taichung University of Science and Technology in Taiwan. She received her BS degree in computer science and information engineering from National Chiao Tung University and PhD degree in computer science and information engineering from National Chung Cheng University, Taiwan. Her current research interests include electronic commerce, information security, cryptography, mobile communications, image processing, and data hiding.

Guide for Authors

International Journal of Network Security

IJNS will be committed to the timely publication of very high-quality, peer-reviewed, original papers that advance the state-of-the art and applications of network security. Topics will include, but not be limited to, the following: Biometric Security, Communications and Networks Security, Cryptography, Database Security, Electronic Commerce Security, Multimedia Security, System Security, etc.

1. Submission Procedure

Authors are strongly encouraged to submit their papers electronically by using online manuscript submission at <http://ijns.jalaxy.com.tw/>.

2. General

Articles must be written in good English. Submission of an article implies that the work described has not been published previously, that it is not under consideration for publication elsewhere. It will not be published elsewhere in the same form, in English or in any other language, without the written consent of the Publisher.

2.1 Length Limitation:

All papers should be concisely written and be no longer than 30 double-spaced pages (12-point font, approximately 26 lines/page) including figures.

2.2 Title page

The title page should contain the article title, author(s) names and affiliations, address, an abstract not exceeding 100 words, and a list of three to five keywords.

2.3 Corresponding author

Clearly indicate who is willing to handle correspondence at all stages of refereeing and publication. Ensure that telephone and fax numbers (with country and area code) are provided in addition to the e-mail address and the complete postal address.

2.4 References

References should be listed alphabetically, in the same way as follows:

For a paper in a journal: M. S. Hwang, C. C. Chang, and K. F. Hwang, "An ElGamal-like cryptosystem for enciphering large messages," *IEEE Transactions on Knowledge and Data Engineering*, vol. 14, no. 2, pp. 445--446, 2002.

For a book: Dorothy E. R. Denning, *Cryptography and Data Security*. Massachusetts: Addison-Wesley, 1982.

For a paper in a proceeding: M. S. Hwang, C. C. Lee, and Y. L. Tang, "Two simple batch verifying multiple digital signatures," in *The Third International Conference on Information and Communication Security (ICICS2001)*, pp. 13--16, Xian, China, 2001.

In text, references should be indicated by [number].

Subscription Information

Individual subscriptions to IJNS are available at the annual rate of US\$ 200.00 or NT 7,000 (Taiwan). The rate is US\$1000.00 or NT 30,000 (Taiwan) for institutional subscriptions. Price includes surface postage, packing and handling charges worldwide. Please make your payment payable to "Jalaxy Technique Co., LTD." For detailed information, please refer to <http://ijns.jalaxy.com.tw> or Email to ijns.publishing@gmail.com.