IJNS
International Journal of Network Security

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

Vol. 17, No. 1 (Jan. 2015)

INTERNATIONAL JOURNAL OF NETWORK SECURITY

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

International Journal of Network Security

Vol. 17, No. 1 (Jan. 1, 2015)

Improving Security of a Communication-efficient Three-party Password Authentication Key Exchange Protocol

Cheng-Chi Lee[1,3], Shih-Ting Chiu[1], and Chun-Ta Li[2]
(Corresponding author: Chun-Ta Li)

Department of Library and Information Science, Fu Jen Catholic University[1]
510 Jhongjheng Rd., Sinjhuang Dist., New Taipei City 24205, Taiwan, R.O.C.
Department of Information Management, Tainan University of Technology[2]
529 Zhongzheng Road, Tainan 71002, Taiwan, R.O.C.
Department of Photonics & Communication Engineering, Asia University[3]
No. 500, Lioufeng Road, Wufeng Shiang,Taichung 402, Taiwan, R.O.C.
(Email: *th0040@mail.tut.edu.tw*)

(Received Mar. 29, 2013; revised and accepted Nov. 06, 2013)

Abstract

Three-party Password-based Authentication Key Exchange (3PAKE) allows a trusted server to assist two users to establish a common session key. Recently, Wu et al. pointed out that Chang et al.'s 3PAKE was vulnerable to the off-line guessing attack and proposed an improved 3PAKE to fix the problem. However, we found that Wu et al.'s protocol is still subject to the off-line guessing attack. In addition, the paper offers a simple method to detect the attack.

Keywords: Authentication, cryptanalysis, guessing attack, key exchange, password-based, three-party

1 Introduction

To verify remote users' identities, password authentication schemes are most commonly used when it comes to allowing users to choose their own passwords [5, 6, 11, 12, 22, 25, 28-30, 33-37, 43]. Lamport [16] was the first to propose a password authentication scheme, and since then password authentication schemes have prospered and developed into many new forms [1, 3, 4, 7-10, 13-15, 26, 27, 31, 32, 39, 42], among which Password-based Authentication Key Exchange (PAKE) is now a main stream.

1.1 Related Work

The first password-based authentication key exchange protocol was proposed by Bellovin and Merritt [1]. Using their PAKE protocol, two users can share a password to establish their common session key. However, PAKE cannot live up to the requirement of modern multi-user systems, so many researchers [2, 23, 24, 38, 40, 41] have endeavored to develop PAKE into three-party password-based authentication key exchange (3PAKE) protocols. In a 3PAKE design, there is a trusted server that assists two users to cooperate in establishing a common session key which they can use to communicate with each other privately [17-21].

Among the many 3PAKE protocols, Chang et al.'s work [2], which is based on LHL-3PAKE [24], is quite an outstanding design. Chang et al.'s protocol needs no server's public key and no symmetric cryptosystems, and they claim that the protocol meets such security requirement as mutual authentication, session key security, know-key security, forward secrecy, and protection against the off-line password guessing attack. Unfortunately, Wu et al. [38] pointed out the fact that Chang et al.'s protocol has a flaw against the off-line guessing attack. Wu et al. then proposed an improved protocol to remedy the security weakness.

1.2 Contributions

However, we found that Wu et al.'s protocol is still vulnerable to the off-line guessing attack. Therefore, in this paper, we will prove that even Wu et al.'s protocol is not secure enough against the off-line guessing attack. In addition, the paper offers a simple method to detect the attack.

1.3 Organization

The organization of this paper is as follows. Section 2 will be a brief review of Wu et al.'s protocol. Then, in Section 3, we will show why Wu et al.'s protocol is still vulnerable to the off-line password guessing attack. In Section 4, we will propose a simple method to detect the attack. Finally, the conclusion will be presented in Section 5.

2 Review of Wu et al.'s Protocol

In this Section, we review the three-party password

Table 1: The notations

Notations	Description
ε	An elliptic curve defined over a finite field $GF(p)$
P	A base point in ε with large order q, where q is a secure large prime
G	A cyclic additive group generated by P
$x \cdot P$	The point multiplication defined as $x \cdot P = P + P + \cdots + P$($x$ times)
Z_q	The ring of integers modulo q, $Z_q = \{0,1, \ldots, q-1\}$
Z_q^*	The multiplicative group of non-zero integers modulo q
$\mathcal{H}(.)$	A one-way hash function:$\{0,1\}^* \rightarrow \{0,1\}^l$
$\|$	A concatenation of bit strings
A, B	Two communication clients (users) (also representing their identities)
S	The trusted server(also representing its identities)
PW_A, PW_B	A's and B's password secretly shared with S

authenticated key exchange protocol proposed by Wu et al. [38]. In Table 1 below, there are some notations used in Wu et al.'s protocol.

The structure of their protocol is illustrated in Figure 1, and the detailed steps are as follows. To begin with, the expression $A \rightarrow B: \langle m \rangle$ means A sends a message $m$to B.

Step 1: $A \rightarrow S: \langle A, B \rangle$

A sends his/her identity and B's identity to the trusted server S as an initial request.

Step 2: $S \rightarrow A: \langle Y_A, Y_B \rangle$

After receiving A's request, S chooses two random numbers y_A, $y_B \in Z_q^*$ and computes $Y_A = y_A P + PW_A$ and $Y_B = y_B P + PW_B$, then sends Y_A and Y_B to A.

Step 3: $A \rightarrow B: \langle A, X_A, Y_B, \alpha_{AS} \rangle$

When A receives Y_A and Y_B from S, A chooses a random number $x_A \in Z_q^*$ to compute X_A=x_AP, K_{AS} = $x_A(Y_A - PW_A)$ and the hash value α_{AS} = $H(A \,||S\, ||B\, ||X_A\, ||Y_A\, ||PW_A\, ||K_{AS})$. After computing these values, A sends $\langle A, X_A, Y_B, \alpha_{AS} \rangle$ to B.

Step 4: $B \rightarrow S: \langle X_A, X_B, \gamma_B, \alpha_{AS}, \alpha_{BS} \rangle$

After B receives A's messages, B chooses a random number $x_B \in Z_q^*$ to compute $X_B = x_B P$, $K_{BS} = x_B(Y_B - PW_B)$, $K_{AB} = x_B X_A$, and two hash values $\alpha_{BS} = \mathcal{H}(B \parallel S \parallel A \parallel X_B \parallel Y_B \parallel PW_B \parallel K_{BS})$ and $\gamma_B = \mathcal{H}("1" \parallel A \parallel S \parallel B \parallel X_A \parallel X_B \parallel K_{AB})$. After computing these values, B sends $\langle X_A, X_B, \gamma_B, \alpha_{AS}, \alpha_{BS} \rangle$ to the server S.

Step 5: $S \rightarrow A: \langle X_B, \beta_{AS}, \beta_{BS}, \gamma_B \rangle$

After S receives B's messages, S uses the number chosen in Step 2to compute $K_{AS} = y_A X_A$ and the hash values $\alpha'_{AS} = \mathcal{H}(A \parallel S \parallel B \parallel X_A \parallel Y_A \parallel PW_A \parallel K_{AS})$, and then S verifies the consistency between the computed $\alpha'_{AS}$and the value α_{AS} sent from B. In order to authenticate B, S computes $K_{BS} = y_B X_B$ and the hash value $\alpha'_{BS} = \mathcal{H}(B \parallel S \parallel A \parallel X_B \parallel Y_B \parallel PW_B \parallel K_{BS})$, and then S verifies the consistency between the computed α'_{BS} and the value α_{BS} sent from B. If these values are correct, S computes the hash values $\beta_{AS} = \mathcal{H}(A \parallel S \parallel B \parallel X_A \parallel Y_A \parallel PW_A \parallel K_{AS} \parallel X_B)$ and $\beta_{BS} = \mathcal{H}(B \parallel S \parallel A \parallel X_B \parallel Y_B \parallel PW_B \parallel K_{BS} \parallel X_A)$, and then Ssends $X_B, \beta_{AS}, \beta_{BS}, \gamma_B$ to A.

Step 6: $A \rightarrow B: \langle \beta_{BS}, \gamma_A \rangle$

When A receives S's messages, A uses K_{AS}, which was computed in Step 3, and X_B to compute the hash value $\beta'_{AS} = \mathcal{H}(A \parallel S \parallel B \parallel X_A \parallel Y_A \parallel PW_A \parallel K_{AS} \parallel X_B)$. In order to authenticate S, A verifies the consistency between the computed β'_{AS} and the value β_{AS} sent from S. If the result is correct, A computes $K_{AB} = x_A X_B$ and the hash value $\mathcal{H}("1" \parallel A \parallel S \parallel B \parallel X_A \parallel X_B \parallel K_{AB})$ and then verifies the value γ_B. If these values are correct, A can make sure that B has the ability to compute the session key $SK = \mathcal{H}(2 \parallel A \parallel S \parallel B \parallel X_A \parallel X_B \parallel K_{AB})$. After that, A sends β_{BS} and γ_A to B.

Step 7:

After receiving A's messages, B derives the hash value $\mathcal{H}(B \parallel S \parallel A \parallel X_B \parallel Y_B \parallel PW_B \parallel K_{BS} \parallel X_A)$ from X_A and K_{BS}. In order to authenticate S, B verifies the consistency between β_{BS} and the hash value $\mathcal{H}(B \parallel S \parallel A \parallel X_B \parallel Y_B \parallel PW_B \parallel K_{BS} \parallel X_A)$. If the result is correct, B computes the hash value $\mathcal{H}("0" \parallel A \parallel S \parallel B \parallel X_A \parallel X_B \parallel K_{AB})$ and verifies whether the value γ_A which was sent from A is correct or not. If the result is positive, B can make sure that A has ability to compute the session key $SK = \mathcal{H}(2 \parallel A \parallel S \parallel B \parallel X_A \parallel X_B \parallel K_{AB})$.

With the above steps done, A and B can generate a common session key $SK = \mathcal{H}(2 \parallel A \parallel S \parallel B \parallel X_A \parallel X_B \parallel K_{AB})$ via the trusted server S.

3 Some Vulnerabilities of Wu et al.'s Protocol

In this section, we will show that an off-line guessing attack can break Wu et al.'s protocol. An attacker can pretend to be the server and intercept the messages sent from the users. The structures of the steps of our attack are shown in Figure 2, Figure 3, and Figure 4.

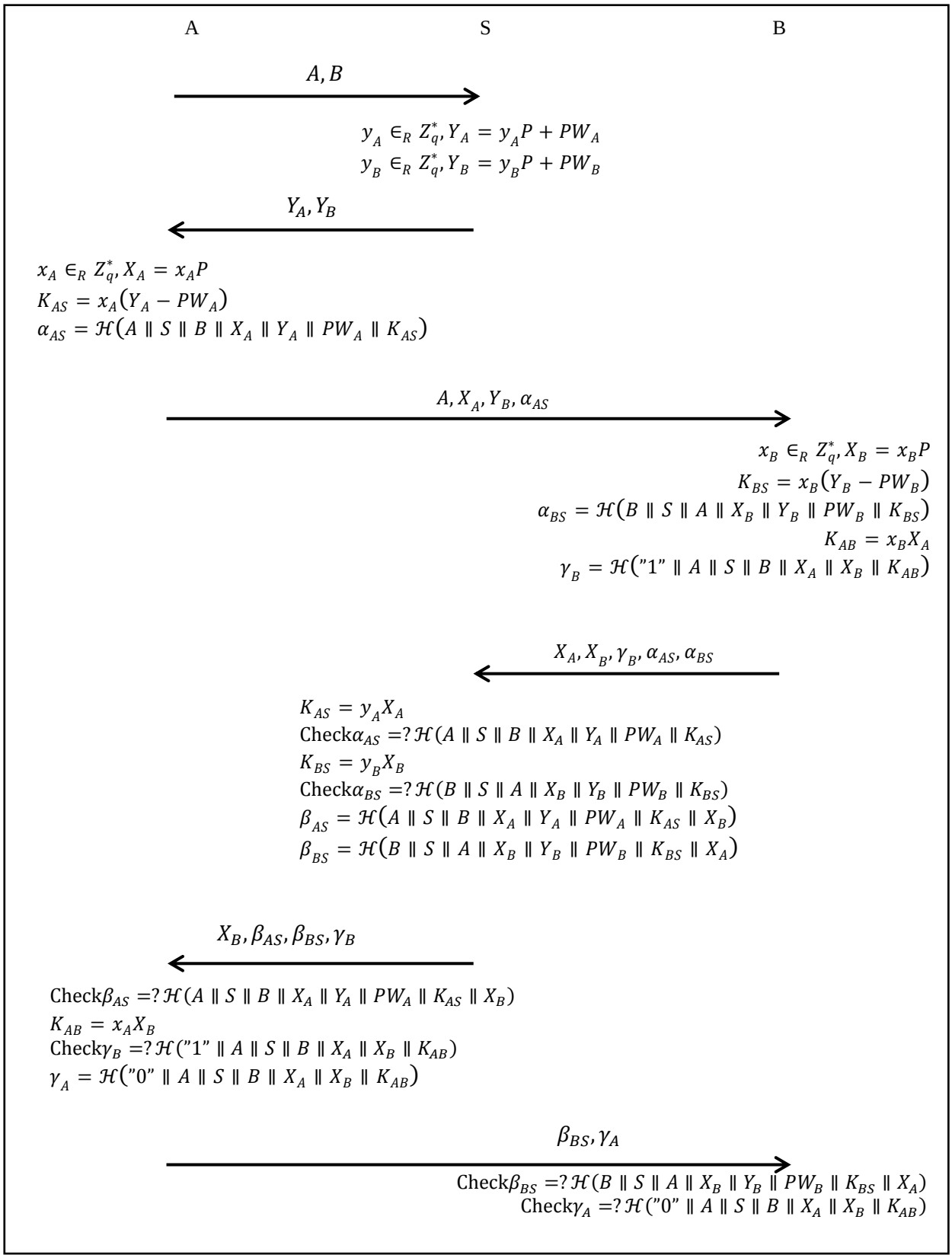


Figure 1: Wu et al.'s 3PAKE protocol

Step 1:

Suppose there is a user A who wants to communicate with another person $\star$. A sends his/her identity along with $\star$'s identity to the server as an initial request. At this point of time, the attacker S^* pretends to be the sever $S$and intercepts the messages sent from A and

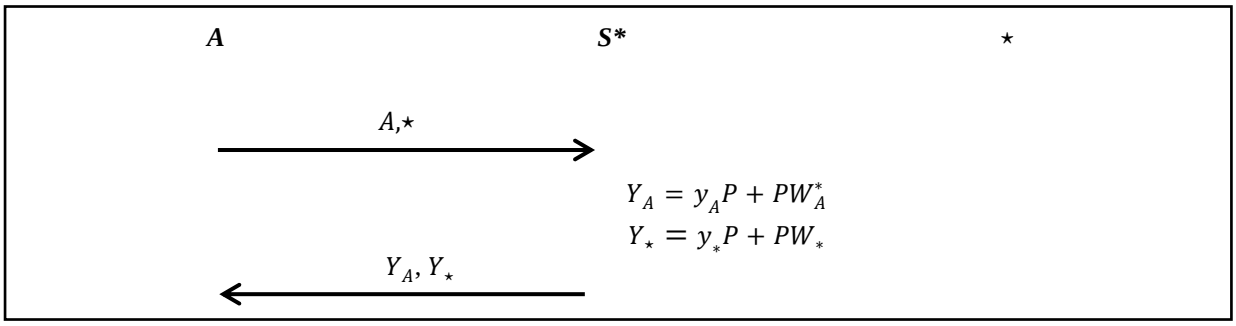


Figure 2: Step 1 of our attack

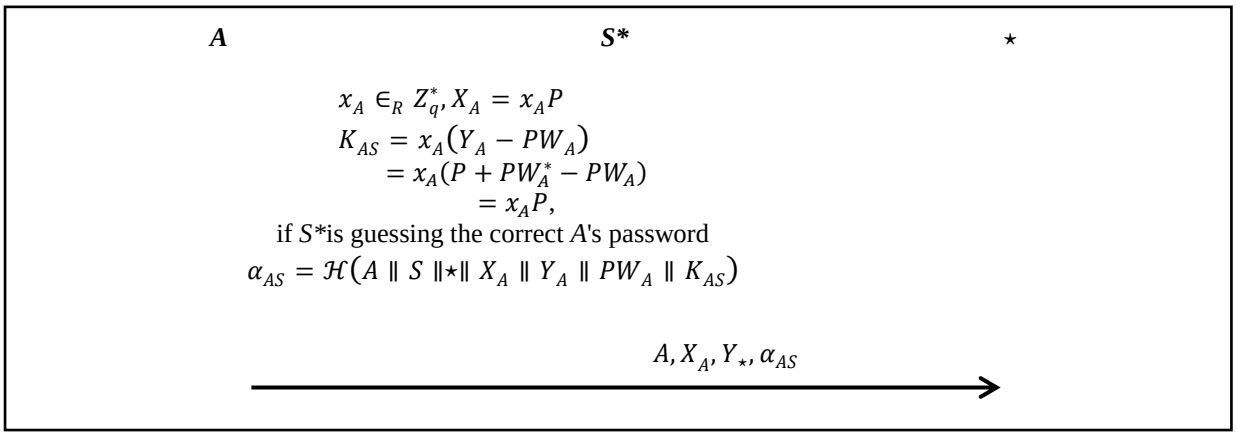


Figure 3: Step 2 of our attack

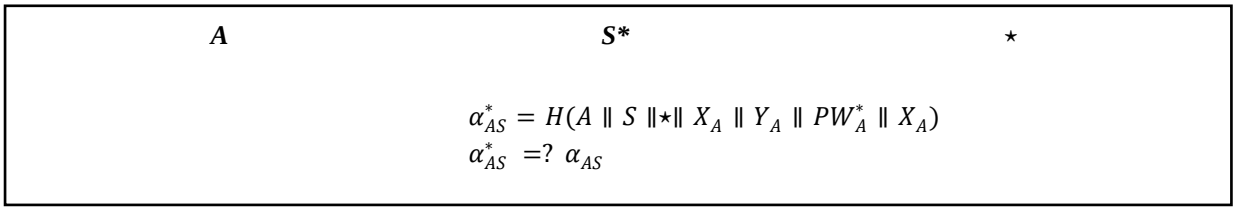


Figure 4: Step 3 of our attack

sets y_A=1 and computes$Y_A = y_A P + PW_A^*$, where PW_A^* is the password which the attacker has guessed. After that, S^* sendsY_A and $Y_\star$ to A, where $Y_\star = y_* P + PW_*$. y_* is a random number and $PW_*$is a possible password.

Step 2:

When A receives Y_A and $Y_\star$ from S^*, A computes $X_A = x_A P$, $K_{AS} = x_A(Y_A - PW_A)$ and $\alpha_{AS} = \mathcal{H}(A \parallel S \parallel \star \parallel X_A \parallel Y_A \parallel PW_A \parallel K_{AS})$. After finishing the computation, Awill send $A, X_A, Y_\star, \alpha_{AS}$ to $\star$. Note that $\mathcal{H}()$is a public one-way hash function.

Step 3:

When A sends $A, X_A, Y_\star, \alpha_{AS}$ to $\star$, the attacker can intercept the messages and then compute $\alpha_{AS}^* = H(A \parallel S \parallel \star \parallel X_A \parallel Y_A \parallel PW_A^* \parallel X_A)$. If the attacker's guess of the password PW_A^* is correct, then K_{AS} is equal to $x_A P$. The attacker can then use it to compute α_{AS}^* and check if α_{AS}^* is equal to α_{AS}. If it is, the attacker can make sure that he/she has guessed A's password.

4 Improving Security of Wu et al.' Protocol

To detect the attack during the communication, in Step 3 of Wu et al.'s protocol, A can check to see if X_A is the same as K_{AS}. If it holds, A can be sure that the communication is under attack. In addition, in Step 2 of Wu et al.'s protocol, the server must choose y_A and y_B such that y_A not equal to 1 and y_B not equal to 1.

5 Conclusions

In this paper, we have shown that Wu et al.'s 3PAKE protocol is still vulnerable to the off-line password guessing attack. In addition, we have also offered a simple method to detect the attack.

Acknowledgements

The authors would like to express their appreciation to the anonymous referees for their valuable suggestions and

comments. This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC 101-2221-E-030-018 and NSC 102-2221-E-030-003.

References

[1] S. M. Bellovin and M. Merritt, "Encrypted key exchange: password-based protocols secure against dictionary attacks," in Proceedings of 1992 IEEE Computer Society Conference on Research in Security and Privacy, pp. 72-84, 1992.

[2] T. Y. Chang, M. S. Hwang, and W. P. Yang, "A communication-efficient three-party password authenticated key exchange protocol," Information Sciences, vol. 181, pp. 217-226, 2011.

[3] T. Y. Chang, C. C. Yang and M. S. Hwang, "Improvement of convertible authenticated encryption schemes and its multiple recipients version", International Journal of Security and Its Applications, vol. 6, no. 4, pp. 151-162, 2012.

[4] T. Y. Chang, W. P. Yang, M. S. Hwang, "Simple authenticated key agreement and protected password change protocol", Computers & Mathematics with Applications, vol. 49, pp. 703-714, 2005.

[5] T. Y. Chen, C. C. Lee, M. S. Hwang, J. K. Jan, "Towards secure and efficient user authentication scheme using smart card for multi-server environments," The Journal of Supercomputing, vol. 66, no. 2, pp. 1008-1032, 2013.

[6] T. H. Feng, C. H. Ling, and M. S. Hwang, "Cryptanalysis of Tan's improvement on a password authentication scheme for multi-server environments," International Journal of Network Security, vol. 16, no. 4, pp. 318-321, 2014.

[7] D. He, J. Chen, and J. Hu, "Weaknesses of a remote user password authentication scheme using smart card," International Journal of Network Security, vol. 13, no. 1, pp. 58-60, 2011.

[8] H. C. Hsiang and W. K. Shih, "Weaknesses and improvements of the Yoon–Ryu–Yoo remote user authentication scheme using smart cards," Computer Communications, vol. 32, no. 4, pp. 649-652, 2009.

[9] W. B. Hsieh and J. S. Leu, "Exploiting hash functions to intensify the remote user authentication scheme," Computers & Security, vol. 31, no. 6, pp. 791-798, 2012.

[10] M. S. Hwang, S. Y. Hsiao, W. P. Yang, "Security on improvement of modified authenticated key agreement protocol," Information - An International Interdisciplinary Journal, vol. 17, no. 4, pp.1173-1178, 2014.

[11] M. S. Hwang, C. C. Lee, 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.

[12] M. S. Hwang, S. K. Chong, T. Y. Chen, "DoS-resistant ID-based password authentication scheme using smart cards", Journal of Systems and Software, vol. 83, pp. 163-172, 2010.

[13] M. S. Hwang and C. H. Lee, "Authenticated key-exchange in a mobile radio network", European Transactions on Telecommunications, vo1. 8, no.3, pp.265-269, 1997.

[14] M. S. Hwang, C. W. Lin, C. C. Lee, "Improved Yen-Joye's authenticated multiple-key agreement protocol", IEE Electronics Letters, vol. 38, no. 23, pp. 1429-1431, 2002.

[15] L. C. Huang, M. S. Hwang, "Two-party authenticated multiple-key agreement based on elliptic curve discrete logarithm problem", International Journal of Smart Home, vol. 7, no. 1, pp. 9-18, 2013.

[16] L. Lamport, "Password authentication with insecure communication," Communications of the ACM, vol. 24, no. 11, pp. 770-772, 1981.

[17] C. C. Lee, R. X. Chang, and H. J. Ko, "Improving two novel three-party encrypted key exchange protocols with perfect forward secrecy," International Journal of Foundations of Computer Science, vol. 21, no. 6, pp. 979-991, 2010.

[18] C. C. Lee and Y. F. Chang, "On security of a practical three-party key exchange protocol with round efficiency," Information Technology and Control, vol. 37, no. 4, pp. 333-335, 2008.

[19] C. C. Lee, S. D. Chen, and C. L. Chen, "A computation-efficient three-party encrypted key exchange protocol," Applied Mathematics & Information Sciences, vol. 6, no. 3 pp. 573-579, 2012.

[20] C. C. Lee, C. T. Li, and R. X. Chang, "An undetectable on-line password guessing attack on Nam et al.'s three-party key exchange protocol," accepted to appear in Journal of Computational Methods in Sciences and Engineering, 2013

[21] C. C. Lee, C. T. Li, and C. W. Hsu, "A three-party password-based authenticated key exchange protocol with user anonymity using extended chaotic maps," Nonlinear Dynamics, vol. 73, no. 1, pp. 125-132, 2013.

[22] 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.

[23] T. F. Lee, J. L. Liu, M. J. Sung, S. B. Yang, and C. M. Chen, "Communication-efficient three-party protocols for authentication and key agreement," Computers & Mathematics with Applications, vol. 58, no. 4, pp. 641-648, 2009.

[24] T. F. Lee, T. Hwang, and C. L. Lin, "Enhanced three-party encrypted key exchange without server public keys," Computers & Security, vol. 23, no. 7, pp. 571-577, 2004.

[25] C. T. Li and M. S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart

cards", Journal of Network and Computer Applications, vol. 33, no. 1, pp. 1-5, 2010.

[26] C. T. Li, M. S. Hwang, Y. P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular Ad Hoc networks", Computer Communications, vol. 31, no. 12, pp. 2803-2814, 2008.

[27] C. T. Li, M. S. Hwang, Y. P. Chu, "Improving the security of a secure anonymous routing protocol with authenticated key exchange for Ad Hoc networks", International Journal of Computer Systems Science and Engineering, vol. 23, no. 3, pp. 227-234, 2008.

[28] I-En Liao, C. C. Lee, M. S. Hwang, "A password authentication scheme over insecure networks", Journal of Computer and System Sciences, vol. 72, no. 4, pp. 727-740, 2006.

[29] C. W. Lin, C. S. Tsai, M. S. Hwang, "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.

[30] I. C. Lin, H. H. Ou, M. S. Hwang, "A user authentication system using back-propagation network", Neural Computing & Applications, vol. 14, no. 3, pp. 243-249, 2005.

[31] J. W. Lo, J. Z. Lee, M, S. Hwang, Y. P. Chu, "An advanced password authenticated key exchange protocol for imbalanced wireless networks", Journal of Internet Technology, vol. 11, no. 7, pp. 997-1004, 2010.

[32] J. W. Lo, S. C. Lin, M. S. Hwang, "A parallel password-authenticated key exchange protocol for wireless environments", Information Technology and Control, vol. 39, no. 2, pp. 146-151, 2010.

[33] J. J. Shen, C. W. Lin, M. S. Hwang, "Security enhancement for the timestamp-based password authentication scheme using smart cards", Computers & Security, vol. 22, no. 7, pp. 591-595, 2003.

[34] H. Tao and C. Adams, "Pass-go: aproposal to improve the usability of graphical passwords,"International Journal of Network Security, vol. 7, no. 2, pp. 273-292, 2008.

[35] 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.

[36] R. C. Wang and C. C. Yang, "Cryptanalysis of two improved password authentication schemes using smart cards," International Journal of Network Security, vol. 3, no. 3, pp. 283-285, 2006.

[37] H. C. Wu, M. S. Hwang, C. H. Liu, "A secure strong-password authentication protocol", Fundamenta Informaticae, vol. 68, pp. 399-406, 2005.

[38] S. Wu, Q. Pu, S. Wang, and D. He, "Cryptanalysis of a communication-efficient three-party password authenticated key exchange protocol," *Information Sciences*, vol. 215, pp. 83-96, 2012.

[39] C. C. Yang, T. Y. Chang, M. S. Hwang, "Cryptanalysis of simple authenticated key agreement protocols", IEICE Transactions on Foundations, vol. E87-A, no. 8, pp. 2174-2176, 2004.

[40] Y. Zeng, J. Ma, and M. Sangjae, "An improvement on a three-party password-based key exchange protocol using weil pairing," *International Journal of Network Security*, vol. 11, no. 1, pp. 17-22, 2010.

[41] J. Zhao and D. Gu, "Provably secure three-party password-based authenticated key exchange protocol," *Information Sciences*, vol. 184, no. 1, pp. 310-323, 2012.

[42] Y. Zhang and M. Fujise, "Security management in the next generation wireless networks," *International Journal of Network Security*, vol. 3, no. 1, pp. 1-7, 2006.

[43] X. Zhuang, C. C. Chang, Z. H. Wang, Y. Zhu, "A simple password authentication scheme based on geometric hashing function," *International Journal of Network Security*, vol. 16, no. 4, pp. 237-243, 2014.

Cheng-Chi Lee received the Ph.D. degree in Computer Science from National Chung Hsing University (NCHU), Taiwan, in 2007. He is currently an Associate Professor with the Department of Library and Information Science at Fu Jen Catholic University. Dr. Lee is currently as an editorial board member of International Journal of Network Security and Journal of Computer Science. He also served as a reviewer in many SCI-index journals, other journals, other conferences. His current research interests include data security, cryptography, network security, mobile communications and computing, wireless communications. Dr. Lee had published over 100+ articles on the above research fields in international journals.

Shih-Ting Chiu received the B.S. in Computer Science and Information Engineering, National Taitung University, Taitung, Taiwan, R.O.C, in 2012. She will receive the M.S. in Library and Information Science, Fu Jen Catholic University, New Taipei City 24205, Taiwan, R. O. C. Her current research interests include information security and cryptography.

Chun-Ta Li received the Ph.D. degree in Computer Science and Engineering from National Chung Hsing University, Taiwan, in 2008. He is currently an assistant professor of the Department of Information Management, Tainan University of Technology, Tainan, Taiwan. He is a member of IEEE, a member of Chinese Information Security Association, a member of Future Technology Research Association International, a member of IFIP WG 11.3, a member of Machine Intelligence Research Labs, and an editorial board member of International Journal of Network Security. His research interests include information security, wireless sensor networks, mobile computing, and security protocols for ad hoc networks. Dr. Li has published more than 70 papers in international journals and international conferences.

Energy-Efficient Security for Voice over IP

Hoseb M. Dermanilian, Farah Saab, Imad H. Elhajj, Ayman Kayssi, and Ali Chehab
(Corresponding author: Imad H. Elhajj)

Department of Electrical and Computer Engineering, American University of Beirut
Riad El-Solh, Beirut 1107 2020, Lebanon
(Email: ie05@aub.edu.lb)

(Received Feb. 24, 2013; revised and accepted Aug. 14, 2013)

Abstract

The fast spread of handheld smart devices contributed to the development of VoIP softphones running over such devices. Most security mechanisms were mainly designed for desktop PCs and hence did not take into consideration the power constraints of handheld devices. This fact highly motivated the development of new security mechanisms that try to minimize the energy consumption without compromising the security of the exchanged data. In this paper, we propose an energy-efficient security algorithm for VoIP applications running on mobile devices (SecVoIP). The algorithm resolves several weaknesses available in current algorithms while maintaining an appropriate security level. Several experiments were conducted and the results showed significant improvement in processing time, CPU cycles, and consumed energy as compared to SRTP, one of the most widely used security protocols for VoIP. Moreover, we present the results of extensive experimental work that demonstrates that known plaintext attacks against audio streams are not feasible.

Keywords: Energy efficiency, handheld devices, selective encryption, SRTP, VoIP security

1 Introduction

Voice over Internet Protocol (VoIP) has become widely used worldwide as an alternative for the traditional phone service. Besides offering cheaper rates for long distance calls, VoIP freely supports a wide variety of services that users previously had to pay for, such as caller ID, voicemail, call waiting, call forwarding and call conferencing [21]. VoIP technology operates based on two types of standardized protocols: signaling and media protocols. Signaling protocols are responsible for call initiation, control, and termination, while media protocols are intended to carry voice data.

VoIP security has become one of the main concerns for both users and service providers since telephone conversations may carry sensitive and confidential information. Additionally, telephone services are used to verify the identity of the speaker as an authentication method. Therefore, whenever VoIP services are offered, they are expected to provide security services such as confidentiality, integrity, and authentication. However, providing secure VoIP services that are immune to the various types of attacks is a challenging issue, especially that many vulnerabilities related to the core IP network are inherited by VoIP. In addition, VoIP also suffers from signaling and media protocol specific vulnerabilities [8, 13, 31]. Furthermore, there is usually a trade-off between VoIP security and Quality of Service (QoS) [27]. The fact that the usage of VoIP over handheld devices has recently increased dramatically makes the process of implementing security mechanisms more challenging because of the power constraints of these handheld devices. We note here that securing the signaling of VoIP is outside the scope of this paper and the focus is on providing confidentiality of the media stream.

There is little work in the literature regarding efficient security mechanisms that meet both security requirements and processing overhead. It is known that conventional security mechanisms incur significant processing overhead and hence high energy consumption. This work proposes an energy-aware security mechanism for VoIP on handheld devices. This mechanism is based on a fact (demonstrated in this paper) that it is almost impossible for an attacker to predict the audio encoders' output frames of data (known as plaintext attacks) and the fact that these data frames contain much lower information density than that of textual data. The developed method reduces the processing time, which in turn reduces the consumed energy, while providing end-to-end security and maintaining good QoS from an end-to-end delay perspective. The proposed method is an enhanced security method over that proposed in [6]. The enhancement targets the required processing time to a level that is even lower than that of the Secure Real-time Transport Protocol (SRTP) yet without compromising end-to-end security.

The rest of the paper is organized as follows: Section 2 presents a literature review related to VoIP security in general and covers the work done in evaluating conventional and new security mechanisms. Section 3 introduces the proposed enhanced algorithm along with its analysis. In Section 4, the efficiency of the proposed mechanism is demonstrated experimentally. Finally, Section 5 concludes the paper.

2 Literature Review

The literature review covers two main categories: (1) VoIP signaling and media security, and (2) proposed security mechanisms:

2.1 VoIP Security

Since the core architecture of VoIP differs from that of the traditional Public Switched Telephone Network (PSTN), serious security issues are associated with VoIP and hence should be addressed [22]. The main challenge in VoIP security is to provide a service that possesses a level of security comparable to that of PSTN while maintaining an acceptable level of QoS and energy consumption.

Butcher et al. discuss general security issues related to VoIP and IP networks. They also discuss several attacks related to VoIP at the application level (attacks related to the Session Initiation Protocol (SIP)) suggesting different countermeasures to these attacks [4]. VoIP can also be protected by well-known security mechanisms such as IP Security (IPSec), Transport Layer Security (TLS), etc., with each having its own advantages and drawbacks. Barbieri et al. studied the impact of IPSec when used to secure VoIP. The results showed that the effective bandwidth is reduced by 50% in case of VoIP IPSec when compared to VoIP service alone [2]. Gupta et al. presented a structured discussion of VoIP security whereby they targeted three main aspects: media, signaling, and key derivation. They recommended that a replay-protected key exchange mechanism should be used along with SRTP [17]. Comparison of different security methods is also performed to investigate the impact on multimedia traffic. Hong et al. compared three main protocols: H.235, IPSec and SRTP. IPSec suffers from computational and bandwidth overhead over the other two protocols. SRTP seems to be the most suitable protocol due to the use of more advanced and modern cryptographic algorithms that take into account the QoS requirements of multimedia transmission [20]. Diab et al. conducted a comparison of different VPN security protocols that are used to protect VoIP data [11].

In order to answer the question of whether to use block or stream cipher to protect VoIP communications, Elbayoumy and Shepherd tried to compare the impact of AES cipher when it is applied both in block and stream mode to secure VoIP. Results showed that in terms of packet size, stream mode adds overhead to the packet less than block mode does. Results also showed that crypto engine performs better in case of stream cipher. Researchers concluded that subjective MOS and end-to-end delay measures gave better results in case of stream cipher compared to that of block cipher [12].

2.2 Evaluation of Conventional and New Security Algorithms

In order to evaluate the performance of SRTP and its effect on voice quality, Alexander et al. conducted an experiment to measure packet inter-arrival and jitter with and without security using a G.711 codec. The results showed that authentication is more time consuming than encryption [1]. New security algorithms based on selective encryption methodology as an alternative to conventional security mechanisms were also proposed in the literature. Servetti et al. proposed a new mechanism that partially encrypts the compressed bit stream at the output of a G.729 codec. The proposed method is based on the fact that the compressed bits have unequal perceptual importance. The proposed algorithm was subjected to both objective and subjective tests to prove its efficiency [29]. Choo et al. proposed a new lightweight mechanism to secure multimedia transmission and it was mainly proposed for video traffic. The algorithm involves two block transposition operations along with a single XOR operation on each video frame. Experiments showed that the new proposed algorithm is three times faster than applying the Advanced Encryption Standard (AES) on video data. It was also shown that Secure Real Time Media Transmission (SRMT) is better than previously proposed mechanisms in terms of security and QoS [9].

In order to reduce the complexity of encrypting a voice stream to fulfill the power constraints of handheld devices, a new method based on selective encryption for Moving Picture Experts Group (MPEG) voice streams was proposed by Servetti et al. The method exploits the fact that a voice stream can be divided into perceptual and non-perceptual parts and it achieves security by only encrypting the perceptual bits [30]. Wu et al. applied syntax-aware selective encryption that takes into account communication and transmission constraints. The location of the encryption process within the bit stream is also discussed [33]. Xie et al. introduced a new method to encrypt the compressed bit stream that represents the output of entropy encoders. It is stated that because the resulting bit stream at the output of the encoder has significant randomness, it is not necessary to perform heavyweight cryptographic techniques, and hence inserting a simple randomness operation in the stream is sufficient [32]. Han et al. proposed a new encryption method for multimedia content on handheld devices and it works by alternating between AES in block mode and RC4 in stream mode. The proposed method was evaluated using desktop computers and MPEG Layer III (MP3) audio files [19]. Abou Charanek et al. proposed a new method for encrypting voice traffic based on selective encryption called Energy Efficient Voice over IP Privacy (E^2VoIP^2) [6]. The study showed that encrypting the voice traffic with conventional algorithms consumes a significant amount of energy in addition to the introduced delays, specifically for handheld devices. Compared to SRTP, E^2VoIP^2 is more efficient in terms of CPU cycles and processing time when it is implemented on HP iPAQ handheld devices. The proposed mechanism was based on mixing a block cipher with a stream cipher by simply applying an AES block cipher on the first packet which is padded with a random number within segmented groups, and performing XOR operation on the remaining packets within the same group using the corresponding random

number.

SRTP is one of the most popular security mechanisms used to secure media streams in VoIP applications. SRTP has a very low overhead and it is the secure version of the traditional Real Time Protocol/ Real-time Transport Control Protocol (RTP/RTCP) which is mainly used for real-time transmission of multimedia over IP. SRTP provides confidentiality, integrity, authentication, and replay protection for RTP and RTCP traffic. In SRTP, AES in counter or f8 mode and HMAC-SHA-1 are the predefined algorithms for encryption and authentication, respectively [3].

Although there is significant work in the literature that aims at developing an efficient VoIP security solution, only a few of them took into consideration the limited energy capabilities of handheld devices. Most of the proposed selective encryption methods are codec-dependent and are rarely tested and assessed on handheld devices [16]. In the next sections, we describe our proposed algorithm (SecVoIP) and show how it achieves a good balance between energy consumption and security without affecting the quality of the exchanged voice. We will highlight the enhancement of SecVoIP as compared to the recent algorithm presented in [6], namely, E^2VoIP^2. The first improvement is related to the generation of the random number that was added to the first packet of each group in E^2VoIP^2. This random number was used to encrypt/decrypt the remaining packets of the group. Therefore, any loss of the first packet of a group leads to discarding the remaining packets in the group. We overcome this weakness by eliminating the padding process of any additional data to the original packet. The generation of the random number that is used to decrypt the packets of the group can still be performed even if there is a packet loss. Moreover, avoiding the padding process solves major drawbacks in E^2VoIP^2 such as additional bandwidth and time consumption, which resulted from adding such extra information to the packet. Moreover, the comparative assessment was performed on a modern platform consisting of a Samsung Nexus S smartphone running the Android 2.3 operating system.

3 SecVoIP Design and Analysis

As mentioned previously, SRTP is the most widely used standardized protocol to secure VoIP communications. The global trend to develop more energy-efficient mechanisms for battery-powered handheld devices motivated the design and implementation of an energy-efficient security mechanism that outperforms SRTP in terms of processing time and energy consumption without compromising the security of the data. As in [6], the attacker model incorporates packet sniffing, replaying, dropping, and reordering capabilities. Based on experimental and analytical analysis presented in [6] and further validation in this work, it is demonstrated that such an attacker is not capable of performing known plain text attacks even with direct access to the raw signal.

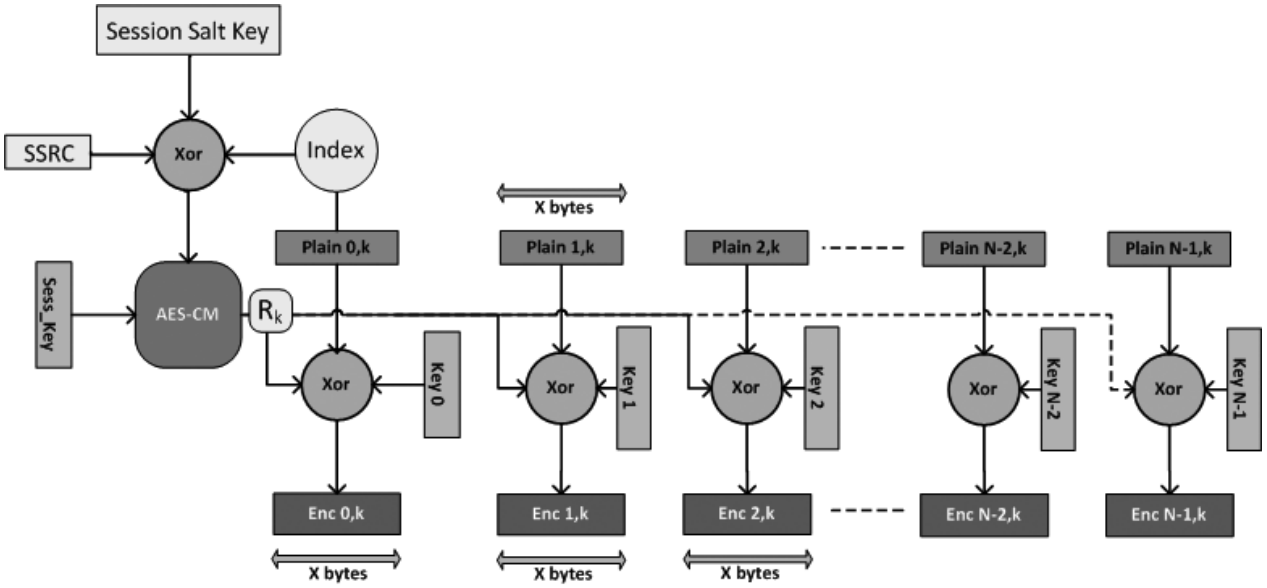


Figure 1: Design of SecVoIP encryption algorithm

3.1 SecVoIP Design

SecVoIP combines the mechanism of E^2VoIP^2 in encrypting voice packets and the mechanism of SRTP in generating the key stream. As shown in Figure 1, voice packets are divided into groups of N packets each. For the first packet of each group, AES in counter mode is applied to generate a pseudorandom stream involving attributes similar to those used in SRTP. Afterwards, every packet in the group is encrypted by XOR-ing the triplet: plaintext, random number, and the predefined key at every packet position. Let X be the size of the plaintext in bytes which is

defined by the encoder in use. Considering a group k of N packets as shown in Figure 1, every plain packet ($Plain_{x,k}$) in the group is encrypted based on Equations (1) and (2).

$$Enc_{x,k} = Plain_{x,k} \oplus Key_x \oplus R_k \quad (1)$$

$$Let\, K_{xk} = Key_x \oplus R_k \Rightarrow Enc_{x,k} = Plain_{x,k} \oplus K_{xk} \quad (2)$$

The pseudorandom string R_k of X bytes used in Equation (1) is distinct for every group. One major difference between SecVoIP and SRTP is that instead of generating a pseudorandom string for every packet being transmitted and received, SecVoIP does so only once at the beginning of every group of N packets. Therefore, R_k for a certain group is calculated over an initial value (IV_k) using:

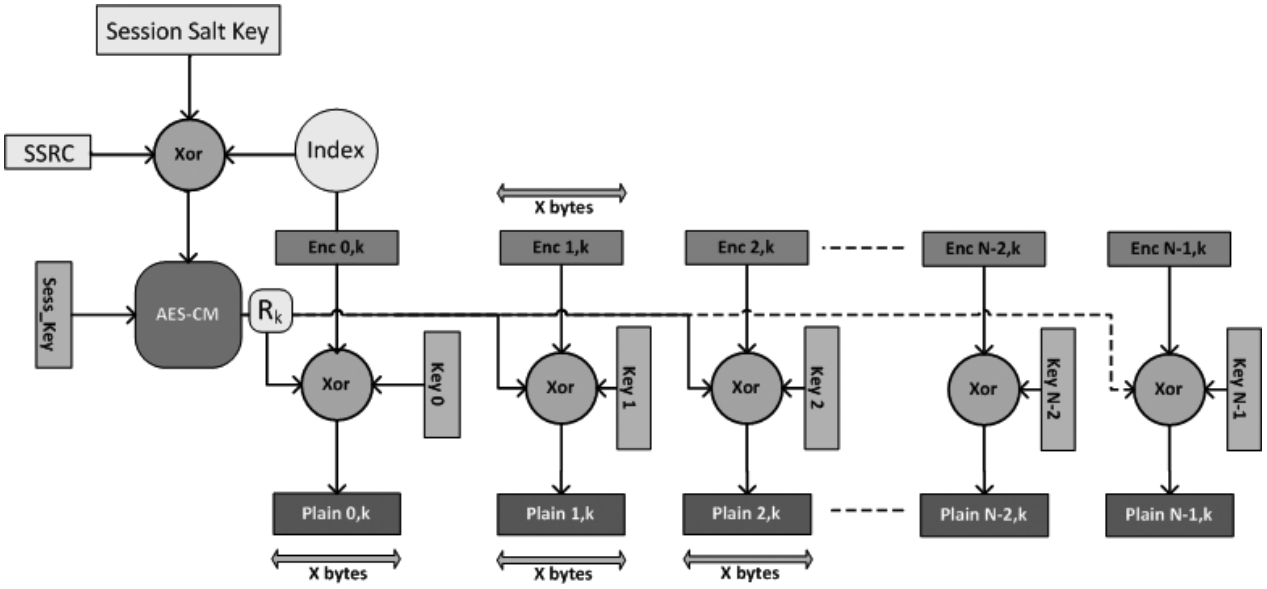


Figure 2: Design of SecVoIP decryption algorithm

$$IV_k = (SSRC) \oplus (Session\_Salt\_Key) \oplus (index_{k,0}) \quad (3)$$

Where SSRC is a 32 bit Synchronization Source Identifier that is chosen randomly and Session Salt Key is a random number used to defeat pre-calculation attacks, whereas $index_{k,0}$ is formed based on the Sequence Number (SEQ) of the first packet in group *K* and current Roll Over Counter ROC as defined in [3]:

$$Index = 2^{16} \times ROC \oplus SEQ$$

As soon as IV_k is calculated, it is fed to AES in counter mode to generate R_k. The same procedure is repeated for the next group (K+1) of packets and a distinct R_{k+1} is generated. This process continues as long as voice packets are produced by the encoder.

In addition to session key and session salt keys, which are used by AES to generate the random stream that will be used to encrypt the packets in the group, N predefined keys of size X bytes need to be shared between the sender and the receiver as in E^2VoIP^2. However, E^2VoIP^2 did not suggest any special mechanism to exchange these keys. Therefore, instead of using conventional key exchange mechanisms which may be considered costly, we suggest using SRTP's key generation mechanism [3]. From a single exchanged master key and master salt, we can generate all necessary keys by assigning different label values for each key at a certain position. Hence, both sides can agree on a key derivation rate at which all keys are refreshed, thus increasing the security of the method. In either case, key derivation must be performed once at the start of the conversation such that sufficient keys are supplied to the encryption and decryption modules. Any mechanism can be used to exchange the required master key, master salt, and key derivation rate. However, there are various key exchange mechanisms proposed in the literature in the context of VoIP security. Among these mechanisms are SDES, MIKEY, ZRTP, DTLS-SRTP and others [1]. MIKEY is the most widely used mechanism for SRTP. Any of these key exchange mechanisms can be used to share the required keys between parties. Gupta et al. present a detailed security analysis for each of these key exchange mechanisms along with some security considerations in applying each of them [17]. The exchanged keys should be kept secret and stored by the caller and the callee within a cryptographic context along with other transformation related parameters. The additional overhead caused by the generation of additional keys is analyzed later in this section. Note that the attributes involved in the generation of the random number R_k are all known to the receiver except the ROC which is maintained by the receiver using the mechanism proposed in [3] or any other efficient mechanism. This fact eliminates the need to pad the random number to the first packet of each group, giving SecVoIP a major advantage over E^2VoIP^2.

Assuming that the number of packets per group (N) is known to the receiver, decryption is performed in the same way as encryption, as shown in Figure 2, and hence only the encryption process is analyzed in the next section.

3.2 SecVoIP Analysis

In the following section, we analyze the proposed algorithm from a networking and a security perspective.

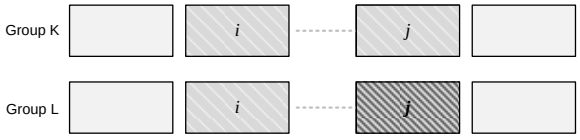
3.2.1 Bandwidth Overhead and Packet Loss

Assuming that all the previously-mentioned algorithms are using RTP as the media-carrying protocol, the ability to generate the random number at the receiver side without the need to transmit additional data allowed the bandwidth consumption to be equal to that of SRTP.

From a packet loss perspective, and since all the attributes involved in generating the group-specific random number can be generated by the receiver, even if the first packet of the group is lost, synchronization between sender and receiver can be maintained which is not the case in E^2VoIP^2. Packet loss effect in SecVoIP is similar to that in SRTP. So, the same packet loss concealment methods used in conjunction with SRTP can be used in SecVoIP.

3.2.2 Security Concerns

A security analysis is performed in [6] in order to ensure the security of the proposed mechanism. It is shown that E^2VoIP^2 is theoretically immune against different scenarios of known ciphertext and known plaintext/ciphertext attacks. Since SecVoIP is designed based on the basic principles of both SRTP and E^2VoIP^2, it inherits the security properties of both. The same security concerns of SRTP mentioned in [3] are also applicable to SecVoIP. In addition to the scenarios mentioned in [6], there is a specific scenario to which SecVoIP and E^2VoIP^2 are vulnerable. The success of this attack highly depends on the ability of the attacker to deduce some of the plaintext packets in the voice stream. If the attacker is able to know the plaintext packets at positions i and j in a certain group K and a plaintext packet at position i within a different group L, the attacker can deduce the plaintext packet at position J in group L.



From Equations (1) and (2):

$$Enc_{i,k} \oplus Enc_{j,k} =$$
$$(Plain_{i,k} \oplus R_k \oplus Key_i) \oplus (Plain_{j,k} \oplus R_k \oplus Key_j) = C$$
$$\Rightarrow Plain_{i,k} \oplus Key_i \oplus Plain_{j,k} \oplus Key_j = Key_i \oplus Key_j = C$$

$$Enc_{i,L} \oplus C =$$
$$(Plain_{i,L} \oplus R_L \oplus Key_i) \oplus (Key_i \oplus Key_j) = W$$
$$\Rightarrow (Plain_{i,L} \oplus R_L \oplus Key_j) = R_L \oplus Key_j = W$$

$$Enc_{j,L} \oplus W =$$
$$(Plain_{j,L} \oplus R_L \oplus Key_j) \oplus (R_L \oplus Key_j) = Plain_{j,L}$$

In general, this type of attack becomes highly sophisticated if the nature of the plaintext prevents the attacker from predicting or estimating some packets. In previous work, the authors presented exhaustive experimental results to demonstrate the fact that it is not possible to deduce voice plaintext at encoder output, and hence it is not feasible to perform known plaintext/ciphertext attacks [6]. In these experiments, specialized hardware and software systems were used in order to investigate various realistic scenarios with variable environmental characteristics. The main purpose of the experiments which are further detailed in [7] was to measure the similarity between two instantaneously recorded sound files in an acoustically controlled environment and under different scenarios with respect to the position of the microphones.

The captured voice by the two microphones of the attacker and the victim were encoded with G.729 codec. Based on the fact that the encoder produces 10-byte frames, and instead of comparing the whole two files together, the two following methods are used to measure the similarity:

- One of the two binary files is broken into frames of 80 bits, and for each frame a sliding window with a size of 80 bits is shifted bit by bit through the other file. For every bit shift, a binary similarity coefficient is measured between the two 80-bit strings.
- The two binary files are broken into frames of 80 bits. Each frame is compared to all other frames in the second file.

Table 1 shows the average similarity measure values for both techniques and for all test cases specified in [6].

Table 1: Average percentage of similar bits

Technique	Average percentage of similar bits
Bit shift	50.3%
Frame shift	53%

We also calculated the average of the maximum similarity values for each of the cases and the results were very close to that of two randomly generated files as shown in Table 2.

Table 2: Average of maximum similarity measure

Technique	Recorded Files	Random Files
Bit shift	73.9%	73.75%
Frame shift	70%	67.5%

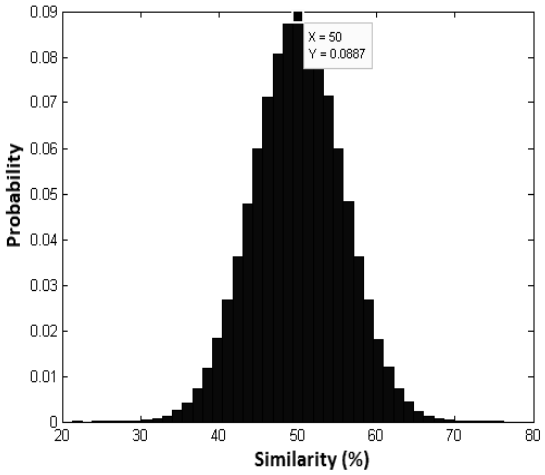


Figure 3: Similarity measures distribution of two random files

In addition to the statistical results and studies presented in [6], further analyses are performed based on the outcome of the previous experiment in this paper. The distribution plots for various scenarios are presented and analyzed. Because the distributions of similarity measures for all scenarios are almost identical to each other, we only include the normalized distribution plots of the similarity measures for three different scenarios including the case in which the victim's and attacker's microphones are at the same distance with angle 0, which is considered a worst case scenario. These distributions are depicted in Figure 3 and Figure 4. Based on the values and the figures presented, we can conclude that the similarity measures behave like a random variable with binomial distribution representing the discrete probability distribution of the number of matches in successive 80 independent Bernoulli trials with a probability of 0.5 for both match and mismatch. Therefore, this demonstrates that the two output files look almost like two randomly generated files.

In order to confirm that the results obtained are codec-independent, a similar procedure was performed using the "Speex" codec. Similar outcomes were obtained. It is expected that all CELP based encoders would provide similar results.

We have seen in [6] that introducing a natural silence of 10ms at the beginning of the conversation breaks the similarity. To study the worst case scenario, another test

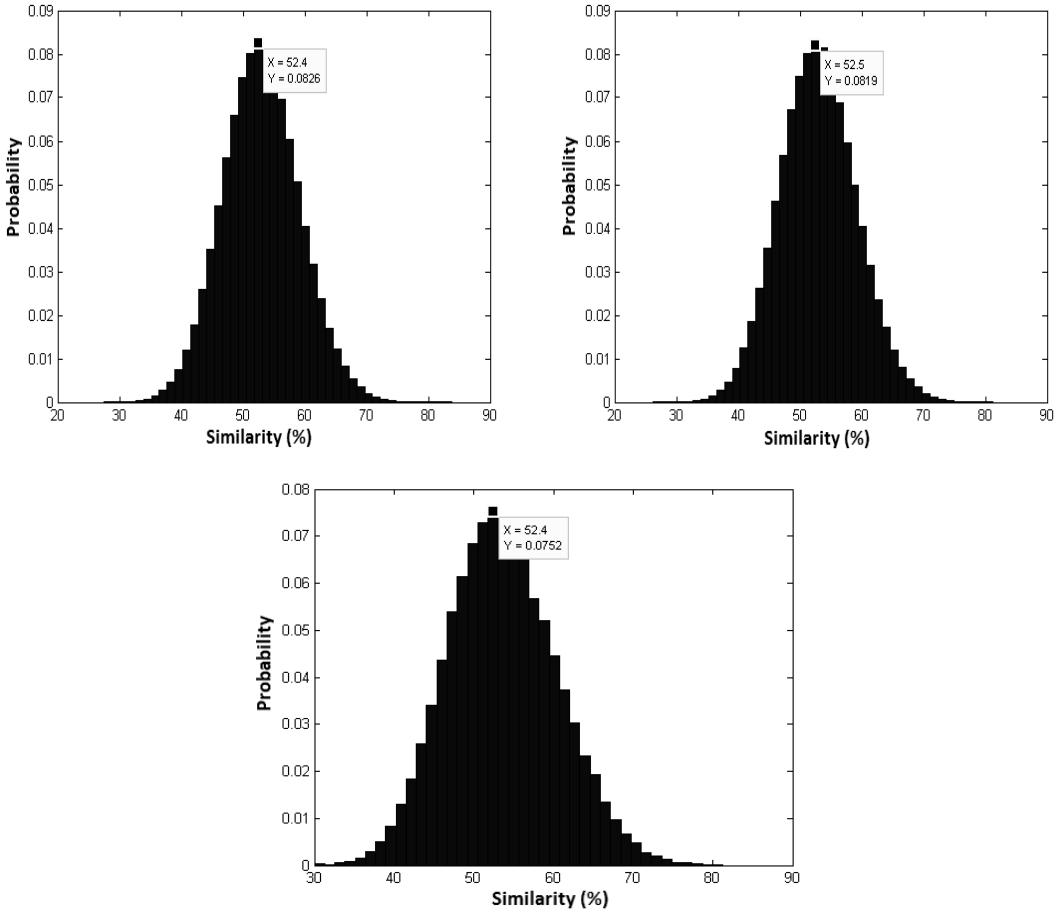


Figure 4: Similarity measures distribution of three different scenarios

was conducted by adding a frame of 160 bytes of 0s at the beginning of the recorded file and then measuring the similarity between the original and the modified one. The added bytes represent a single 10ms frame of speech at the beginning of the G.729 encoded file. After applying the same comparison methods, the results showed that adding just a 10ms of 0 bits to a file containing human speech is enough for the encoder to break the similarity and to reduce the maximum similarity value from 100% to 75.8% on average. A string of random bits instead of a string of 0s was also added at the beginning of the file and the maximum similarity was further reduced to 66.3%. It is also observed that for computer-generated sound, the longer the added string at the beginning of the file, the higher the reduction in the maximum similarity. It is believed that this is related to the fact that differential encoders reset variables in order to reduce the propagation of error after a given duration causing the 100% similarity for the frames occurring after this reset. This outcome is very important because it clearly demonstrates how a very simple modification in the original speech propagates and affects many subsequent frames. Therefore, if one of these 10ms frames exists at any location in the streams recorded by the two microphones, it would be practically impossible for an attacker to reproduce the exact bit stream.

Therefore, and quoting from [3], "It is difficult for an adversary to acquire the RTP plaintext data, since for many codecs, an adversary that does not know the input signal cannot manipulate the output signal in a controlled way. In many cases it may be difficult for the adversary to determine the actual value of the plaintext.", and from the results in [6] and the results presented in this paper, a strong case is made that it is not feasible for an attacker to perform known plaintext/ciphertext attacks due to the stochastic nature of the output of the codec. Nevertheless, the only threat model that affects the proposed algorithm from a confidentiality perspective is the ability of the attacker to successfully perform an attack by using the same exact input as the victim's. However, this requires direct physical access to the victim's device in order to record the conversation, which is assumed beyond the attacker model considered in this paper.

3.2.3 Group Size and Key Management Analysis

The lower bound for N, size of group used, is defined such that the ratio of time taken to encrypt N packets using SecVoIP to the time taken to encrypt N packets using SRTP is lower than a certain threshold. Let AES[S] be the time taken to encrypt a data block of size S bytes with AES and XOR[S] be the time taken to XOR two chains of size S bytes. The times needed to encrypt a group of N packets using SecVoIP ($\tau_{SecVoIP}$) and SRTP (τ_{SRTP}) are:

$$\tau_{SecVoIP} = \frac{AES[X+16-(X \bmod 16)] + 2N \times XOR(X)}{N} \quad (4)$$

$$\tau_{SRTP} = N \times \left[\frac{AES[X+16-(X \bmod 16)]}{N} + \frac{XOR(X)}{N} \right] \quad (5)$$

It is obvious that the size of the packet on which AES is performed is smaller than that in the previous E^2VoIP^2 since there is no additional padding of bytes. Let γ be the average time taken to XOR a packet of X bytes over the time taken to encrypt a packet with SRTP. The ratio of time taken by SecVoIP to the time taken by SRTP is given by:

$$\Omega = \frac{\tau_{SecVoIP}}{\tau_{SRTP}} = \frac{AES[X+16-(X \bmod 16)] + 2N \times XOR(X)}{N \times AES[X+16-(X \bmod 16)] + N \times XOR(X)} \quad (6)$$

$$\Rightarrow \frac{AES[X+16-(X \bmod 16)] + 2N \times XOR(X)}{N \times AES[X+16-(X \bmod 16)] + N \times XOR(X)} < \rho$$

$$\Rightarrow \frac{[AES(Z) + XOR(X)]}{\rho \times N \times [AES(Z) + XOR(X)]} + \frac{(2N-1) \times XOR(X)}{\rho \times N \times [AES(Z) + XOR(X)]} < 1$$

$$\Rightarrow \frac{1}{\rho \times N} + \frac{(2N-1) \times \gamma}{\rho \times N} < 1$$

$$\Rightarrow 1 + (2N-1) \times \gamma < \rho \times N$$

$$\Rightarrow N > \frac{1-\gamma}{\rho - 2\gamma} \quad (7)$$

The condition given in Equation (7) is experimentally validated in the subsequent sections. Although there is no certain upper bound for N, as we will see later, increasing N increases the efficiency of the proposed algorithm at the cost of generating the additional number of predefined keys needed for encryption. Comparing the time needed by SRTP and the time needed by SecVoIP in generating the required keys we can compute the additional key generation overhead incurred by SecVoIP.

Assuming that both the sender and the receiver share for every session a master key and a master salt, two 128-bit keys are generated: session key and session salt key, which are refreshed every ***R*** packets. SecVoIP requires ***N*** keys of X bytes in addition to these two session keys. These additional keys may also be refreshed every ***R*** packets. Let P_{SRTP} and $P_{SecVoIP}$ represent the time needed to generate the keys in SRTP and SecVoIP, respectively, for every ***R*** packet:

$$P_{SRTP} = 2 \times AES[16] \quad (8)$$

$$P_{SecVoIP} = 2 \times AES[16] + N \times AES[X-(X \bmod 16)] \quad (9)$$

Comparing Equations (8) and (9), the larger the number of packets in a group (N), the larger the key generation overhead of SecVoIP as compared to SRTP. This one time additional overhead is overcome by the gain acquired in the encryption process of every packet. The total time taken to encrypt R packets can be given by:

$$\tau'_{SRTP} \approx R \times AES[X+16-(X \bmod 16)] + R \times XOR(X) \quad (10)$$

$$\tau'_{SecVoIP} \approx Ceil\left(\frac{R}{N}\right) \times AES[X+16-(X \bmod 16)] + 2R \times XOR(X) \quad (11)$$

For R=N, there will be (N) AES operations in SRTP

and (N+1) AES operations in SecVoIP in total for every R packet. In this case, SRTP outperforms SecVoIP by one less AES operation which clearly indicates that R should be greater than N. In general, assuming that R is larger than N and that at least R packets are exchanged, the relation between ***R*** and ***N*** such that SecVoIP outperforms SRTP, can be derived as follows:

$$G = \tau'_{SRTP} - \tau'_{SecVoIP} - P_{SecVoIP} + P_{SRTP} > 0$$

$$\Rightarrow R \times AES[Z] + R \times XOR(X) - Ceil\left(\frac{R}{N}\right) \times AES[Z]$$

$$- 2R \times XOR(X) - N \times AES[Z] > 0$$

For simplicity, assume that, $XOR(X) = k \times AES[Z]$, where k < 1, therefore:

$$\Rightarrow R(1+k) - Ceil\left(\frac{R}{N}\right) - 2RK > N \quad (12)$$

Given that R and N are integer values, R can be written as:

$$R = qN + r \quad (13)$$

Substituting Equation (13) in (12):

$$\Rightarrow q > \frac{N + kr - r}{N - kN - 1}$$

Therefore, for $q = 1$, which represents the worst case scenario in terms of key generation cost:

$$\Rightarrow N + kr - r < N - kN - 1 \Rightarrow r > \frac{kN + 1}{1 - k} \quad (14)$$

$$\Rightarrow R > N + \frac{kN + 1}{1 - k} \quad (15)$$

Since XOR operation is negligible compared to AES, without loss of generality, Equation (14) after substituting *k=0* becomes:

$$\Rightarrow r > 1$$

The next possible positive integer for r is 2. As a result, in order to have a positive gain G, R should be greater than (N + 2). The previous analysis shows that increasing the number of packets per group increases the number of required predefined keys which in turn increases the key management overhead. However, this overhead is compensated for by the encryption process as long as the condition of Equation (14) is satisfied. When the rate of refreshing keys R=0, the keys are not refreshed. In this case, for SecVoIP to outperform SRTP, the number of exchanged packets should exceed N by 2, which is considered as a very relaxed condition.

The next section includes the implementation of the proposed algorithm along with experimental results that demonstrate the efficiency of the algorithm in terms of processing time and energy.

4 Implementation and Experimental Results

The prototype implementation of SecVoIP was done using Csipsimple [5], which relies on PJSIP [25], installed on a Samsung Nexus S smartphone running the Android 2.3 operating system. SRTP is used as the benchmark algorithm. PJSIP's SRTP implementation is used to calculate the processing time of SRTP encryption. In order to study the impact of having different number of packets per group on the efficiency of the algorithm, two group sizes, N=5 and N=15, are used. The analytical study previously presented regarding the group size is experimentally validated in this section.

First, the energy efficiency of SecVoIP over SRTP is demonstrated in terms of time consumption and number of CPU cycles which are directly related to the consumed energy. The outcomes are further validated through direct energy measurements performed on the Android phone. Note that the presented experimental results do not include the initial key generation cost, which was analyzed in the previous section. The cost of implementing several AES operations at the beginning of the session to generate the keys is very small compared to the cost of implementing AES to encrypt the large number of voice packets generated throughout the session.

4.1 PJSIP

PJSIP softphone is an open source application written in the C language and provides basic and advanced VoIP features [24]. PJMEDIA is a fully featured stack that controls the media component of PSJIP. PJMEDIA-CODEC contains a wide variety of well-known voice codecs such as G.711 (μ-law and a-law), G.722, GSM, and others that are integrated into PJMEDIA framework. Additionally, PJSIP provides SRTP functionality through the libsrtp() library. The SRTP module is plugged in between the stream block and the transport block. Csipsimple is a project relying on PJSIP to provide native SIP functionality for Android devices [5].

4.2 Time Consumption: Results and Analysis

Creighton et al. showed how energy consumption is directly related to the time taken to encrypt data using a certain security algorithm [18]. Similarly, Diaa et al. show how the packet size and the time consumed to encrypt this packet affect throughput and consumed energy. For the same packet size, higher encryption time results in lower throughput and higher energy consumption [10].

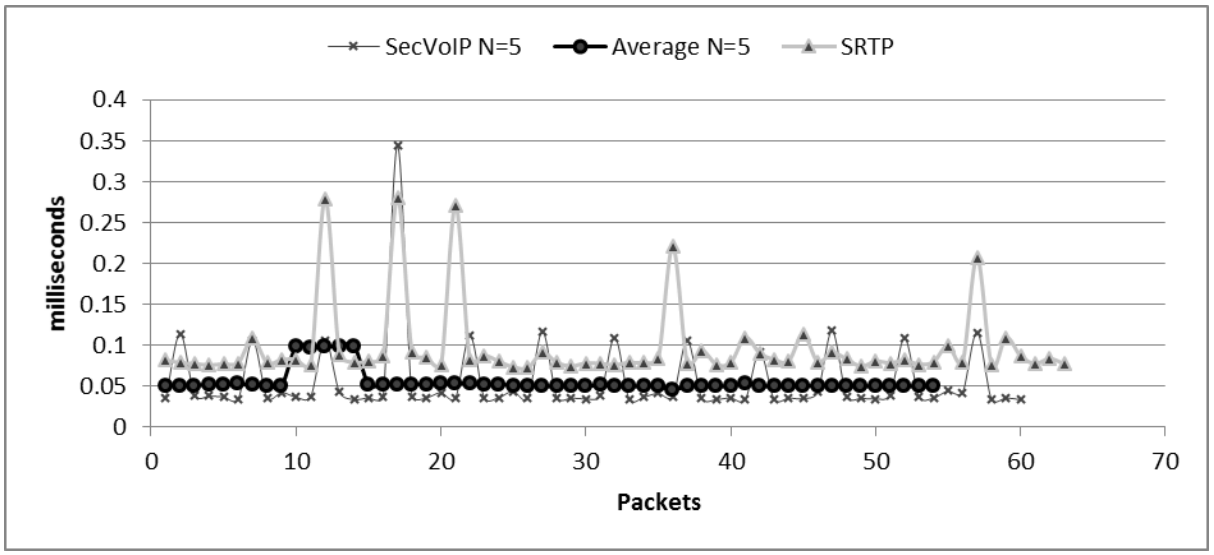


Figure 5: GSM encryption time in milliseconds for N=5

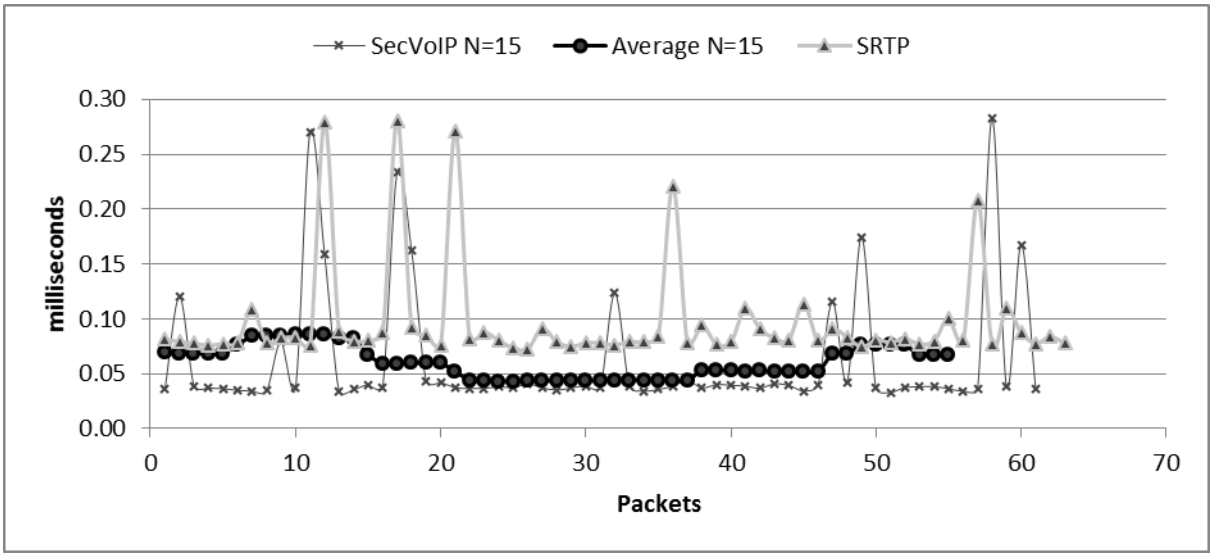


Figure 6: GSM encryption time in milliseconds for N=15

In order to calculate the time taken to encrypt a packet with SecVoIP and SRTP, timing markers were introduced into the code in order to calculate the processing time required by the encryption. For similar computations between SRTP and SecVoIP, i.e. AES counter mode, special care was taken to use identical functions in both algorithms such that we obtain as fair a comparison as possible. During the experiments, two types of codecs, G.722 and GSM, were used to investigate the relationship between the processing time and the payload size. The G.722 codec operates at 64 kbps and produces a payload of 160 bytes every 20ms, whereas the GSM codec produces 33 bytes of 20ms voice payload. For each codec, two group sizes were considered: N=5 and N=15. Because decryption in our algorithm for all possible N values works exactly the same way as encryption, only results for the encryption part are presented. It is worth mentioning that during the experiments, random spikes of up to 2 ms in the processing times appeared. These spikes are operating system related and are not specific to SecVoIP or SRTP. However, these spikes are all included in our figures and measurements.

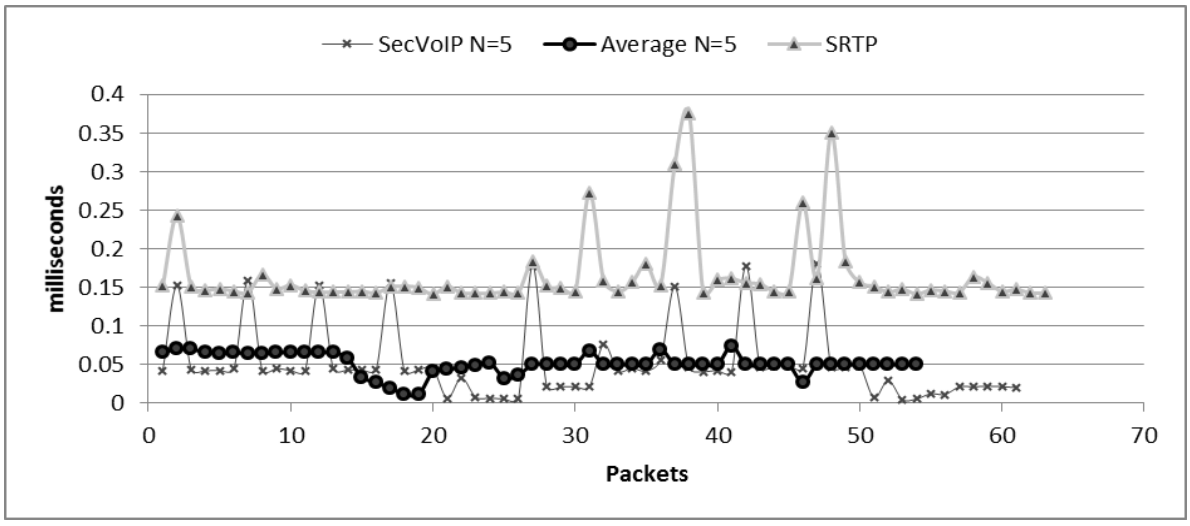


Figure 7: G.722 encryption time in milliseconds for N=5

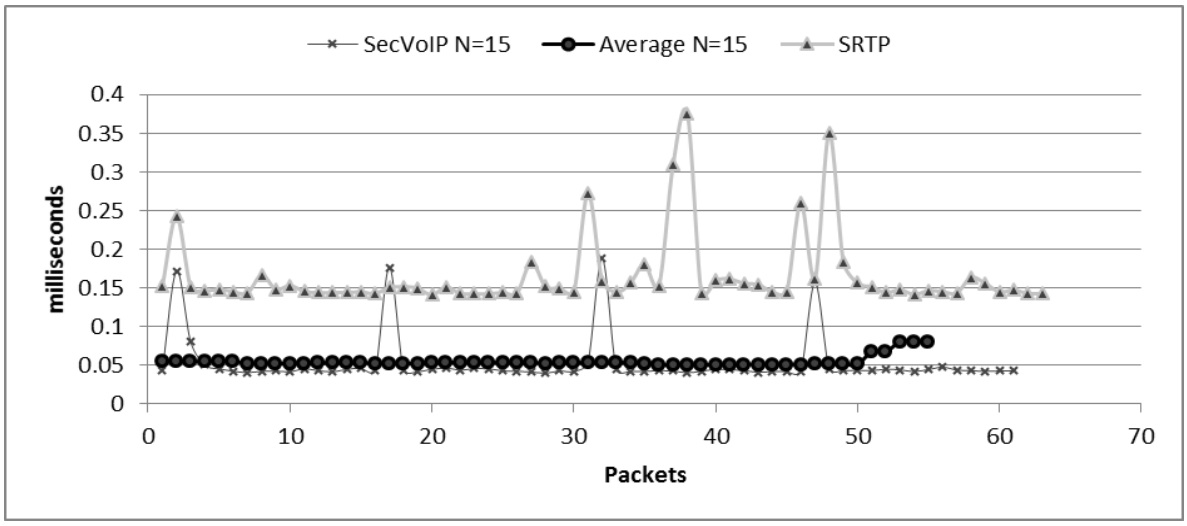


Figure 8: G.722 encryption time in milliseconds for N=15

Figure 5 and Figure 6 show the average processing time of SecVoIP for N=5 and N=15, respectively, for GSM-encoded packets. We can clearly notice the additional overhead added to the first packet of each group resulting from the generation of the pseudorandom sequence of X bytes. Results show that, on average, for 10 minutes of voice conversation, SecVoIP has 53% and 58% less operation time than that of SRTP for N=5 and N=15, respectively. Because the way SecVoIP encrypts the first packet of every group is similar to how SRTP encrypts each and every packet, they almost have identical processing times.

The same was done for packets encoded with G.722 codec. Figure 7 and Figure 8 represent the average processing time needed to encrypt G.722 encoded packets with SecVoIP and SRTP for N=5 and N=15, respectively. On average, SecVoIP is 58% faster than SRTP for N=5 and 83% faster for N=15.

Table 3 shows the smallest possible value for N obtained from the condition in Equation (7) for which γ is extracted from the plots. It illustrates the existing inverse relationship between N and Ω such that for a certain packet size, the higher the value of N, the lower the Ω ratio.

Based on the results presented above, it can be concluded that for the G.722 codec, SecVoIP outperforms SRTP in terms of processing time for the two group sizes, whereas for the GSM codec, the group size should be greater than 8.2. As analyzed previously, increasing the group size improves the efficiency over SRTP even further.

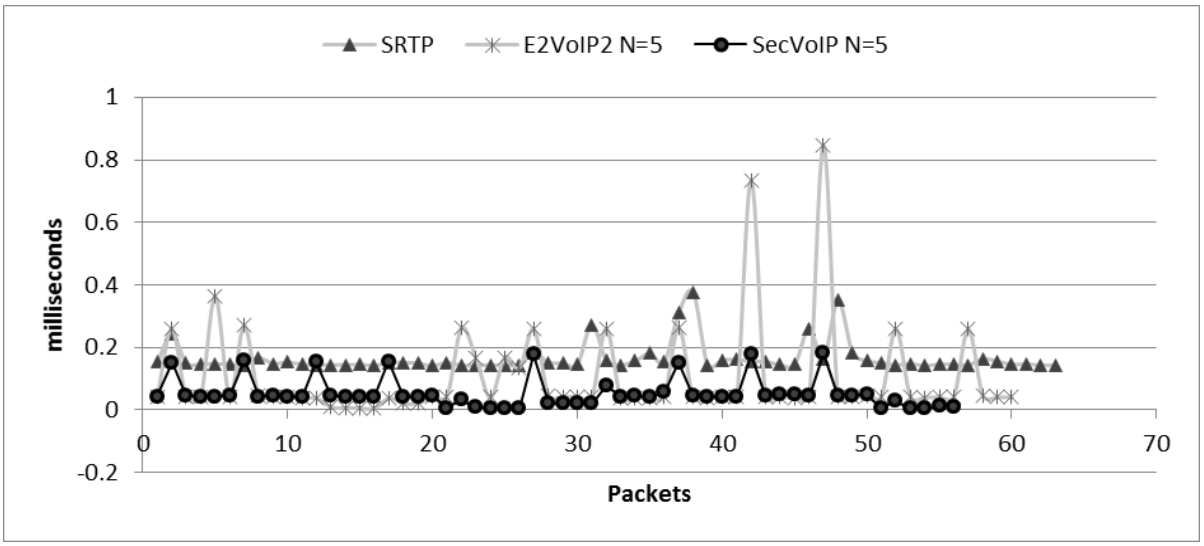


Figure 9: SecVoIP versus SRTP and E^2VoIP^2 for G.711 codec and N=5

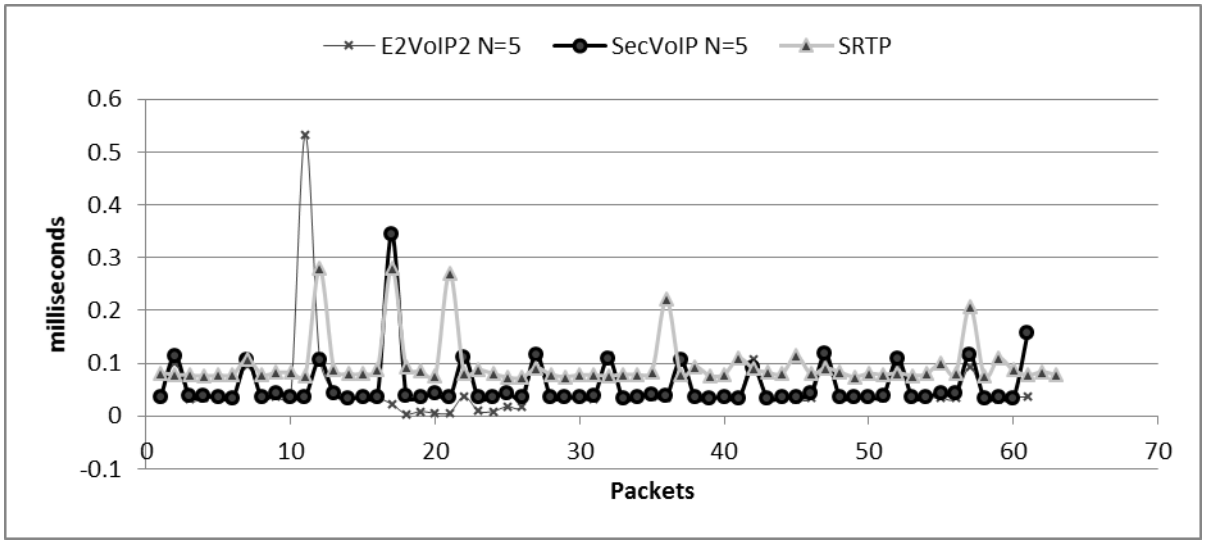


Figure 10: SecVoIP versus E^2VoIP^2 and SRTP for GSM codec and N=5

Table 3: Results in terms of different N Values

Codec	Packet Size "X"	N	Ω(N,X)	ρ(X)	γ(X)	η = (1-γ)/(ρ-2γ)
GSM	33	5	0.46	0.46	0.18	8.2
		15	0.42			
G.722	160	5	0.42	0.53	0.18	4.8
		15	0.208			

In order to compare the experimental results with those of the previous E^2VoIP^2 algorithm presented in [6], E^2VoIP^2 was also implemented on the same Android device. As a result, for G.711 codec, a significant decrease in the E^2VoIP^2 processing time in encrypting the first packet of each group is observed as depicted in Figure 9.

In E^2VoIP^2, AES was applied on a packet size of 320 bytes, which translated into twenty AES operations. In SecVoIP, on the other hand, AES-CM is used to generate a random sequence of 160 bytes, which requires 10 AES operations. In other words, the time needed to encrypt the first packet of each group in SecVoIP is half of that needed in E^2VoIP^2. However, the total operational time is not reduced exactly by 50% due to the additional XORs required by SecVoIP. On the other hand, for the GSM codec, and as is clear from Figure 10, the difference is hard to notice because in E^2VoIP^2 AES is applied on packets of size 64 bytes after padding, while in SecVoIP it is applied on packets of size 48 bytes.

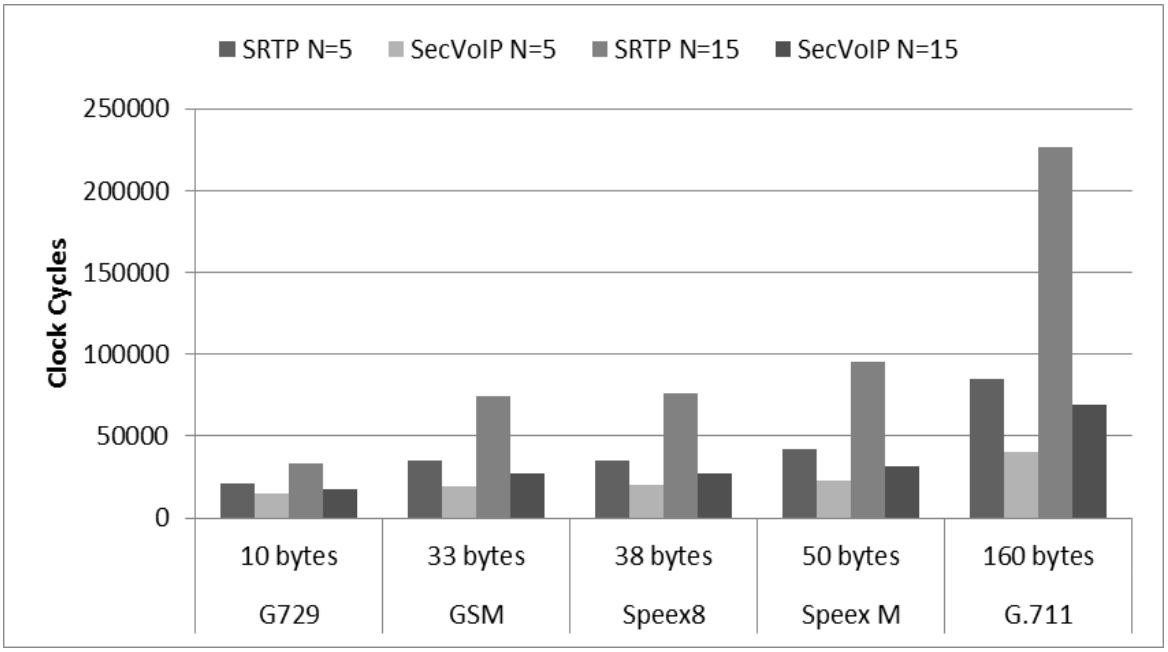


Figure 11: Number of CPU cycles for N=5 and N=15

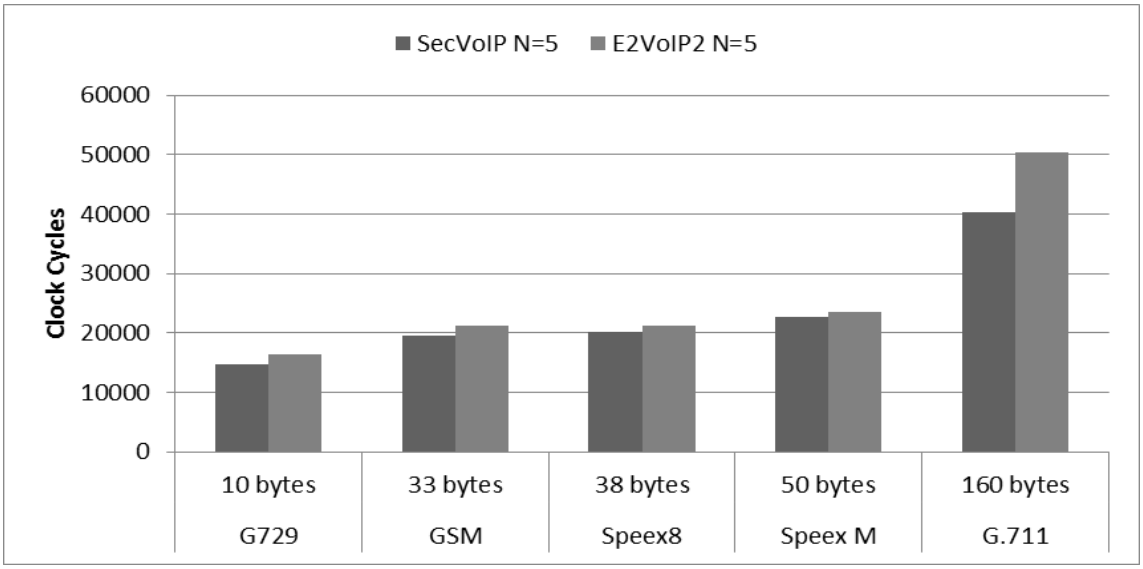


Figure 12: Number of CPU cycles for E^2VoIP^2 versus SecVoIP

4.3 CPU Cycles: Results and Analysis

Ruangchaijatupon et al. calculated the energy consumed by a cryptographic algorithm based on the number of the required CPU cycles. Researchers indicated that the consumed energy from any process is directly related to the CPU cycles consumed by the instructions of the corresponding process [23, 28].

To demonstrate the efficiency of our algorithm in terms of CPU cycles, we used PTLsim as a test bed in order to calculate the number of CPU cycles consumed during encryption. PTLsim is an accurate x86 microprocessor simulator, which is used to simulate x86 and x86-64 instructions [26]. An application was written in C++ to simulate SRTP and SecVoIP encryption. Various codec types are selected in order to cover a wide range of packet sizes. As in the previous section, two values for N were selected: 5 and 15.

Figure 11 depicts the number of CPU cycles required for different packet and group sizes and shows significant improvement of SecVoIP over SRTP. It also shows that the amount of savings is in a direct relation with the number of packets per group and packet size.

The ratios shown in Figure 11 differ from those presented in the previous figures mainly due to the dissimilarity of the processor model used (ARM versus X86). For the same reason stated previously, the savings in SecVoIP as compared to E^2VoIP^2 is of a greater significance for 160-byte data than the others, as shown in Figure 12. Nevertheless, both mechanisms show a great enhancement over SRTP.

4.3 Power Measurements

In order to demonstrate the energy efficiency of SecVoIP by means of real physical measurements, the same application developed in the previous section was compiled and deployed on the Samsung Nexus S Android phone.

A SIP server was used to create SIP accounts. The Android phone was assigned a SIP account, and a softphone was assigned another account. The goal was to measure the energy consumption on the Android phone when calls to the softphone, running on a desktop computer, were being made.

Three applications were installed on the Android phone; E^2VoIP^2, SecVoIP, and the original CSIPSimple application as downloaded from the PJSIP website. Experimental calls were made to measure the energy consumption when deploying E^2VoIP^2, SecVoIP and CSIPSimple with SRTP encryption enabled. During these calls the same audio snippet was played repeatedly.

Table 4: Energy measurements (Joules) for all cases

Codec	Packet Size (Bytes)	Algorithm	Energy (J)
GSM	33	SRTP	65
		E^2VoIP^2, N=5	52
		E^2VoIP^2, N=15	46
		SecVoIP, N=5	47
		SecVoIP, N=15	43
G.722	160	SRTP	171
		E^2VoIP^2, N=5	124
		E2VoIP2, N=15	119
		SecVoIP, N=5	123
		SecVoIP, N=15	103

In addition, the Android phone and the PC that has the softphone running were always kept at the same distance from each other and from the router. This was all done to ensure that the measurements were being recorded in a controlled environment. For every application, five 10-minute calls were made in a random order, and energy measurements were recorded using the PowerTutor application [15]. The results for all cases were then averaged and are displayed in Table 4.

The results clearly indicate that SecVoIP outperforms both E^2VoIP^2 and SRTP in terms of the consumed energy. For the case of GSM with N = 5, the percent improvement in energy consumption between SRTP encryption and SecVoIP is 28%, and is 34% for N = 15. For the case of G.722 and N = 5, the percent improvement is 28%, and increases to 40% for N = 15.

In order to translate these results into battery lifetime, we first measured the energy consumption of the Samsung Nexus S phone when in standby mode with the WiFi and 3G radios ON and the screen OFF. Table 5 lists the recorded standby energy values for several time intervals.

The standby energy for 30 minutes is 106 Joules, and the consumption is relatively linear with respect to time. For 60 minutes of standby time, the energy consumed according to our measurements should be around 212 J. This result agrees with those observed in [14] whereby researchers stated that the energy consumption of the Samsung Nexus S Android phone for one hour is 216 J when in standby.

Table 5: Possible values of N

Time (min)	Standby Energy (J)
5	22
10	37
15	56
20	71
25	89
30	106

To calculate the amount of standby time gained when using SecVoIP instead of SRTP, the following formula is applied:

$$\text{Gain in Standby Time} = \frac{(TalkTime) \times (Saved\ J/\min)}{(\text{Standby}\ Energy\ J/\min) = (3.5\ J/\min)}$$

According to [32], the typical AT&T customer averaged 21 minutes per day in the first quarter of the year 2011. For a talking time of only 21 minutes per day, the gain in extended standby and talk times when using SecVoIP as compared to SRTP are as shown in Table 6.

To generalize, the formulas in Table 7 can be used to calculate the extension of standby time and talk time for any value of the overall talk time per day.

Table 6: Saving values for the 21 minute/day case

Case	Savings (J/min)	Extension in standby time (min) per day	Extension in talk time (min) per day
GSM SecVoIP N=5	1.8	10.8	8.0
GSM SecVoIP N=15	2.2	13.2	10.7
G.722 SecVoIP N=5	4.8	28.8	8.2
G.722 SecVoIP N=15	6.8	40.8	13.9

4 Conclusions

The paper presented SecVoIP, which is a proposed algorithm to overcome several weaknesses that existed in previous algorithms to secure VoIP such as E^2VoIP^2. Eliminating the need to pad additional encryption-related information to the first packet of each group was the key

solution. SRTP was selected as the benchmark protocol due to its popularity and efficiency. The algorithm is secure as long as the attacker is incapable of deducing the original plaintext data. Several experiments were conducted in this context and invariably show that the stochastic nature of the codec output prevents the attacker from recovering the original plaintext data even when eavesdropping on the victim's conversation. The efficiency of the proposed mechanism over SRTP and over E^2VoIP^2 is demonstrated using three different experiments. The degree of improvement is dependent on the voice packet size and on the number of packets per group. Finally, experimental results showed that SecVoIP outperforms SRTP in terms of battery usage and talk time.

Table 7: General extension values

Case	Savings (J/min)	Extension in standby time (min)	Extension in talk time (min) per day
GSM SecVoIP N=5	1.8	0.514 x Talking Time	0.383 x Talking Time
GSM SecVoIP N=15	2.2	0.629 x Talking Time	0.512 x Talking Time
G.722 SecVoIP N=5	4.8	1.371 x Talking Time	0.390 x Talking Time
G.722 SecVoIP N=15	6.8	1.943 x Talking Time	0.660 x Talking Time

Acknowledgments

The authors would like to acknowledge the support of the Lebanese National Council for Scientific Research and the American University of Beirut University Research Board.

References

[1] A. L. Alexander, A. L. Wijesinha, and R. Karne, "An evaluation of secure real-time transport protocol (SRTP) performance for VoIP," in *Third International Conference on Network and System Security*, pp. 95-101, 2009.

[2] R. Barbieri, D. Bruschi, and E. Rosti, "Voice over IPsec: Analysis and solutions," in *Proceedings of the 18th Annual Computer Security Applications Conference*, pp. 261, 2002.

[3] M. Baugher, D. McGrew, M. Naslund, E. Carrara and K. Norrman, *The Secure Real-time Transport Protocol (SRTP)*, RFC 3711, Mar. 2004.

[4] D. Butcher, X. Li, and J. Guo, "Security challenge and defense in VoIP infrastructures," *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, vol. 37, no. 6, pp. 1152-1162, Nov. 2007.

[5] Csipsimple Group, *SIP Application for Android Devices*, 2012. (http://code.google.com/p/csipsimple/)

[6] E. A. Charanek, H. Dermanilian, Imad H. Elhajj, A. Kayssi, and A. Chehab, "E^2VoIP^2: Energy efficient voice over IP privacy," *International Journal of Computers and Security*, vol. 30, no. 8, pp. 815-829, Nov. 2011.

[7] A. H. Cheetham and J. E. Hazel, "Binary (presence-absence) similarity coefficients," *J. Paleontol*, vol. 43, pp. 1130-1136, 1969.

[8] S. Cherry, "Winner: Sprint's broadband gamble," *IEEE* Spectrum, Jan. 2008.

[9] E. Choo, J. Lee, H. Lee, and G. Nam, "SRMT: A lightweight encryption scheme for secure real-time multimedia transmission," *Multimedia and Ubiquitous Engineering*, pp. 60–65, 2007.

[10] S. E. Diaa, A. M. Hatem, and H. M. Mohty, "Evaluating the performance of symmetric encryption algorithms", *International Journal of Network Security*, vol. 10, no. 3, pp. 213-219, May 2010.

[11] W. B. Diab, S. Tohme, and C. Bassil, "VPN analysis and new perspective for securing voice over VPN networks," in *Fourth International Conference on Networking and Services*, pp. 73-78, 2008.

[12] A. Elbayoumy and S. Shepherd, "Stream or block ciphers for securing VoIP*?" International Journal of Network Security*, vol. 5, no. 2, pp. 128-133, 2007.

[13] J. François, R. State, T. Engel, and O. Festor, "Digital forensics in VoIP networks," *IEEE International Workshop on Information Forensics and Security*, pp. 1-6, 2010.

[14] Google Docs, *Nexus S Battery Drain Benchmark*, 2012. (https://docs.google.com/spreadsheet/ccc?key=0AntDDKv-lS6IdEY4T3dXWVFDWk9lREdJNGFfU2NwRlE#gid=0)

[15] M. Gordon, *A Power Monitor for Android-Based MobilePlatforms*, 2012. (http://ziyang.eecs.umich.edu/projects/powertutor/)

[16] M. Grangetto, E. Magli, and G. Olmo, "Multimedia selective encryption by means of randomized arithmetic coding," *IEEE Transactions on Multimedia*, vol. 8, no. 5, pp. 905-917, Oct. 2006.

[17] P. Gupta, V. Shmatikov, I. VMWare, and P. Alto, "Security analysis of voice-over-IP protocols," in *20th IEEE Computer Security Foundations Symposium*, pp. 49-63, 2007.

[18] C. T. Hager, S. F. Midkiff, J. M. Park, and T. L. Martin, "Performance and energy efficiency of block ciphers in personal digital assistants," in *Proceedings of the 3rd IEEE International Conference on Pervasive Computing and Communications*, pp. 127-136, 2005.

[19] J. K. Han, H. Y. Chang, S. Cho, and M. Park, "EMCEM: An efficient multimedia content encryption scheme for mobile handheld devices" in *International Conference on Information Science and Security*, pp. 108-114, Jan. 2008.

[20] K. Hong, S. Jung, L. L. Iacono, and C. Ruland, "Impacts of security protocols on real-time multimedia communications," *Information Security Applications*, pp. 1-13, 2005.

[21] S. Karapantazis and F. N. Pavlidou, "VoIP: A comprehensive survey on a promising technology," *Computer Networks*, vol. 53, pp. 2050-2090, 2009.

[22] D. R. Kuhn, T. J. Walsh, and S. Fries, "Security considerations for voice over IP systems," *NIST Special Publication*, pp. 800-858, 2005.

[23] National Institute of Standards and Technology, *Random Number Generation*, Computer Security Resource Center, 2011. (http://csrc.nist.gov/groups/ST/toolkit/rng/index.html)

[24] P. Prahithsangaree and P. Krishnamurthy, "Analysis of energy consumption of RC4 and AES algorithms in wireless LANs," in *IEEE Global Telecommunications Conference (GLOBECOM)*, vol. 3, pp. 1445-1449, 2003.

[25] B. Prijono, *Open Source SIP Stack and Media Stack for Presence*, 2011. (http://www.pjsip.org)

[26] PTLsim, *x86-64 Cycle Accurate Processor Simulation Design Infrastructure*, 2012. (http://www.ptlsim.org)

[27] D. Qiao, M. Gursoy, and S. Velipasalar, "Secure wireless communication and optimal power control under statistical queuing constraints," *Information Forensics and Security, IEEE Transactions on*, no. 99, pp. 628-639, 2011.

[28] N. Ruangchaijatupon and P. Krishnamurthy, "Encryption and power consumption in wireless LANs," in *Third IEEE Workshop on Wireless LANs, Newton*, pp. 27-28, Massachusetts, Sep. 27-28, 2001.

[29] A. Servetti and J. C. De Martin, "Perception based selective encryption of G.729 speech," in *IEEE International Conference on Acoustics, Speech, and Signal Processing*, vol. 1, pp. I-621-I-624, 2002.

[30] A. Servetti, C. Testa, and J. C. De Martin, "Frequency selective partial encryption of compressed audio," in *Proceedings of CASSP*, pp. 668-671, 2003.

[31] Thermos and A. Takanen, *Securing VoIP Networks: Threats, Vulnerabilities, and Countermeasures*, Addison-Wesley Professional, USA, Aug. 2007.

[32] S. Woolley, *Cell phone use is way up. So why did brain cancer rates fall?*, CNN, 2012. (http://tech.fortune.cnn.com/2011/06/07/cell-phone-use-is-way-up-so-why-are-brain-cancer-rates-down/)

[33] D. Xie and C. C. J. Kuo, "Multimedia data encryption via random rotation in partitioned bit streams," *IEEE International Symposium on Circuits and Systems*, vol. 6, pp. 5533-5536, May. 2005.

[34] M. Wu and Y. Mao, "Communication friendly encryption of multimedia," in *IEEE Workshop on Multimedia Signal Processing*, pp. 292-295, Dec. 2002

.

Hoseb Dermanilian received the BE degree with high distinction in Electric and Computer Engineering from Aleppo University in 2009. He holds a Masters in Engineering degree from the American University of Beirut, his research interests are in the field of computer and communications networks with emphasis on communications security, VoIP security, energy efficient security, and has to date published one paper in energy aware computing. He is currently working as an ICT Project Engineer in an Airport Expansion Project leading Computing and Storage System.

Farah Saab received the BE degree in Electrical and Computer Engineering in 2011 from the American University of Beirut (AUB). She is currently a graduate research assistant at AUB and part of the Middle East Energy Efficiency Research project. Her main research interests include energy efficient computing as well as networks and security.

Imad H. Elhajj received his Bachelor of Engineering in Computer and Communications Engineering, with distinction, from the American University of Beirut in 1997 and the M.S. and Ph.D. degrees in Electrical Engineering from Michigan State University in 1999 and 2002, respectively. He is currently an Associate Professor with the Department of Electrical and Computer Engineering at the American University of Beirut. Dr. Elhajj is the vice-chair of IEEE Lebanon Section, senior member of IEEE and senior member of ACM. His research interests include instrumentation and robotics, cyber security, sensor and computer networks, and multimedia networking with more than 100 publications. Imad received the Most Outstanding Graduate Student Award from the Department of Electrical and Computer Engineering at Michigan State University in April 2001, the Best Paper award at the IEEE Electro Information Technology Conference in June 2003, and the Best Paper Award at the International Conference on Information Society in the 21st Century in November 2000. Dr. Elhajj is recipient of the Teaching Excellence Award at the American University of Beirut, June 2011.

Ayman Kayssi was born in Lebanon. He studied electrical engineering and received the BE degree, with distinction, in 1987 from the American University of Beirut (AUB), and the MSE and PhD degrees from the University of Michigan, Ann Arbor, in 1989 and 1993, respectively. He received the Academic Excellence Award of the AUB Alumni Association in 1987. In 1993, he joined the Department of Electrical and Computer Engineering (ECE) at AUB, where he is currently a full professor. In 1999-2000, he took a leave of absence and joined Transmog Inc. as chief technology officer. From 2004 to 2007, he served as chairman of the ECE Department at AUB. He teaches courses in electronics and in networking, and has received AUB's Teaching Excellence Award in 2003. His research interests are in information security and networks, and in integrated circuit design and test. He has published more than 165 articles in the areas of VLSI, networking, security, and engineering education. He is a senior member of IEEE, and a member of ACM, ISOC, and the Beirut OEA.

Ali Chehab received his Bachelor degree in EE from AUB in 1987, the Master's degree in EE from Syracuse University in 1989, and the PhD degree in ECE from the University of North Carolina at Charlotte, in 2002. From 1989 to 1998, he was a lecturer in the ECE Department at AUB. He rejoined the ECE Department at AUB as an Assistant Professor in 2002 and became an Associate Professor in 2008. He received the AUB Teaching Excellence Award in 2007. He teaches courses in Programming, Electronics, Digital Systems Design, Computer Organization, Cryptography, and Digital Systems Testing. His research interests include: Wireless Communications Security, Cloud Computing Security, Multimedia Security, Trust in Distributed Computing, Low Energy VLSI Design, and VLSI Testing. He has about 130 publications. He is a senior member of IEEE and a member of ACM.

Ciphertext-Auditable Identity-based Encryption

Changlu Lin[1], Yong Li[2], Kewei Lv[3], and Chin-Chen Chang[4,5]
(Corresponding author: Chin-Chen Chang)
Fujian Province Key Laboratory of Network Security and Cryptology & Fujian Normal University[1]
Fuzhou 350007, China
Key Laboratory of Communication & Information Systems (Beijing Jiaotong University)[2]
Beijing Municipal Commission of Education, Beijing 100044, China
State Key Laboratory of Information Security, Institute of Information Engineering, CAS [3]
Beijing 100049, China
Department of Information Engineering and Computer Science& Feng Chia University [4]
Taichung 40724, Taiwan
Department of Computer Science and Information Engineering& Asia University [5]
Taichung, 41354, Taiwan
(Email: alan3c@gmail.com)
(Received Aug. 28, 2013; revised and accepted Nov. 6, 2013)

Abstract

Ciphertext-auditability of public key encryption scheme means that the ciphertext should been verified by anyone whether it was actually created by the public key. It also should satisfy two additional requirements: 1) no adversary can create a valid-looking ciphertext and then it can pass the verification process together with a public key and a plaintext; 2) the plaintext cannot be revealed from ciphertext without the help of the correct private key. This paper, in the first time, proposes an ciphertext-auditable identity-based encryption. Our scheme doesn't need the certificates and the sender can directly encrypt message via using the identity without the progress of public key authentication. Furthermore, the proposed scheme is provably secure under the standard model against the k-resilient ciphertext-auditability.

Keywords: Ciphertext-auditability, identity based encryption, public key cryptography

1 Introduction

In current information age, many companies, e.g., Bank (some critical business data), have the number of very important personal information (**PI**), such as the personal consumption information of some productions, customer and account information of the bank, etc. The company may use them for various purposes, including adverting, marketing, etc. Furthermore, if the **PI** is leaked by the malicious employees, then it would cause great losses for the company. Usually, there are two ways against this leakages from insiders: *network security* and *physical security* [8]. When the company wants to store the **PI** in secure warehouse, the company duplicates the **PI** and saves it to backup tape, and then the company requires a transport service (**TS**) to deliver this tape to a secure warehouse. During the transiting, the backup tape may be lost and potentially give out to outsiders. To avoid this kind of potential leakages, the encryption technique is used and the company encrypts the **PI** before copying it to backup tape.

Hada and Sakurai [8] observed that it could *not* prevent the potential attack by using the traditional encryption technique. They introduced an *auditor* who ensured that the message is encrypted by a correct public key, and showed that the backup operation done by the following three entities:

- *Backup manager* (BM): Backup manager does the management service for enterprise-wide backup. Usually, BM needs to inform every department to backup the **PI** data periodically and then deliveries the message to a secure warehouse under the corporate backup policy. In addition, all encryption keys are managed by BM.
- *Operator* (O): Operator holds the **PI** databases in a department and encrypts them via a public key before duplicating the data to the backup tape.
- *Auditor* (A): Auditor is in some same department as the operator and audits the backup tape and ensures that the encrypted message is encrypted by the correct public key.

Ciphertext-Auditable Public Key Encryption. Hada and Sakurai [8] presented the concept of ciphertext-

auditable public key encryption, denoted by CA-PKE, to capture the above scenarios, such as backup the very important personal information in the company. They described the general scenario via the public key encryption, and this case should satisfy two special requirements: *verifiability* and *unforgeability* (see Def. 1). Furthermore, a CA-PKE scheme has four steps as follows: 1) BM makes a backup request in an authenticated way and sends a public key to both O and A; 2) O encrypts the **PI** under the public key and duplicates this encrypted message to a backup tape; 3) A audits this backup tape and verifies whether O encrypted the **PI** by the correct public key or not. Furthermore, the audit should ensure that the message cannot be recovered, even if O is malicious, from the backup tape without the help of the corresponding private key; 4) O requires the **TS** to delivery the backup tape to a secure warehouse after it passes the audit. Hada and Sakurai [8] proposed a general CA-PKE with random oracle assumption. There are some cryptographic tools, such as non-interactive zero-knowledge (NIZK) proof of knowledge together with a trapdoor one-way permutation, are used in the concreted construction. Actually, their proposed scheme is a modification of the encryption scheme which is presented by Bellare and Rogaway [2]. Recently, Lin and Liu [9] proposed a ciphertext-auditable public key encryption scheme based on the Paillier's cryptosystem and is secure under the standard model.

Identity-based Encryption. Identity-based encryption [3, 11], denoted by IBE, is a public key encryption scheme and the encryption key is an arbitrary string, e.g., the receiver's unique email address or telephone number. The Private Key Generator (PKG) generates the user's private key via using its master key after the user authenticates itself. Public key certificates and certificate authorities don't be required any more in the IBE scheme. It simplifies public key and the certificate management, that is, such scheme eliminates certificates and the sender could just encrypt the message by using the receiver identity as the public key. In 2001, Boneh and Franklin [3] proposed the first secure and practical IBE scheme based on the pairing. Their scheme is provable security under the random oracle model. After that, many IBE schemes are proposed based on the pairing [5, 10, 12] or lattice [7].

Our Contributions. This paper, in first time, proposes cipertext-auditable identity-based encryption (CA-IBE). Our proposed CA-IBE scheme also has four steps and satisfies the additional two properties of *verifiability* and *unforgeability* as the CA-PKE scheme proposed by Hada and Sakurai [8]. In the second step, it requires t ($t \geq 2$) operators who encrypt the **PI** together and requires at least one operator is honest. Our main contributions are as follows.

- In the CA-IBE scheme, it only requires that the BM sends a backup request to both O and A by authenticated way and does *not* need the public key authentication in the first step;
- In the CA-IBE scheme, the operator O can encrypt the **PI** before receiving the backup request and duplicates the ciphertext to backup tape right now after getting the backup request;
- Our proposed scheme satisfies the provable security under the standard model against the k-resilient ciphertext-auditability.

2 Preliminaries

This section recalls some notations, the formal definition of the identity based encryption, and also gives the formal definition of the ciphertext-auditable identity-based encryption.

Some Notations. Assume $\mathcal{A}$ is a probabilistic algorithm and $\mathcal{A}(x_1, \ldots, x_n; r)$ is the output result of $\mathcal{A}$ on input $(x_1, \ldots, x_n)$ and coins r. Assume $y \leftarrow \mathcal{A}(x_1, \ldots, x_n)$ is an experiment of picking r randomly, and y is $\mathcal{A}(x_1, \ldots, x_n; r)$. If S is a finite set, $x \xleftarrow{R} S$ is the operation of choosing an element from S uniformly. Assigning a value α to a variable x will be denoted by $x \leftarrow \alpha$. Let $S, T, \ldots$, denote probability spaces, and then let $\Pr[x \leftarrow S; y \leftarrow T; \ldots : p(x, y, \ldots)]$ denote the probability where the predicate $p(x, y, \ldots)$ is true if the experiments, $x \leftarrow S; y \leftarrow T; \ldots$, are executed correctly and in order. Function $f : \mathbb{N} \rightarrow \mathbb{R}^+$ is a function and it is *negligible* in k if for any real number $c > 0$, there exists $k_0 \in \mathbb{N}$ such that for any k and $k > k_0$, then have $f(k) \leq (\frac{1}{k})^c$, where $\mathbb{R}^+ := \{x \in \mathbb{R} | x > 1\}$. PPTM stands for "probabilistic polynomial time machine" and PSCF means "polynomial-size circuit family". If $\{D_n\}$ is probability distribution ensemble and the largest probability of an element, that is, $\max_v \Pr[x \leftarrow D_n : x = v]$, is negligible in n [6], then call that a $\{D_n\}$ is *well-spread*.

Identity-based Encryption. An identity-based encryption (IBE) scheme is consisted by following four algorithms: **Setup**, **Key Generation**, **Encryption**, **Decryption**, they denoted by $\mathcal{IBE} = (\mathcal{S}, \mathcal{K}, \mathcal{E}, \mathcal{D})$:

- *Setup* ($\mathcal{S}$): it is the setup algorithm and takes the security parameter $k \in \mathbb{N}$ as input, and this algorithm outputs the system parameters **params** and the master-key **mk**. Usually, the system parameters are all description of the message and ciphertext space $\mathcal{M}$ and $\mathcal{C}$ respectively. Intuitively, **params** is known publicly, while **mk** is the secret key of the PKG.
- *Key Generation* ($\mathcal{K}$): it is the extraction algorithm and takes **params**, **mk**, and an arbitrary **ID** $\in \{0,1\}^*$ as inputs, and this algorithm outputs $d_{\mathbf{ID}}$ as

the private key for the identity **ID**. Here **ID** is a public key, and $d_{\mathbf{ID}}$ is the corresponding private key.

- *Encryption* ($\mathcal{E}$): it is the encryption algorithm and takes **params**, **ID**, and one plaintext M from message space $\mathcal{M}$ as inputs, and then this algorithm outputs the ciphertext $C \in \mathcal{C}$.
- *Decryption* ($\mathcal{D}$): it is the decryption algorithm and takes **params**, one ciphertext C from message space $\mathcal{C}$ and one $d_{\mathbf{ID}}$ as inputs, and then this algorithm outputs the message $M \in \mathcal{M}$ as the corresponding plaintext.

The above algorithms should satisfy the constraint of consistency. That is, the following equation holds if $d_{\mathbf{ID}}$ is the correct private key created from the extraction algorithm $\mathcal{K}$ which is run **ID** as input, and for any message $M \in \mathcal{M}$:

$\mathcal{D}(\mathbf{params}, C, d_{\mathbf{ID}}) = M$, where $C = \mathcal{E}(\mathbf{params}, \mathbf{ID}, M)$.

Definition of Ciphertext-Auditable Identity-based Encryption. As the ciphertext-auditable public key encryption is defined in [8], the ciphertext-auditable identity-based encryption is defined as follows:

Definition 1 (CA-IBE) *An identity-based encryption scheme $\mathcal{IBE} = (\mathcal{S}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is ciphertext-auditable if it satisfies two properties:*

- ***Verifiability:*** *There is a PPTM verification algorithm, $\mathcal{CV}$, such that, for each message M from the space $\{0,1\}^*$, then have*

$$Pr\begin{bmatrix}(\mathbf{ID}, d_{\mathbf{ID}}) \leftarrow \mathcal{K}(\mathbf{params}, \mathbf{mk});\\ (C, p) \leftarrow \mathcal{E}(M, \mathbf{ID}) :\\ \mathcal{CV}(C, \mathbf{ID}, p) = \mathbf{Accept}\end{bmatrix} = 1.$$

- ***Unforgeability:*** *Given each pair of non-uniform PSCFs as $< \mathcal{A}^e, \mathcal{A}^d >=< \{\mathcal{A}_n^e\}, \{\mathcal{A}_n^d\} >$, and each well-spread distribution $\mathcal{X}(1^k)$, then have*

$$Pr\begin{bmatrix}(\mathbf{ID}, d_{\mathbf{ID}}) \leftarrow \mathcal{K}(\mathbf{params}, \mathbf{mk});\\ M \leftarrow \mathcal{X}(1^k); (C, p) \leftarrow \mathcal{A}_n^e(M, \mathbf{ID}) :\\ \mathcal{CV}(C, \mathbf{ID}, p) = \mathbf{Accept},\ \mathcal{A}_n^d(C, \mathbf{ID}) = M\end{bmatrix},$$

is negligible in n.

In the real scenario, adversaries $\mathcal{A}^e$ and $\mathcal{A}^d$ are the malicious operator and transport service respectively, and p is the proof string.

To analyze our proposed scheme, a stronger notion than the ciphertext-auditability as above definintion should be defined, called *k-resilient* ciphertext-auditability. This notion satisfies the *verifiability* and *k-unforgeability*. The property of k-unforgeability means that there are at most l ($l \leq k-1$, and $k \geq 2$) malicious encryption adversaries $\mathcal{A}^e$ (malicious operators) in the unforgeability notion. In other words, the k-resilient ciphertext-auditability implies that the scheme can pass the verification even there are l malicious operators in the scenario which includes the k operators.

Mix strategy is the generalization of the semi-honest strategy introduced by Hada and Sakurai [8]. There are two settings, the *real* setting and the *ideal* setting, in the mix strategy. In the *real* one, there exist some (but not all) malicious encryption adversaries which could make some modifications on the message and choose some fixed numbers as the randomized inputs in the encryption progress, while all encryption adversaries are honest in the *ideal* one. The gaps between the probabilities which the decryption adversaries obtain messages in the two settings should be considered. The formal definition of the mix strategy is as follows:

Definition 2 (Mix Strategy) *It says that a standard IBE scheme $\mathcal{IBE} = (\mathcal{S}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ satisfies the secure property of the mix strategy if, for each pair of non-uniform PSCFs as $< \mathcal{F}, \mathcal{DA} >=< \{\mathcal{F}_n\}, \{\mathcal{DA}_n\} >$, and each well-spread distribution $\mathcal{X}(1^k)$, for the set $X \subset \{1, 2, \ldots, k\}$, we set the subset Y is $\{1, 2, \ldots, k\} - X$, then the following function*

$$Pr\begin{bmatrix}(\mathbf{ID}, d_{\mathbf{ID}}) \leftarrow \mathcal{K}(\mathbf{params}, \mathbf{mk}); M \leftarrow \mathcal{X}(1^k);\\ (M', r_1, \ldots, r_{|X|}) \leftarrow \mathcal{F}_n^X(\mathbf{ID}, M);\\ (r_{|X|+1}, \ldots, r_k) \leftarrow_R \mathcal{F}_n^Y(\mathbf{ID});\\ C = \mathcal{E}(\mathbf{ID}, M'; r') : \mathcal{DA}_n(\mathbf{ID}, C) = M\end{bmatrix}$$

$$-Pr\begin{bmatrix}(\mathbf{ID}, d_{\mathbf{ID}}) \leftarrow \mathcal{K}(\mathbf{params}, \mathbf{mk}); M \leftarrow \mathcal{X}(1^k);\\ (r_1, r_2, \ldots, r_k) \leftarrow_R \mathbf{coins}; C = \mathcal{E}(\mathbf{ID}, M; r) :\\ \mathcal{DA}_n(\mathbf{ID}, C) = M\end{bmatrix},$$

is negligible for n, where $r' = \sum_{i=1}^{|X|} r_i + \sum_{j=|X|+1}^{k} r_j$ and $r = \sum_{i=1}^{k} r_i$. And the set X is the set of all malicious encryptors, while Y is the set of all honest encryptors.

The reader is referred to reference [5] for the standard security notions and models for identity-based encryption, such as IND-ID-CPA and IND-ID-CCA.

3 Cipertext-Auditable Identity-based Encryption (CA-IBE)

This section constructs a CA-IBE scheme, denoted by $\mathcal{CA}$-$\mathcal{IBE}$, without random oracles. There are k encryptors in our scheme, and anyone who picks randomized input itself encrypts the ciphertext from the former encryptors. In addition, our scheme assumes all encryptors must join in the encryption progress.

Assume $\mathbb{G}$, $\mathbb{G}_1$ are the group with prime order p and g is a generator for group $\mathbb{G}$; the function $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_1$ is a bilinear map. All public parameters are similar with in the other IBE scheme in [5].

Initialization. Select t-length vector $X = (x_i) \in \mathbb{Z}_p^t$ and compute $Y = (y_i) = (g^{x_i}) \in \mathbb{G}^t$, where x_i and y_i is the

private key and the public key for the i-th encryptor respectively.

Setup. The PKG selects a random secret integer $\alpha \in \mathbb{Z}_p$ and $g \in \mathbb{G}$ as a random generator. PKG computes $g_1 = g^\alpha$ and choose a random g_2 from $\mathbb{G}$. Furthermore, PKG picks randomly a value $u' \in \mathbb{G}$ and a n-length vector $U = (u_i) \in \mathbb{G}^n$. Then, the public parameters **params** and the private master-key **mk** are as follows.

$$\textbf{params} = (g, g_1, g_2, u', U),\ \textbf{mk} = g_2^\alpha.$$

Key Generation. Assume $\textbf{ID} = (v_1, \ldots, v_n)$ from $\{0,1\}^n$ is a bit string, and $\mathcal{V} = \{i | v_i \neq 1\} \subseteq \{1, \ldots, n\}$. The PKG picks a random number $r_{\textbf{ID}}$ from $\mathbb{Z}_p$ and generates $d_{\textbf{ID}}$ for identity **ID** via using the master key as below:

$$d_{\textbf{ID}} = (d_1, d_2) = (g_2^\alpha \cdot (u' \prod_{i \in \mathcal{V}} u_i)^{r_{\textbf{ID}}}, g^{r_{\textbf{ID}}}). \quad (1)$$

Encryption. This algorithm encrypts any message M from $\mathbb{G}_1$ for a receiver $\textbf{ID} \in \{0,1\}^n$, set $h = u' \prod_{i \in \mathcal{V}} u_i$, the k encryptors choose $r_j \in_R \mathbb{Z}_p$ randomly and independently, where $j = 1, \ldots, k$. So the ciphertext is

$$C = (C_0, C_1, C_2; T) = (M \cdot e(g_1, g_2)^r, g^r, h^r; (h^i)). \quad (2)$$

Here, the k encryptors compute as follows:

$$\begin{aligned}
&(C_0^0, C_1^0, C_2^0; T_0)\\
&= (M \cdot e(g_1, g_2)^{r_0 x_0}, g^{r_0 x_0}, h^{r_0 x_0}; h^{r_0})\\
&= (M \cdot 1, 1, 1; 1, 1),\\
&(C_0^1, C_1^1, C_2^1; T_1)\\
&= (C_0^0 \cdot e(g_1, g_2)^{r_1 x_1}, C_1^0 \cdot g^{r_1 x_1}, C_2^0 \cdot h^{r_1 x_1}; (h^{r_0}, h^{r_1}))\\
&= (M \cdot e(g_1, g_2)^{r_0 x_0 + r_1 x_1}, g^{r_0 x_0 + r_1 x_1}, h^{r_0 x_0 + r_1 x_1}; (h^{r_0}, h^{r_1})),
\end{aligned}$$

$$\vdots$$

$$\begin{aligned}
(C_0^i, C_1^i, C_2^i; T_i) =& (C_0^{i-1} \cdot e(g_1, g_2)^{r_i x_i}, C_1^{i-1} \cdot g^{r_i x_i},\\
& C_2^{i-1} \cdot h^{r_i x_i}; (h^{r_0}, \ldots, h^{r_i}))\\
=& (M \cdot e(g_1, g_2)^{\sum_{j=1}^{i} r_j x_j}, g^{\sum_{j=1}^{i} r_j x_j},\\
& h^{\sum_{j=1}^{i} r_j x_j}; (h^{r_0}, \ldots, h^{r_i})),
\end{aligned}$$

$$\vdots$$

$$\begin{aligned}
(C_0^k, C_1^k, C_2^k; T_k) =& (C_0^{k-1} \cdot e(g_1, g_2)^{r_k x_k}, C_1^{k-1} \cdot g^{r_k x_k},\\
& C_2^{k-1} \cdot h^{r_k x_k}; (h^{r_0}, \ldots, h^{r_k}))\\
=& (M \cdot e(g_1, g_2)^{\sum_{j=1}^{k} r_j x_j}, g^{\sum_{j=1}^{k} r_j x_j},\\
& h^{\sum_{j=1}^{k} r_j x_j}; (h^{r_0}, \ldots, h^{r_k}))\\
=& (M \cdot e(g_1, g_2)^r, g^r, h^r; (h^{r_0}, \ldots, h^{r_k}))\\
\triangleq& (C_0, C_1, C_2; T) = C,
\end{aligned}$$

where $r = \sum_{j=1}^{k} r_j \in_R \mathbb{Z}_p$, and $x_0 = 0$, $r_0 = 0$. Note that the k encrypters are the k operators in the scenario respectively, and the last encrypter is responsible to send the encrypted message to backup. Usually, there is an honest encrypter at least among the k encrypters.

Audit. When the auditor A reads the ciphertext C from backup tape, he/she computes $h = u' \prod_{j \in \mathcal{V}} u_j$ and checks

$$e(C_1, h) =^? e(y_1, t_1) e(y_2, t_2) \cdot \cdots \cdot e(y_t, t_k),$$

where $C_1 = g^{\sum_{j=1}^{k} r_j x_j}$, and $T = (t_1, t_2, \ldots, t_k) = (h^{r_1}, h^{r_2}, \ldots, h^{r_k})$. That is,

$$e(g^{\sum_{j=1}^{k} r_j x_j}, h) =^? \prod_{j=1}^{k} e(g, h)^{r_j x_j}. \quad (3)$$

If the above equation is correct and pass the verifiability (whether the ciphertext is actually encrypted by the identity ID or not), then the auditor passes the audit progress.

Decryption. Given the ciphertext $C' = (C_0, C_1, C_2)$, the reciever can get the message as follows via using the private key $d_{\textbf{ID}} = (d_1, d_2)$:

$$\begin{aligned}
& C_0 \cdot \frac{e(d_2, C_2)}{e(d_1, C_1)}\\
&= M \cdot e(g_1, g_2)^r \cdot \frac{e(g^{r_{\textbf{ID}}}, (u' \prod_{i \in \mathcal{V}} u_i)^r)}{e(g_2^\alpha (u' \prod_{i \in \mathcal{V}} u_i)^{r_{\textbf{ID}}}, g^r)}\\
&= M \cdot e(g_1, g_2)^r \cdot \frac{e(g, (u' \prod_{i \in \mathcal{V}} u_i)^{r_{\textbf{ID}}})}{e(g_1, g_2)^r e((u' \prod_{i \in \mathcal{V}} u_i)^{r_{\textbf{ID}} r}, g)}\\
&= M.
\end{aligned}$$

Theorem 1 *If the decisional BDH assumption holds, the proposed $\mathcal{CA}$-$\mathcal{IBE}$ scheme is a secure CA-IBE scheme which satisfies the k-resilient ciphertext-auditability and the security of the standard IND-ID-CPA in the standard model.*

The proof of the above theorem are with three aspects: the standard IND-ID-CPA security, verifiability and unforgeability respectively.

Proof. Firstly, the $\mathcal{CA}$-$\mathcal{IBE}$ scheme is proved with the standard IND-ID-CPA secure; and then, the proposed scheme is verifiable; lastly, it claims the scheme is secure against the mix strategy in the standard model, that is, the scheme is k-resilient unforgeable.

IND-ID-CPA. In our construction, notice that there always exists one honest encrypter at least in the k encrypters, that is, there exists a real random number at least in the set $\{r_1, \ldots, r_k\}$. This show that the cipertertext encrypted by the k encrypters is same as one encrypted by the honest encrypter. So, the standard security of the proposed $\mathcal{CA}$-$\mathcal{IBE}$ scheme can reduce to the security of the Waters's scheme. Since the Waters's scheme [13] is secure against IND-ID-CPA under decisional BDH assumption in the standard model, the proposed $\mathcal{CA}$-$\mathcal{IBE}$ scheme is also secure against standard IND-ID-CPA under the same hard problem assumption in the standard model.

Verifiability. Note that the *anonymous* identity-based encryption [1, 4] scheme requires that the ciphertext can

not reveal the identity of the receiver, so the property of the verifiability is opposite to it. As the observation in [4], some IBE schemes are anonymous, for example, the Boneh et al's IBE scheme [3]; while some IBE schemes are *not* anonymous, for example, Waters's IBE scheme [13]. Since the private key is created randomly, *some extra information* should be embedded into the ciphertext to counteract the randomness of the private key upon decryption. Notice that the "some extra information" is useful for the verifiability in our CA-IBE scheme. The detailed descriptions are as follows:

Given the public **params**=(g, g_1, g_2, u', U), a message M from $\{0,1\}^l$ and a public key **ID** $= (v_1, \ldots, v_n)$, and set $h = u' \prod_{i \in \mathcal{V}} u_i$ where $\mathcal{V} = \{i | v_i \neq 0\}$ is a subset of $\{1, \ldots, n\}$, and get the ciphertext as follows.

$$C = (C_0, C_1, C_2) = (M \cdot e(g_1, g_2)^r, g^r, h^r).$$

Notice that the g, u' and U are public parameters, and there are enough "extra information" to ensure whether the ciphertext was created for a given receiver with the identity **ID**. Then, there are the tuple information

$$[g, h, C_1, C_2] = [g, h, g^r, h^r],$$

so it is not hard to test whether the tuple is Diffie-Hellman tuple as below:

$$e(C_1, h) =^? e(C_2, g),$$

that is,

$$e(g^r, h) =^? e(h^r, g).$$

The progress which test whether the above tuple is Diffie-Hellman tuple or not is sufficient to get the goal of the *verifiability* of the CA-IBE, that is, the test can say whether the ciphertext was actually created by using the identity **ID** as public key.

Unforgeability. If the $\mathcal{CA}$-$\mathcal{IBE}$ scheme satisfies the property of the mix strategy, then the proposed scheme satisfies k-resilient unforgeability. So, it only needs to consider the extreme setting, that is, there are $k-1$ malicious encryption adversaries and one honest encryption adversary in our proof. Without loss of generality, a random number j is selected from the set $\{1, \ldots, k\}$, and assume that the j-th encrypter is honest in our above construction. Note that our construction is unforgeable if there only exists one encrypter and it is honest (it is *regular* scheme if $j = k = 1$). This is because the encrypted message always looks like random for anyone (including the decryption adversary) and it can not give any helpful information to get correct message from this ciphertext for decryption adversary.

Now, assume that the scheme is not k-resilient unforgeable, and let adversary $\mathcal{A}$ control the $k-1$ encrypters. It is easy to show that there is a forger $\mathcal{F}$ who can forge successfully a message in the regular scheme using the adversary $\mathcal{A}$. This is contrary to the case the regular scheme is unforgeable and the theorem is proofed. The detailed descriptions are as follows:

First, in our scheme, $\mathcal{F}$ chooses a modified message M' and the $k-1$ fixed randomized input of $\mathcal{A}$, $\{r_1, \ldots, r_{j-1}, r_{j+1}, \ldots, , r_k\}$, and chooses one random randomized input r_j, then the forger can get the following ciphertext by using the adversa ry $\mathcal{A}$:

$$C' = (M' \cdot e(g_1, g_2)^{r_0 + \cdots + r_j + \cdots + r_k},$$
$$g^{r_0 + \cdots + r_j + \cdots + r_k}, (u' \prod_{i \in \mathcal{V}} u_i)^{r_0 + \cdots + r_j + \cdots + r_k}).$$

Since the scheme is not k-resilient unforgeable, the adversary $\mathcal{A}$ can get the correct message M with the non-negligible probability from the above ciphertext C'.

Secondly, the forger do as the above progress aside from setting $M' = 1$ and no choosing a random randomized input r_j, then he get the following ciphetext:

$$C'' = (1 \cdot e(g_1, g_2)^{r'}, g^{r'}, (u' \prod_{i \in \mathcal{V}} u_i)^{r'}),$$

where $r' = r_0 + \cdots + r_{j-1} + r_{j+1} + \cdots + r_k$. From the ciphertext C' and C'', the forger can get easily the following ciphertext which is a ciphertext in the regular scheme:

$$C = (M' \cdot e(g_1, g_2)^{r_j}, g^{r_j}, (u' \prod_{i \in \mathcal{V}} u_i)^{r_j}).$$

So, the forger also can output a correct message from the ciphertext C with the non-negligible probability, which implies the regular scheme is forgeable. It makes contradiction. □

Remark 1 *Notice that the above $\mathcal{CA}-\mathcal{IBE}$ scheme can not prevent the decryption adversary to recover a single bit of the plaintext when the t-encryptor is malicious. This is because the malicious encryptor can choose fixed randomized input and hide the single bit in the ciphertext. For example, if the last bit of plaintext is 1 (or 0), then the malicious encryptor can choose the randomized input and compute the ciphertext until make the last bit of ciphertext is 1 (or 0). Hada and Sakurai's scheme also has this limitation as above mentioned (Remark 8 in [8]).*

4 Conclusions

This paper constructs the ciphertext-auditable identity-based encryption without the random oracles. There are four steps in our scheme, and it only requires that the backup manager BM sends a backup request to both O and A by authenticated way and does *not* need the public key authentication in the first step. In our proposed scheme, the operator O can encrypt the **PI** before receiving the backup request and duplicates the ciphertext to backup tape right now after getting the backup request. Our scheme is secure against the k-resilient ciphertext-auditability in the standard model. How to design a secure ciphertext-auditable identity based encryption scheme which can prevent the decryption adversary to reveal a single bit of the plaintext if there are t-malicious encryptor, is still an open problem.

Acknowledgements

This research is supported in part by the National Natural Science Foundation of China under Grant No. 61103247. The work of Yong Li is partially supported by the Fundamental Research Funds for the Central Universities under Grant No. 2012JBM004. The first author also thanks S. Hada and K. Sakurai for their valuable discussions at the early stage of this work.

References

[1] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. M. Lee, G. Neven, P. Paillier, and H. Shi, "Searchable encryption waterssrevisited: Consistency properties relation to anonymous ibe, and extensions," *Journal of Cryptology*, vol. 21, no. 3, pp. 350–391, 2007.

[2] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *Proceedings the First Annual Conference Computer and Communications Security*, pp. 62–73, 1993.

[3] D. Boneh and M. Franklin, "Identity based encryption from the weil pairing," in *Advances in Cryptology - Crypto '01*, vol. LNCS 2139, pp. 213–229, Springer-Verlag, 2001.

[4] X. Boyen and B. Waters, "Anonymous hierarchical identity based encryption," in *Advances in Cryptology - Crypto '06*, vol. LNCS 4117, pp. 290–307, Springer-Verlag, 2006.

[5] S. C. and P. Sarkar, *Identity-based encryption*. London: Springer-Heidelberg Publisher, 2010.

[6] R. Canetti, "Towards realizing random oracles: Hash funtions that hide all partial information," in *Advances in Cryptology - Crypto '97*, vol. LNCS 1294, pp. 455–469, Springer-Verlag, 1997.

[7] M. Clear, A. Hughes, and H. Tewari, "Homomorphic encryption with access policies: Characterization and new constructions," in *Proceedings Africacrypt '13*, vol. LNCS 7918, pp. 61–87, Springer-Verlag, 2013.

[8] S. Hada and K. Sakurai, "Ciphertext-auditable public key encryption," in *Proceedings IWSEC '06*, vol. LNCS 4266, pp. 308–321, Springer-Verlag, 2006.

[9] C. Lin and C. Liu, "Ciphertext-auditable public key encryptions without random oracles," *Information*, vol. 15, no. 6, pp. 2599–2602, 2012.

[10] A. Sahai and H. Seyalioglu, "Fully secure accountable-authority identity-based encryption," in *Proccedings PKC '11*, vol. LNCS 6571, pp. 296–316, Springer-Verlag, 2011.

[11] A. Shamir, "Identity based cryptosystems and signature schemes," in *Advances in Cryptology - Crypto '84*, vol. LNCS 196, pp. 47–53, Springer-Verlag, 1984.

[12] M. Tian, W. Yang, and L. Huang, "Security of a biometric identity-based encryption scheme," *International Journal of Network Security*, vol. 14, no. 6, pp. 362–365, 2012.

[13] B. Waters, "Efficient identity based encryption without random oracles," in *Advances in Cryptology - EuroCrypt '05*, vol. LNCS 3494, pp. 114–127, Springer-Verlag, 2005.

Changlu Lin received the BS degree and MS degree in mathematics from the Fujian Normal University, P.R. China, in 2002 and in 2005, respectively, and received the Ph.D degree in information security from the state key laboratory of information security, Graduate University of Chinese Academy of Sciences, P.R. China, in 2010. He works currently for the School of Mathematics and Computer Science, and the Key Laboratory of Network Security and Cryptology, Fujian Normal University. He is interested in cryptography and network security, and has conducted research in diverse areas, including secret sharing, public key cryptography and their applications.

Yong Li received his M.S. degree in Computer Science from Wuhan University in 2003, and the Ph.D. degree from State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences in 2007. He works currently for the Key Laboratory of Communication & Information Systems (Beijing Jiaotong University), Beijing Municipal Commission of Education. He is interested in applied cryptography and secure cloud computing.

Kewei Lv works at the State Key Laboratory of Information Security, Institute of Information Engineering, CAS. He is interested in provable security, design and analysis of algorithm, computational complexity, and secure multiparty protocol.

Chin-Chen Chang received his PhD in Computer Engineering from National Chiao Tung University. He received BS in Applied Mathematics and MS in Computer and Decision Sciences. Both were awarded in National TsingHua University. He served in National Chung Cheng University from 1989 to 2005. He works currently for Chair Professor in Department of Information Engineering and Computer Science, Feng Chia University, from February 2005. He has won many research awards and honorary positions by and in prestigious organizations both nationally and internationally. He is currently a Fellow of IEEE and a Fellow of IEE, UK. His current research interests, including database design, computer cryptography, image compression and data structures.

Notes on Proxy Signcryption and Multi-proxy Signature Schemes

Chunhua Pan[1], Shunpeng Li[1], Qihui Zhu[1], Chunzhi Wang[2], and Mingwu Zhang[1,2]
(Corresponding author: Mingwu Zhang)

College of Information, South China Agricultural University[1]
School of Computer Sciences, Hubei University of Technology[2]
(Email: csmwzhang@gmail.com)
(Received Dec. 26 2012; revised and accepted Oct. 1, 2013)

Abstract

Proxy signcrytipn scheme allows an original signer to delegate his signing power to a proxy such that the latter can signcrypt a message on behalf of the former. Recently, Lin et al. proposed a proxy signcryption with CCA and CMA security. In this work, we indicate that the Lin et al.'s proxy signcryption scheme does not hold the security of indistinguishability against adaptive chosen-ciphertext attacks and existential unforgeability against adaptive chosen-message attacks. Also, we show that the Jin-Wen's certificateless multi-proxy signature scheme does not hold the security of existential unforgeability against adaptive chosen-message attacks.
Keywords: Cryptanalysis, multi-proxy signature, proxy signcryption, unforgeability

1 Introduction

Proxy signcryption, first proposed by Gamage et al. [5, 12, 13], is a cryptographic primitive, which combines the functionality of a proxy signature scheme with that of an encryption, to allow an original signer to delegate his signing power to a proxy one such that the proxy can signcrypt a message on behalf of the delegator. The signcrypted message can only be decrypted by a designated recipient who is also responsible for verifying the recovered proxy signature function [2, 4, 9]. Recently, Lin et al. [10, 11] proposed an efficient proxy signcryption scheme based on bilinear pairings. Jin and Wen et al. [8] proposed a multi-proxy signature scheme in certificateless setting. They also stated that their scheme achieves the *confidentiality* against indistinguishability under adaptive chosen-ciphertext attacks (IND-CCA2) and *unforgeability* against existential forgery under adaptive chosen-message attacks (UEF-CMA2) in the random oracle models.

Multi-proxy signature, which was first introduced by Hwang and Shi et al. [3, 6, 7], could be viewed as a variation of the proxy signature primitive. In such a scheme, an original signer delegates his signing power to a group of proxy signers, and then only the cooperation of all proxy signers can generate proxy signatures, referred to as multi- proxy signatures, on behalf of the original signer.

In this work, we show that the Lin et al.'s proxy signcryption scheme [10] is insecure since they cannot obtain the unforgeability and forward security. We also indicate that the Jin-Wen's certificateless multi-proxy signature scheme does not hold the security of existential unforgeability against adaptive chosen-message attacks of their declared.

2 Model of Proxy Signcryption and Multi-proxy Signature

2.1 Proxy Signcryption

Definition 1. ***Proxy Signcryption.*** *A proxy signcryption contains four probabilistic polynomial-time algorithms:*

1) *Setup: Taking as input 1^k where k is a security parameter, the algorithm generates the systems public parameters pp*

2) *Proxy-Credential-Generation (PCG): The PCG algorithm takes as input the private key of original signer and outputs a corresponding proxy credential for the proxy signer.*

3) *Signcrypted-Message-Generation (SMG): The SMG algorithm takes as input a plaintext m, a proxy credential, the public key of designated recipient and the private key of proxy signer, and outputs signcrypted message δ.*

4) *Signature-Recovery-and-Verification (SRV): The SRV algorithm takes as input a signcrypted message δ, the private key of designated recipient and the public keys of original and proxy signers, and outputs a plaintext m and its converted ordinary*

proxy signature if the signcrypted message is valid, and returns an error symbol $\perp$ otherwise.

2.2 Certificateless Multi-proxy Signature

Definition 2. ***Certificateless Multi-proxy Signature.*** *A certificateless multi-proxy signature scheme is defined by a collection of probabilistic polynomial-time algorithms as follows:*

1) *Setup: Given a security parameter k, the PKG generates a master key s and the system parameters pp.*

2) *Partial-Private-Key-Extract (PPKE): Given a user's identity ID_i, the PKG produces the corresponding partial private key D_i with the master key s after verifying the user's identity.*

3) *User-Key-Generate (UKG): After receiving the partial private key D_i from PKG, the user with identity ID_i randomly selects a secret value x_i to construct his full private key sk_i with D_i, and publishes his public key P_i w.r.t x_i.*

4) *Sign: Given a message m, the user, whose identity is ID_i and public key is P_i, generates a signature σ on m with his private key sk_i.*

5) *Verify: Given a signature σ on message m, the verifier accepts it if σ is a valid signature relative to m, the signer's identity ID_i and his public key P_i and rejects otherwise.*

6) *Proxy-Key-Generate (PKG): It is a protocol between the original signer and all proxy signers formed by a group of interactive randomized algorithms. All participants take their identities ID_{OS} and $\mathsf{ID}_{PS_1}, \mathsf{ID}_{PS_2}, \cdots, \mathsf{ID}_{PS_n}$ as inputs. Additionally, the original signer also takes his secret key sk_{OS} and the delegation warrant w as inputs, where w includes the restrictions on the class of messages delegated, the identities of the original signer and all proxy singers, the period of delegation and etc. Every proxy signer also takes his secret key sk_{PS_i} as input. As a result, each proxy signer gets a multi-proxy signature secret key PSK_i which could be used to cooperatively produce multi-proxy signatures with other proxy signers.*

7) *Multi-Proxy-Sign (MPS): Given a message m which satisfies the requirements stated in w, all proxy signers cooperatively produce a multi-proxy signature σ_{MPS} on behalf of the original signer with the multi-proxy signature secret keys PSK_i for $i \in [n]$.*

8) *Multi-Proxy-Verify (MPV): Given a multi-proxy signature σ_{MPS} on message m under the warrant w, the verifier accepts it if σ_{MPS} is a valid signature relative to m and w by proxy signers $PS_1, PS_2, \cdots, PS_n$ on behalf of the original signer OS.*

For certificateless cryptosystems, the widely accepted notion of security was defined by Al-Riyami and Paterson [1]. According to their definitions, two types of adversaries with different capabilities were considered, which could be described as follows:

1) **Type I Adversary $\mathcal{A}_I$**: This type of adversary acts as a dishonest user who does not have access to the master key but has the ability to replace the public key of any entity with a value of his choice.

2) **Type II Adversary $\mathcal{A}_{II}$**: This type of adversary acts as a malicious PKG who has access to the master key but cannot perform the public key replacements.

3 Review of Lin et al.'s Proxy Signcryption

Setup Taking as input 1^k, the system authority selects two groups $(\mathbb{G}_1, +)$ and $(\mathbb{G}_2, \times)$ of the same prime order q. Let P be a generator of order q over $\mathbb{G}_1$, $\hat{e} : \mathbb{G}_1^2 \to G_2$ a bilinear pairing and $h_1 : \{0,1\} \times \mathbb{G}_1 \to \mathcal{Z}_q$, $h_2 : \mathbb{G}_1 \to \mathbb{G}_1$, $h_3 : \mathbb{G}_2 \times \mathbb{G}_1 \to \{0,1\}^k$ be collision resistant hash functions. The system publishes $pp = (\mathbb{G}_1, \mathbb{G}_2, q, P, \hat{e}; h_1, h_2, h_3)$. Each user $\mathcal{U}_i$ chooses his private key $x_i \in \mathcal{Z}_q$ and computes the corresponding public key as $Y_i = x_i P$.

PCG Let $\mathcal{U}_o$ be an original signer delegating his signing power to a proxy signer $\mathcal{U}_p$. $\mathcal{U}_o$ first chooses an integer $d \in \mathcal{Z}_q$ and a warrant m_w to compute $N = dP$, $\sigma = x_o + d(m_w) \bmod q$.

SMG To signcrypt a message $m \in \{0,1\}^k$ on behalf of the original signer U_o, U_p chooses $r \in \mathcal{Z}_q$ to compute: $R = rP$, $S = r(h_1(m, R) + x_p + \sigma)^{-1} P$, $V = \hat{e}(h_2(\sigma Y_v), x_p Y_v)$, $X = E_V(S)$ and $Y = h_3(V, R) \oplus m$. It outputs the ciphertext $\delta = (R, X, Y, N)$ together with the warrant m_w.

SRV Upon receiving $\delta = (R, X, Y, N)$, U_v computes $V = \hat{e}(h_2(x_v(Y_o + m_w N)), x_v Y_p)$, $m = h_3(V, R) \oplus Y$, $S = D_V(X)$, and accepts the message if $\hat{e}(h_1(m, R) + Y_p + Y_o + m_w N, S) = \hat{e}(P, R)$ holds.

3.1 Cryptanalysis

In this section, we give a forgery attack and a confidentiality attack to show that the Lin et al.'s scheme does not hold the claimed properties such as unforgeability against UEF-CMA2 and confidentiality against IND-CCA2.

3.1.1 Unforgeability Attack

Definition 3. ***Unforgeability of Proxy Signcryption.*** *A proxy signcryption scheme is said to achieve unforgeability against existential forgery under adaptive chosen-message attacks (EF-CMA) if there exists*

no probabilistic polynomial-time) forger $\mathcal{F}$ with non-negligible advantage in the following game played with a challenger $\mathcal{B}$:

Setup *$\mathcal{B}$ runs the $\mathsf{Setup}(1^k)$ algorithm and sends the system's public parameters pp to the forger $\mathcal{F}$.*

Phase 1 *The forger $\mathcal{F}$ can issue several kinds of following queries adaptively.*

- *PCG queries: $\mathcal{F}$ issues a PCG query with respect to the target proxy signer. $\mathcal{B}$ returns the corresponding warrant and its proxy credential (σ, N, m_w).*
- *SMG queries: $\mathcal{F}$ chooses a message m and a warrant, and $\mathcal{B}$ outputs the corresponding signcrypted message δ to $\mathcal{F}$.*
- *SRV queries: On receiving a signcrypted ciphertext δ with its warrant sent by $\mathcal{F}$, $\mathcal{B}$ returns a message m and its converted proxy signature if the signcrypted message δ is valid. Otherwise, an error symbol $\perp$ is returned.*

Forgery *$\mathcal{F}$ arbitrarily chooses a message m and produces a ciphertext δ^* which is not outputted by the SMG query. The forger $\mathcal{F}$ wins if δ^* is valid.*

Forgery Attacks. We now show that the receiver U_v may forge a new valid ciphertext $\tilde{\delta}$ for any message $\tilde{m}$ on behalf of the proxy signcrypter U_p. Receiver U_v does

1) Random pick $\tilde{r} \in \mathcal{Z}_q$, compute $\tilde{R} = \tilde{r}(Y_o + Y_p + m_w N)$ and $\tilde{S} = \tilde{r}P - \tilde{r} \cdot h_1(\tilde{m}, \tilde{R})P$.
2) Compute $V = \hat{e}(h_2(x_v(Y_o + m_w N)), x_v Y_p)$ using U_v's secret key x_v.
3) Compute $\tilde{Y} = \tilde{m} \oplus h_3(V, \tilde{R})$.
4) Set $\tilde{X} = E_V(\tilde{S})$.
5) Output the forged ciphertext $\tilde{\delta} = (\tilde{R}, \tilde{X}, \tilde{Y}, N)$.

The forged ciphertext $\tilde{\delta} = (\tilde{R}, \tilde{X}, \tilde{Y}, N)$ is valid for the decryption algorithm SRV: $V = \hat{e}(h_2(x_v(Y_o + m_w N)), x_v Y_p)$, $\tilde{m} = h_3(V, \tilde{R}) \oplus \tilde{Y}$, $S = D_V(\tilde{X})$.

$$\begin{aligned}
&\hat{e}(h_1(\tilde{m}, \tilde{R})P + Y_p + Y_o + m_w N, \tilde{S}) \\
=&\hat{e}(h_1(\tilde{m}, \tilde{R})P + Y_p + Y_o + m_w N, \tilde{r}P - \tilde{r}h_1(\tilde{m}, \tilde{R})P) \\
=&\hat{e}(Y_p + Y_o + m_w N, P)^{\tilde{r}} \\
=&\hat{e}(P, \tilde{R}).
\end{aligned}$$

Remark 1. *Because the verification equation is only to verify the components R and S where $R = rP$ and $S = r(h_1(m, R) + x_p + \sigma)^{-1}P = (h_1(m, R) + x_p + \sigma)^{-1}R$. We can construct the new $\tilde{R}, \tilde{S}$ such that $\tilde{R} = \tilde{r}(Y_o + Y_p + m_w N)$ and $\tilde{S} = \tilde{r}P - \tilde{r}h_1(m, \tilde{R})P$. Then $\tilde{R}, \tilde{S}$ have the same relation with R, S in the verification. i.e.,*

$$\hat{e}(h_1(m, R)P + Y_o + Y_p + m_w N, S) = \hat{e}(P, R) \Leftrightarrow$$

$$\hat{e}(h_1(m, R)P + Y_o + Y_p + m_w N, \tilde{S}) = \hat{e}(P, \tilde{R}).$$

Remark 2. *Actually, any user can forge a signcrypted ciphertext on behalf of the proxy signcrypter successfully, since anyone may compute the proxy agreement key V with his secret key.*

3.1.2 Confidentiality Attack

Definition 4. ***Confidentiality.*** *A proxy signcryption scheme is said to achieve the security requirement of confidentiality against indistinguishability under adaptive chosen-ciphertext attacks (IND-CCA2) if there is no PPT distinguisher $\mathcal{D}$ with non-negligible advantage in the following game played with a challenger $\mathcal{B}$.*

Setup *$\mathcal{B}$ first runs the $\mathsf{Setup}(1^k)$ algorithm and sends the system's public parameters pp to $\mathcal{D}$.*

Phase 1 *The distinguisher $\mathcal{D}$ adaptively issues PCG, SMG and SRV queries as those in Phase 1 of unforgeability definition.*

Challenge *$\mathcal{D}$ produces two plaintexts m_0 and m_1 of the same length, then $\mathcal{B}$ flips a coin $\eta \in \{0, 1\}$ and generates a ciphertext δ^* for m_η. The ciphertext δ^* is then delivered to $\mathcal{D}$ as a target challenge.*

Phase 2 *The distinguisher $\mathcal{D}$ issues new queries as those in Phase 1, except the SRV query for the target challenge δ^*.*

Guess *$\mathcal{D}$ outputs a bit η' and wins the game if $\eta' = \eta$.*

Confidentiality Attacks. We show that the scheme is not forward secure as the confidentiality definition declared. In the forward security definition, only designated recipient can decrypt the message legally. That is, it is infeasible for a distinguisher $\mathcal{D}$ to extract the message even though the signcrypter leaks his secret key to $\mathcal{D}$. To guess the message m_η in the ciphertext $\delta^* = (R, X, Y, N)$, $\mathcal{D}$ gets the guess η as follows:

1) Computes $V = \hat{e}(h_2(\sigma Y_v), x_p Y_v)$;
2) Recovers $m = Y \oplus h_3(V, R)$.
3) If $m = m_0$, $\mathcal{D}$ outputs $\eta' = 0$ as the guess, otherwise outputs $\eta' = 1$.

Remark 3. *In Lin et al.'s proxy signcryption scheme, the agreement key V between the proxy signcrypter and the decrypter is fixed and constant that does not import a randomness. This means that any ciphertext generated by proxy signcrypter U_p to U_v may be decrypted using this decrypted key V. This violates the probabilistic encryption principle.*

4 Cryptanalysis of Jin-Wen Certificateless Multi-proxy Signature Scheme

4.1 Review of Jin-Wen's Scheme

Setup Given a security parameter k, the PKG does as follows: first choose groups $\mathbb{G}$ and G_T of prime order q such that an admissible bilinear pairing $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ can be constructed and pick an arbitrary generator P of $\mathbb{G}$; Choose a random number $s \in \mathcal{Z}_q$ as the master key msk and set $Q = sP$ as the master public key; Choose six different cryptographic hash functions that $H_1, h_2, H_3 : \{0,1\}^* \to \mathbb{G}$ and $H_4, H_5, H_6 : \{0,1\}^* \to \mathcal{Z}_q$; Finally, output and publish system parameters $pp = (\mathbb{G}, \mathbb{G}_T, \hat{e}, P, Q, H_1, H_2, H_3, H_4, H_5, H_6)$ while keeping the master key $msk = s$.

PPKE Given a user's identity $\mathsf{ID} \in \{0,1\}^*$, the PKG generates the partial private key for the user by computing $D = sH_1(\mathsf{ID})$ and sends D to user ID.

UKG The user with identity ID selects a random number $x \in \mathcal{Z}_q$, sets his public key as $P_{\mathsf{ID}} = xP$ and makes it public while keeping the secret value x and the partial private key D as his secret key sk_{ID}.

Sign To sign a message $m \in \{0,1\}^*$ with $sk = (x, D)$, the signer (identity ID and $pk = P_{\mathsf{ID}}$) first chooses a random number $r \in \mathcal{Z}_q$ and computes $R = rP$; computes $W = H_2(pp)$, $T = H_3(Q)$, $h = H_4(pp, m, \mathsf{ID}, P, R)$ and $V = hD + xW + rT$. Finally, outputs $\sigma = (R, V)$ as the signature.

Verify. The verifier checks whether $\hat{e}(V, P) = \hat{e}(hH_1(\mathsf{ID}), Q)e(W, P_{\mathsf{ID}})e(T, R)$ holds, where $W = H_2(pp)$, $T = H_3(Q)$, $h = H_4(pp, m, \mathsf{ID}, P_{\mathsf{ID}}, R)$.

PKG The proxy key generation algorithm performs as follows:

1) Delegation generation: To delegate the signing capability, the original signer o, with identity ID_o and public key P_o, first makes the signed warrant w which specifies the necessary proxy details, such as the identities of the original signer and the proxy signers, the type of messages delegated, the period of delegation and etc. Then he produces the delegation as follows
   a. Choose a random number $r_0 \in \mathcal{Z}_q$ and compute $R_0 = r_0 P$;
   b. Compute $h_0 = H_5(pp, w, \mathsf{ID}_o, P_o, R_0)$, $W = H_2(pp)$, $T = H_3(Q)$ and $V_0 = h_0 D_o + x_o W + r_0 T$;
   c. Send (w, R_0, V_0) to each proxy signer ps_i, $i = 1, \ldots, n$.
2) Delegation verification: After receiving the delegation (w, R_0, V_0) from the original signer o, each proxy signer ps_i confirms its validity by checking $\hat{e}(V_0, P) = e(h_0 H_1(\mathsf{ID}_o), Q)\hat{e}(W, P_o)\hat{e}(T, R_0)$, where $h_0 = H_5(pp, w, \mathsf{ID}_o, P_o, R_0)$, $W = H_2(pp)$, $T = H_3(Q)$. ps_i accepts it if the equation holds; otherwise, he requests a valid one from o, or terminates the protocol.
3) Proxy secret key generation: If all proxy signers ps_i confirm the delegation, each of them sets $PSK_i = (sk_{ps_i}, R_0, V_0)$ as his multiproxy signature secret key respectively.

MPS Every proxy signer ps_i computes $R_i = r_i P$ with random picked $r_i \in \mathcal{Z}_q$, and $V_i = h_i D_{ps_i} + x_{ps_i} W + r_i T$, where $W = H_2(pp)$, $T = H_3(Q)$ and $h_i = H_6(pp, w, m, \mathsf{ID}_{ps_i}, P_{ps_i}, R_i)$. Sends (w, R_0, V_0, R_i, V_i) to a clerk.
The clerk verifies its validity by checking the equations $\hat{e}(V_0, P) = \hat{e}(h_0 H_1(\mathsf{ID}_o), Q)\hat{e}(W, P_o)\hat{e}(T, R_0)$ and $\hat{e}(V_i, P) = \hat{e}(h_i H_1(\mathsf{ID}_{ps_i}), Q)\hat{e}(W, P_{ps_i})\hat{e}(T, R_i)$. Then it generates the multi-proxy signature as $\sigma_{MPS} = (w, R_{MPS}, V_{MPS})$ where $R_{MPS} = (R_0, R_1, \ldots, R_n)$ and $V_{MPS} = \sum_i V_i$.

MPV To verify a multi-proxy signature $\sigma_{MPS} = (w, R_{MPS}, V_{MPS})$ of the message m, the verifier checks whether: $\hat{e}(V_{MPS}, P) = \hat{e}(h_0 H_1(\mathsf{ID}_o) + \sum_i h_i H_1(\mathsf{ID}_{ps_i})) \cdot \hat{e}(W, \sum_{i \in \Omega} P_i)$.
$\hat{e}(T, \sum_i R_i)$, where $h_0 = H_5(pp, w, \mathsf{ID}_o, P_o, R_0)$, $\Omega = \{o, ps_1, \ldots, ps_n\}$, $W = H_2(pp)$, $T = H_3(Q)$ and $h_i = H_6(pp, w, m, \mathsf{ID}_{ps_i}, P_{ps_i}, R_i)$.

4.2 Forgery Analysis

In this section, we give a forgery attack to show that the Jin-Wen scheme does not hold the claimed security.

4.2.1 Clerk's Forgery

A clerk $\mathcal{C}$ can forgery a multiproxy signature on behalf of the new original delegator $\tilde{o}$. First, $\mathcal{C}$ requests a Proxy-key-gen query between the original delegator $\tilde{o}$ and multi-proxy $ps_1, \ldots, ps_n$, then he gets a delegation $(\tilde{w}, \tilde{R}_0, \tilde{V}_0)$.

After clerk $\mathcal{C}$ obtains all multi-proxy signatures (w, R_0, V_0, R_i, V_i) on the message m from ps_i $(i = 1, \ldots, n)$, $\mathcal{C}$ replaces w, R_0, V_0 with $\tilde{w}, \tilde{R}_0, \tilde{V}_0$ respectively.

Adversary can forge a valid multi-proxy signature $(\tilde{w}, \tilde{R}_0, \tilde{V}_0, \tilde{R}_i, \tilde{V}_i)$ on message $\tilde{m}$ under warrant $\tilde{w} \neq w$ by ID_i where $i = 2, \ldots, n+1$ on behalf of ID_1 (or the challenger). To forge a valid multi-proxy signature, adversary $\mathcal{A}$ does

1) $\mathcal{A}$ makes a warrant $\tilde{w}$ that the original signer's identity is ID_1, the proxy signers's identities are $\mathsf{ID}_2, \ldots, \mathsf{ID}_{n+1}$.
2) $\mathcal{A}$ requests a signature query on $(\mathsf{ID}_1, \tilde{w})$, and obtains an answer $(\tilde{U}_1, \tilde{V}_1)$.

3) $\mathcal{A}$ performs extraction queries for $\mathsf{ID}_2, \ldots, \mathsf{ID}_{n+1}$. That is, $\mathcal{A}$ knows the secret keys of identities $\mathsf{ID}_2, \ldots, \mathsf{ID}_{n+1}$. $\mathcal{A}$ can generate ID_i's proxy key $(sk_{id_i}, \tilde{U}_1, \tilde{V}_1)$.

4) $\mathcal{A}$ generates a valid multi proxy signature $\sigma_{MPS} = (\tilde{w}, \tilde{R}_{MPS}, \tilde{V}_{MPS})$.

Remark 4. *The Jin-Wen certificateless multi-proxy signature scheme, which can be viewed as a two-level hierarchical IBE scheme, is not secure in the proposed security model. The main reason is the direct employment of the proposed scheme that is a simple aggregation of standard signatures produced by multiple original signer and multi-proxy, respectively.*

5 Conclusion

In this work, two attacks were proposed to show that the Lin etl al.'s proxy signcryption scheme does not hold the indistinguishability against CCA2 and existential unforgeability against CMA. Also, existential forgery attacks was presented to demonstrate that a certificateless multi-proxy signature proposed by Jin and Wen does not hold the existential unforgeability.

Acknowledgements

This work was supported by the National Natural Science Foundation of China under Grants 61370224, 61272404 and 61170135, Guangdong Natural Science Foundation under Grant S2012010010383, and Key Program of Natural Science Foundation of Hubei Province under Grant 2013CFA046.

References

[1] S. S Al-Riyami and K. G. Paterson. "Certificateless public key cryptography,". in *Advances in Cryptology - Asiacrypt '03*, pp. 452–473. 2003.

[2] F. Cao and Z. Cao, "A secure identity-based proxy signature scheme," *Information Sciences*, vol. 179, no. 3, pp. 292–302, 2009.

[3] M. L. Das, A. Saxena, and D. B. Phatak, "Algorithms and approaches of proxy signature: A survey," *International Journal of Network Security*, vol. 9, no. 3, pp. 264–284, 2009.

[4] H. Elkamchouchi, M. Nasr, and R. Ismail, "A new efficient strong proxy signcryption scheme based on a combination of hard problems," in *IEEE International Conference on Systems, Man and Cybernetics*, pp. 5123–5127, 2009.

[5] C. Gamage, J. Leiwo, and Y. Zheng, "An efficient scheme for secure message transmission using proxy-signcryption," in *Proceedings of the Twenty Second Australasian Computer Science Conference*, pp. 18–21, 1999.

[6] M. S. Hwang, C. C. Lee, and S. F. Tzeng, "A new proxy signature scheme for a specified group of verifiers," *Information Sciences*, vol. 227, pp. 102–115, 2013.

[7] S. J. Hwang and C. H. Shi, "A simple multi-proxy signature scheme," in *Proceedings of the Tenth National Conference on Information Security*, pp. 134–138, 2000.

[8] Z. Jin and Q. Wen, "Certificateless multi-proxy signature," *Computer Communications*, vol. 34, no. 3, pp. 344–352, 2011.

[9] F. Li, X. Xin, and Y. Hu, "Id-based threshold proxy signcryption scheme from bilinear pairings," *International Journal of Security and Networks*, vol. 3, no. 3, pp. 206–215, 2008.

[10] H. Y. Lin, T. S. Wu, S. K. Huang, and Y. S. Yeh, "Efficient proxy signcryption scheme with provable CCA and CMA security," *Computers & Mathematics with Applications*, vol. 60, no. 7, pp. 1850–1858, 2010.

[11] S. Mashhadi, "A novel non-repudiable threshold proxy signature scheme with known signers," *International Journal of Network Security*, vol. 15, no. 4, pp. 274–279, 2013.

[12] M. Zhang, B. Yang, Z. Chen, and T. Takagi, "Efficient and adaptively secure broadcast encryption systems," *Security and Communication Networks*, vol. 6, no. 8, pp. 1044–1052, 2013.

[13] M. Zhang, J. Yao, C. Wang, and T. Takagi, "Public key replacement and universal forgery of SCLS scheme," *International Journal of Network Security*, vol. 15, no. 1, pp. 115–120, 2013.

Chunhua Pan is a lecturer at College of Information, South China Agriculutral University. His research interests focus on Secure Computations and Network Protocols.

Shunpeng Li is a postgraduate student at College of Information, South China Agriculutral University. His research is in the field of Information Security and Cryptography.

Qihui Zhu is a postgraduate student at College of Information, South China Agriculutral University. His research is in the field of Information Processing and Security.

Chunzhi Wang is a professor at School of Computer Sciences, Hubei University of Technology. Her research interests focus on Network Protocol and System Security.

Mingwu Zhang is a professor at School of Computer Sciences, Hubei University of Technology. He is a senior member of Chinese Computer Federation, a senior member of Chinese Association for Cryptologic Research (CACR), and a member of IEEE Computer Society. His research interests include Secure Multi-party Computation and Information Security.

Highly Secure Network Switches with Quantum Key Distribution Systems

Mikio Fujiwara[1], Tomoyasu Domeki[2], Shiho Moriai[1], and Masahide Sasaki[1]
(Corresponding author: Mikio Fujiwara)

National Institute of Information and Communications Technology[1]
4-2-1 Nukui-Kita, Koganei, Tokyo 184-8795, Japan
NEC Communication Systems, Ltd.[2]
Chuou Aoba, Sendai, Miyagi 980-0021, Japan
(Email: fujiwara@nict.go.jp)
(Received Oct. 9, 2013 ; revised and accepted Mar. 13, 2014)

Abstract

We have developed network "switches" with security enhanced by "quantum key distribution (QKD) systems". In a Layer 2 "switch", media access control (MAC) addresses are encrypted to prevent unauthorized access from internal network. After an initial authentication, common random key bits are shared between the Layer 2 "switch" and users. MAC addresses are encrypted with shared key at every packet. In Layer 3, secure keys from a "QKD system" are used in the Internet Protocol Security (IPSEC) protocol for encrypting a payload in one-time pad, and also for extracting a message digest for unconditionally secure message authentication. In this way, network security can be effectively enhanced by QKD in an IP compatible manner.

Keywords: IPSEC, layer 2, layer 3, network switch, quantum key distribution

1 Introduction

Data theft is on the increase and set to rise dramatically in the upcoming years. Optical fiber transmission cannot be an exception, despite its reputation for being more secure than standard wiring or airwaves. Indeed, photon crosstalk between neighboring fibers in a field-installed cable is commonly occurred and information theft could easily take place if novel photon detectors are used [4]. Therefore, technology for information security has become a critical issue for the advanced information and communications network infrastructure. Conventionally, data encryption is performed at Layer 3 or above (in terms of OSI layer model) on the basis of protocols such as Internet Protocol Security (IPSEC) and the Secure Socket Layer (SSL) Virtual Private Network (VPN) solution. On the other hand, data protection technology performed at Layer 1 has been developed in recent years. Quantum key distribution (QKD) [5] allows two users, Alice and Bob, to share random key bits in an unconditionally secure manner based on the fundamental laws of physics. BB84 [2] is known as the most famous protocol. The unconditional security of QKD is ensured only for point-to-point link connected via an optical transmission line. Recently, its distance limit has been extended to 250 km [9]. For networking QKD links for multiple users, and extending the range of QKD services, one should currently rely on key encapsulating relay via trusted nodes where eavesdroppers cannot enter [1, 3, 7, 8]. Therefore proper key management is required for the QKD network. Security loopholes are inevitably associated with such a network layer structure, leaving a possibility of causing more serious security problems. Therefore, not only the security of the physical layer but also that of the upper layers should be properly cared using appropriate security technology in a whole network. In such a situation, security functions of switches in Layers 2 and 3 are of particular importance. Secure keys seeded from the QKD layer should be efficiently used in those network "switches".

We have thus developed integrated network "switches" for Layer 2 and Layer 3 whose securities are enhanced with secure keys from "QKD systems". In this paper, we describe a secure architecture of a network-structure via "QKD systems". In Section 2, we introduce the Layer 2 "switch" in which the media access control (MAC) addresses are encrypted per packet to prevent MAC address spoofing and unauthorized access from an internal network. In Section 3, we explain the Layer 3 "switch" in which the secure keys from the QKD system is used in an enhanced IPSEC protocol. IPSEC has an authentication function and, needless to say, an encryption feature. Information-theoretic secure keys are used in encryption and authentication, and information-theoretic security is guaranteed in both. We have developed the "switches" embedded in PCs. We report the performance of the new Layer 2 and Layer 3 "switches" shown in Figure 1.

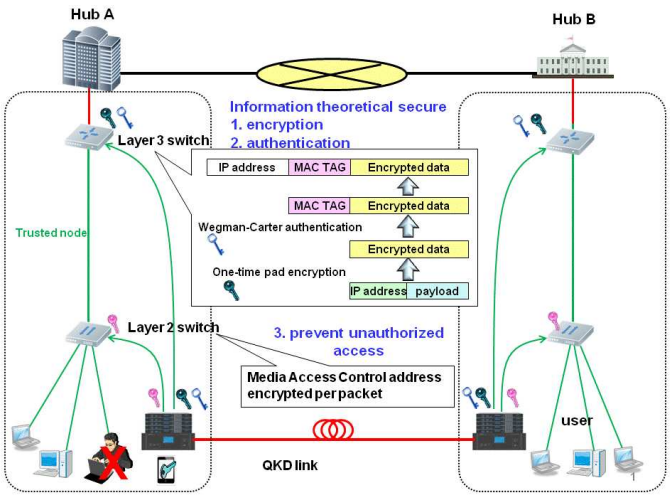


Figure 1: Conceptual view of the integrated network "switches"

2 Layer 2 Switch

The encryption scheme for data exchanged between VPNs has been drawing attention for use in layer 3. However, serious security holes are recognized at layer 2. Ethernet technology has been established on the assumption that users are fundamentally good. In other words, unauthorized access from an internal network PC is very easy because there is no authentication process in layer 2. To prevent such unauthorized accesses, deconcentration of access authority is usually adopted in the network. However, such a protection scheme may be destroyed by an impersonation from an internal-network PC. In fact, spoofing a MAC address, which identifies a "host (PC)" in the layer 2, may easily be made. However, even if network authentication is employed, unauthorized access is difficult to prevent completely due to the sophistication of spoofing attacks. To enhance the security of the internal-network, we have developed a Layer 2 "switch" that uses random bits provided from a "QKD system" for authentication of hosts. First, the switch sends each "host" the random bits by encrypting it with AES. Each "host" encrypts the MAC address by the random bits and sends it to the Layer 2 "switch". The random bits are used only once for each packet between the host and the Layer 2 switch. In the Layer 2 switch, consistency is checked by using a decrypted MAC address and IP address. If the host sends correct addresses, the Layer 2 "switch" passes the packet. Process are summarized as follows:

1) Authentication between the "QKD systems" using a pre-shared key.

2) Authentication between the Layer 2 "switch" and "QKD system" machine using a pre-shared key.

3) Blocks of random bits are downloaded to "switches".

4) Initial authentication process between the "switch" and "hosts" by using pre-shared (USB sticks) keys.

5) MAC addresses are enrolled and checked with registered list.

6) Random bits encrypted by AES are shared between the Layer 2 "switch" and "PCs".

7) MAC addresses are encrypted using the random bits per packet.

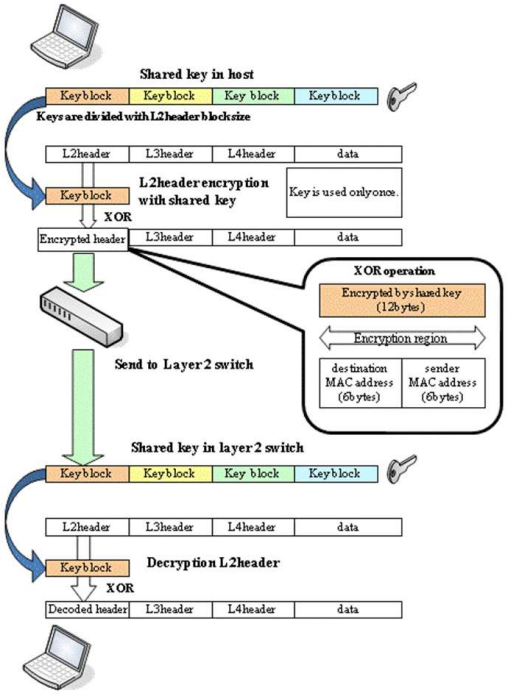
8) MAC addresses are decrypted and checked with IP addresses in the "switch".

9) If the MAC address and IP address are matched with the registered data, the switch allows connection. If not, the packet is silently discarded.

Our "switch" has strong protection against MAC spoofing, IP address spoofing, spoofing using internet control message protocol (ICMP) redirects, address resolution protocol (ARP) poisoning attacks, and so on. This switch obtains 70-90% throughput performance without encryption. MAC addresses are changed in every packet shown in Figure 2. For example, we show the effect of this "switch" for the case of the IP address spoofing in Figure 3. When we operate this "switch", "hosts (PCs)" should be connected with the "switch" directly. In this system, a cascade arrangement is prohibited in order to prevent information leakage by monitoring packets in "hosts". Of course, it is possible to adopt an encryption technique in communication between "hosts", but it depends on the required security level. Moreover, the random number delivery could be more secured, if the host would receive it from a trusted courier, for example, by receiving it from the "switch" via an authenticated smart phone and installing it into the "host". By using this device, key sharing can be done with high security.

3 Layer 3 Switch

The scenario in which the QKD is used for key establishment between two local area networks has been demonstrated within the BBN DARPA network project [3] and other networks [5]. A point-to-point link in a local area network (LAN) or VPN encryptor provides secure keys to the Layer 3 "switch". Payloads are encrypted by IPSEC. The security of the transmitted data over such a link is limited by the security of the encryption scheme. Ideally, Vernam's one-time pad encryption can provide information-theoretical security. When, otherwise, used with modern cryptography, frequent key renewal of the symmetric key encryption also enhances the security level [7, 9]. Problems are the internet key exchange process and the randomness of the key. We are developing the QKD-based Layer 3 "switch" in that the symmetric-key is refreshed in each packet of the IPSEC protocol. Our "switch" uses Vernam's one-time pad



(a)

time	Sender's MAC address	Receiver's MAC address
202 138.096514	48:a1:70:89:4e:7d	d4:4a:47:c0:ba:d0
204 138.128000	e0:48:45:98:48:1a	d0:33:8b:ef:37:31
205 138.128499	58:1e:db:88:cf:44	94:ad:0c:14:fd:f4
208 138.248009	38:49:e5:30:f1:c3	74:b7:b9:5b:0c:75
209 138.248248	f0:a8:1f:11:63:7a	58:f8:a4:4d:67:f7
211 138.258376	08:bc:7c:16:07:8a	40:16:b4:eb:a4:9f
212 138.264384	90:f3:e2:b9:1b:15	f4:cf:87:4d:53:f6
215 138.412626	e0:ab:63:94:11:1e	58:51:03:8c:d3:af
216 138.413125	20:52:b7:ea:d0:48	08:22:09:b3:d0:0c
219 138.506751	b8:b3:17:db:e0:f9	5c:c2:53:2b:dc:18
221 138.517250	bc:74:67:6a:e8:65	f4:19:da:65:16:db
223 138.526251	c0:e4:e4:a2:52:11	24:5b:ac:e6:ee:2d
240 139.882261	ac:cf:e0:05:b3:11	d4:13:24:6a:0e:9c
242 139.964268	e4:0a:86:fb:92:31	20:ff:2e:cc:42:49
244 139.982007	54:be:1c:f2:bf:ee	84:54:63:45:14:00
246 140.040251	2c:3c:cf:00:be:e7	b0:36:19:65:f1:02
250 140.051001	9c:fb:8f:09:3a:57	64:04:97:7b:d6:0c
251 140.054379	c0:ed:e6:c3:d2:3d	4c:76:13:99:2c:95
252 140.057627	1c:e1:50:d4:e8:5d	4c:a8:c6:17:99:96
254 140.106503	0c:21:fe:a0:4f:bd	f4:4e:9c:03:d4:8d
256 140.213499	84:a5:89:e0:62:d7	64:08:6e:a6:d3:14
261 140.224015	44:a8:b1:b0:c2:35	04:f9:4b:70:8f:53
263 140.227499	04:cf:be:ba:26:37	4c:a1:45:0c:95:98

(b)

Figure 2: (a) Process of MAC addresses encryption in Layer 2. (b) Packet monitor image in Layer 2. MAC addresses are encrypted in every packet.

encryption option. The Internet key exchange process

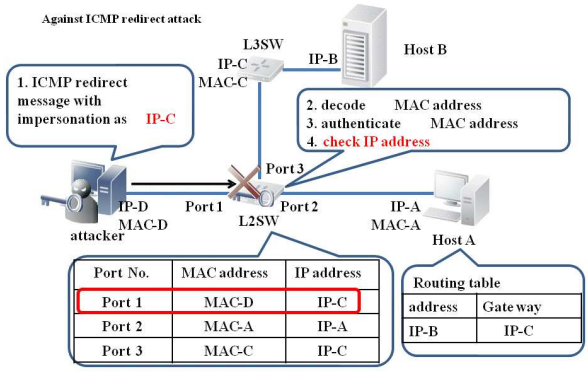


Figure 3: Protection from IP address spoofing. In the layer 2 "switch", decrypted MAC address and IP address are checked.

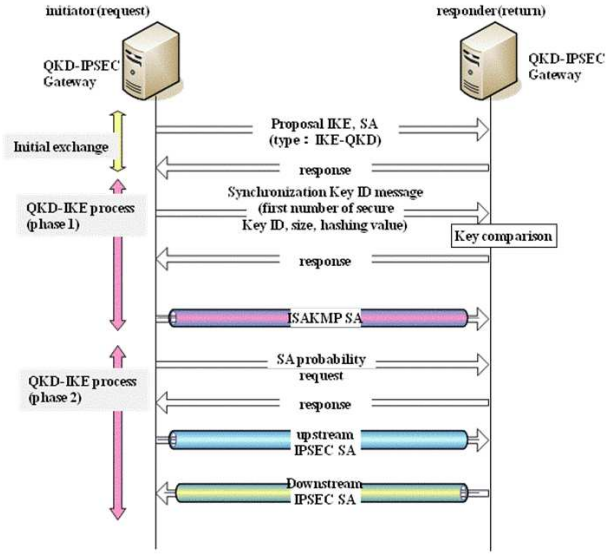


Figure 4: Internet key exchange (IKE) protocol using "QKD System". Secure key is fed from the "QKD system". IKE can be finished without complex calculation. Internet Security Association and Key Management Protocol Security Association (ISAKMP SA) is a generic name of exchanging authentication and encrypted data.

with a "QKD system" is shown in Figure 4. We obtain information-theoretical secure communication through an IP-based network without complex calculation often required in modern cryptography which slows down an effective data transmission rate. Such a secure network switch enables us to use various applications with high security. The packet structure of IPSEC in our "switch" is shown in Figure 5. Tunneling mode is employed. Figure 6 shows the operation image of the Layer 3 "switch". Moreover, a secure key is used to make the message au-

thentication code. We adopt Wegman-Carter authentication [10] to extract message digest. In this process, we use Universal$_2$ hash function. Figures 7(a) and (b) show the processes in the Universal$_2$ hash function and Wegman-Carter authentication, respectively. The one-time pad encoding makes sure no information about the message digest leaks to an eavesdropper. When 12000-bit data are hashed with the Wegman-Carter algorithm, 2048 bits of secure key is used in our system. Our network "switch" simultaneously encrypts and authenticates data with unconditional security.

Our current Layer 3 "switch" consists of a PC-based 100 Mbps router. The throughput of this switch with one-time pad encryption (and AES encryption) is more than 80 Mbps. However, when the authentication function is activated, the throughput falls drastically due to heavy computation load. In the future, the implementation will be made on a dedicated hardware such as the field programmable gate array instead of PCs and the throughput will not degrade.

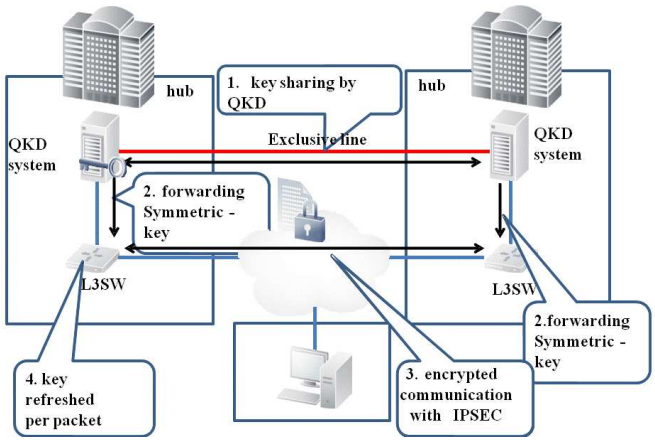


Figure 6: Conceptual view of Layer 3 "switch" connected to the "QKD system"

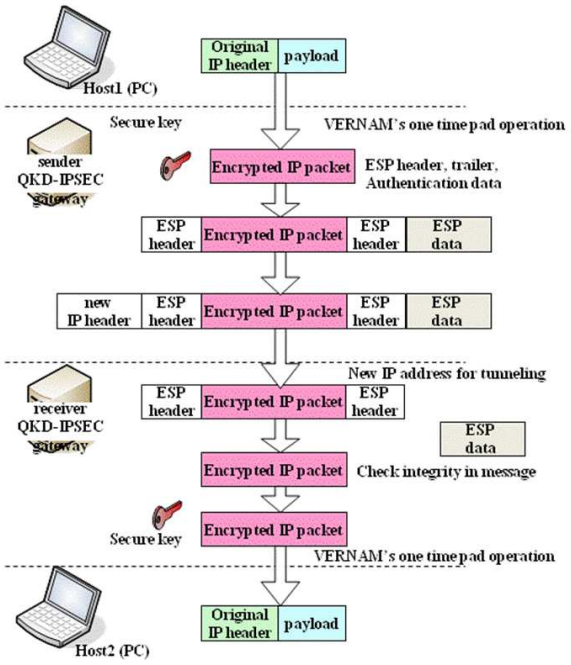


Figure 5: Packet structure of IPSEC with "QKD system". In Encapsulating Security Payload (EPS) data, message digest is stored. Secure key is used in encryption and authentication process in one-time pad manner.

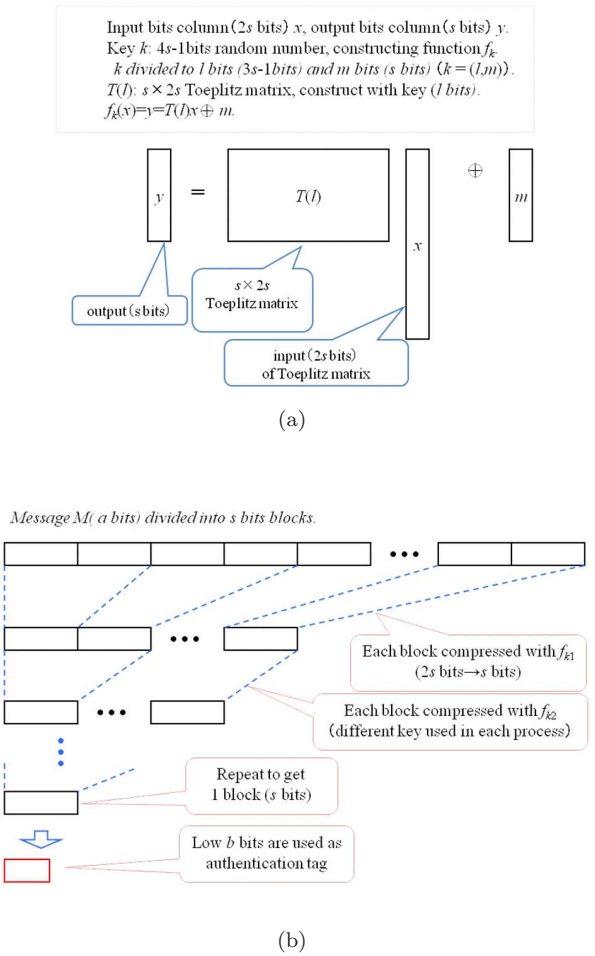


Figure 7: (a) Toeplitz matrix strongly Universal$_2$ hash function. (b) Wegman-Carter authentication.

These functions are used in making authentication data. If the message is composed of z blocks, where each block length is s bits, then the affine transformation defined by Toeplitz matrix and column vector is applied *z-1* times to obtain the authentication tag. Since a *4s-1* bit random sequence is used for each transformation, *(z - 1)(4s - 1)* bit randomness must be prepared in total. To save the random bits prepared by the QKD, we have other choices such as " evaluation hash function", and "division hash function". By employing the evaluation hash function (EFH) as an example, the message M of length ts bits is first divided into t blocks, de-

noted by $M_{t-1} \ldots, M_0$, and then the polynomial $P(x) = M_{t-1}x^{t-1} + M_{t-2}x^{t-2} + \ldots + M_0$ (on some suitable field) is generated. Finally, the authentication tag of the message M becomes $P(r)r$, where$r$ is a random sequence. Thus in this case, the randomness used is only r of length s bits.

4 Secure Key Feed on Smartphone

The "QKD system" guarantees the security at data transmission. When we discuss the security of the network system, we have to consider how to identify authenticated users and store data safely. Secret sharing (SS) is a promising candidate for secure data storage, but it needs a multi-party network. Of course, SS will have affinity to the QKD network. However, we must contemplate the effective utilization of the end-to-end link. Specifically, multi-users are assumed to use the "QKD system", so user administration is very important. We have thus proposed and developed a user management system with smartphones. To access the "QKD system", passwords are given for each smartphone. When the user downloads the secure key from the "QKD system", the key management agent (KMA) checks the password and the SIM card ID in the smartphone. A shared key is used to encrypt data in accordance with the shared key ID at a sender side. At that time, the sender can set access right control on data. Figure 8 shows the conceptual diagram of the "QKD-smartphone system". Security of data transfer is guaranteed by the normal QKD operation. In this system, the smartphone is the ID device and provides the security of the stored data at the receiver side. This system can be applied to the electric medical chart. Gene information of each person will be used for medical care. Such information must be strictly prevented from leaking, because misuse negatively influences kith and kin too. Our system will contribute to improving its security level. Unfortunately, counterfeiting a SIM card is not difficult. Thus, we should consider combining the biometric authentication technique with the smartphone.

In our current system, authentication between "QKD systems" is carried out using pre-shared key. Authentication protocol using quantum channel has been proposed [6]. However, key pre-sharing using a smartphone has high reliability, and it can be matured as a personal device for authentication and privacy protection.

5 Conclusions

We have developed a QKD-based network "switch" that efficiently enables prevention of unauthorized accesses from external and internal networks. This switch will contribute to constructing the trusted node and playing an indispensable role in embedding the QKD network into the current infrastructure of secure networks. Moreover,

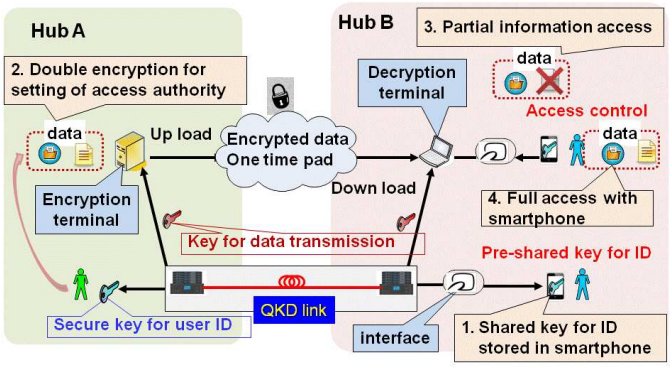


Figure 8: Conceptual diagram of "QKD-smartphone ID system". Access right control can be done using smartphones.

this "switch" can enhance convenience of the "QKD system" and provide seamless connection between QKD network and IP-based network. Poor convenience of the secret communication tool can provoke human errors that pose serious threats to the network security. Moreover, the QKD network rests with the key relay via trusted nodes. Therefore, we must make the trusted node more trustworthy. The QKD-based network "switches" and access right control using smart phones would also be useful to reduce such risks by enhancing the security while maintaining user-friendliness.

Acknowledgments

The authors thank Kenji Terada, Hirokazu Suzuki, Kenichiro Yoshino, Takao Ochi, Kaoru Shimizu, Toshimori Honjo, Kazuhiko Nakamura, Ryo Nojima and Akio Hanzawa for their support in setting up the Tokyo QKD Network and discussions.

References

[1] R. Alleaume, J. Bouda, and et al., *SECOQC white paper on quantum key distribution and cyrptography.*

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of the IEEE International Conference on Computers Systems and Signal Processing*, pp. 175–179, 1984.

[3] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, , and H. Yeh, "Current status of the DARPA quantum network," in *Quantum Information and Computation III*, pp. 138–149. SPIE, 2005.

[4] M. Fujiwara, S. Miki, T. Yamashita, Z. Wang, and M. Sasaki, "Photon level crosstalk between parallel fibers installed in urban area," *Optics Express*, vol. 18, no. 21, pp. 22199–22207, 2010.

[5] N. Gisin, G. Ribordy, W. Tittel, , and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics*, vol. 74, no. 1, pp. 145–195, 2008.
[6] K. Kanamori, S. M. Yoo, D. A. Gregory, and F. T. Sheldon, "Authentication protocol using quantum superposition states," *International Journal of Network Security*, vol. 9, no. 2, pp. 101–108, 2009.
[7] M. Peev, C. Pacher, and et al., "The SECOQC quantum key distribution network in Vienna," *New Journal of Physics*, vol. 11, no. 7, pp. 1–37, 2009.
[8] M. Sasaki, M. Fujiwara, and et al., "Field test of quantum key distribution in the tokyo QKD network," *Optics Express*, vol. 19, no. 11, pp. 10387–10409, 2011.
[9] D. Stuchi, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, "High late, long-distance quantum key distribution over 250 km of ultra low loss fibres," *New Journal of Physics*, vol. 11, no. 7, pp. 1–9, 2009.
[10] M. Wegman and L. Carter, "New hash functions and their use in authentication and set equality," *Journal of Computer and System Science*, vol. 22, no. 3, pp. 265–279, 1981.

Mikio Fujiwara received B.S. and M.S. degrees in electrical engineering from Nagoya University, Aichi Japan, in 1990 and 1992. In 2002, he received a Ph.D. degree in physics from Nagoya University. In 1992, He joined the Communications Research Laboratory, Ministry of Posts and Telecommunications, where he engaged in the development of Ge:Ga far-infrared photoconductors. Since 2000, he has been in the quantum information technology group. His current interests include single photon detectors and entanglement based QKD systems in the telecom-bands. Dr. Fujiwara is a member of the Japanese Society of Physics, and the Institute of Electronics, Information and Communication Engineers of Japan.

Tomoyasu Domeki received a B.E. degree from the College of Engineering, Nihon University, in 1991. The same year, he joined NEC Miyagi, Ltd. He is currently the manager of the software development division at NEC Communication Systems, Ltd. His interests include QKD based key management platforms for smartphones and entanglement based QKD systems in the telecom-bands.

Shiho Moriai received a B.E. degree from Kyoto University in 1993 and a Ph.D. from the University of Tokyo in 2003. She has worked at NTT Laboratories, Sony Computer Entertainment, Inc., and Sony Corporation. She has been involved in design, analysis, and standardization of cryptographic algorithms. She has also worked on designing security architectures of PlayStation platforms. Since 2013, she has been Director of Security Fundamentals Laboratory, Network Security Research Institute, NICT. She was awarded IPSJ Industrial Achievement Award in 2006 and Minister's Award of The Ministry of Economy, Trade and Industry, the Industrial Standardization Awards in 2011.

Masahide Sasaki received B.S., M.S., and Ph.D. degrees in physics from Tohoku University, Sendai Japan, in 1986, 1988, and 1992. During 1992-1996, he worked on the development of Si-MOSFETs with Ayase Laboratory, Nippon Kokan Corporation, Kanagawa Japan. In 1996, He joined the Communications Research Laboratory, Ministry of Posts and Telecommunications. Since 1994, he has worked on Quantum Information Theory and Quantum Optics. He is presently a group leader of a quantum information technology group. Dr. Sasaki is a member of the Japanese Society of Physics and the Institute of Electronics, Information and Communication Engineers of Japan.

Convertible Multi-authenticated Encryption Scheme for Data Communication

Hui-Feng Huang, Pin-Han Lin, and Min-Hsuan Tsai
(Corresponding author: Hui-Feng Huang)
Department of Computer Science and Information Engineering
National Taichung University of Science and Technology
129 Sec. 3, Sanmin Rd. Taichung 404, Taiwan
(Email: *phoenix@nutc.edu.tw)*
(Received Apr. 12, 2013; revised and accepted May 16, 2013)

Abstract

A convertible authenticated encryption scheme allows the signer to create a valid authenticated ciphertext such that only the specified receiver can simultaneously recover and verify the message. To protect the receiver's benefit of a later dispute on repudiation, the receiver has the ability to convert the signature into an ordinary one that can be verified by anyone. However, the previous proposed convertible authenticated encryption schemes are not adequate when the signers are more than one. Based on elliptic curve cryptography, this paper will propose a new efficient convertible multi-authenticated encryption scheme for mobile communication or hardware-limited users. The proposed scheme provides the following advantages: (1) The size of the generated authenticated ciphertext is independent of the number of total signers. (2) The signature is cooperatively produced by a group of signers instead of a signal signer. (3) Except for the designated recipient, no one can derive the signed message and verify its corresponding signature. (4) When a later dispute on repudiation, the receiver has the ability to prove the dishonesty of the signers by revealing an ordinary signature that can be verified by any verifier (or judge) without the cooperation of the signers. (5) The computation costs for the verifier will not significantly increase even if the signer group is expanded. Moreover, we also proposed the convertible multi-authenticated encryption protocol in multi-verifier setting for applications.

Keywords: Elliptic curve cryptography, mobile communication, multi-authenticated encryption, multi-verifier

1 Introduction

A digital signature on an electronic document plays the same role as a handwritten signature does on paper documents. Its main purpose is to specify the person responsible for the document. In some applications of the Internet, transmitted messages are compulsorily transformed into a ciphertext for satisfying the integrity, confidentiality, authenticity, and non-repudiation requirements. It is not necessary for anyone to verify the validity of the signature while keeping the message secret from the public. For example, the use of credit cards only needs to be verified by the credit card company. The straightforward approach is that a signer uses the specified receiver's encryption key to encrypt both the generated signature and the message. In this way, only the specified receiver can recover both the message and its corresponding signature and then check the validity of the signature. However, this method is costly in terms of the computational complexities and the communication overheads. To improve the efficiency, some researchers such as Horster et al. [7] developed authenticated encryption schemes by modifying from Nyberg-Rueppel's scheme [12]. In the authenticated encryption scheme, the signer may make a signature-ciphertext for a message and send it to a specified recipient. Only the specified recipient has the ability to recover and verify the message. But these authenticated encryption schemes are not digital signature schemes, no one except the specified receiver can be convinced of the signer's valid signature. Further, consider the case of a later dispute, e.g., the credit card user denies having signed a signature. In this situation, the credit card company should have the ability to prove the dishonesty of those users. Then, it might be required to reveal the message along with its signature for verifying. To protect the recipient in case of a later dispute, some schemes [22] utilize an interactive repudiation settlement procedure between the recipient and the third party. It is inefficient due to the interactive communication. In 1999, based on Horster et al.'s scheme, Araki et al. proposed a limited verifier signature scheme and a convertible limited verifier signature scheme in which a receiver can convert a limited verifier signature into an ordinary digital signature [1, 2]. In this way, as the signer denies the signature, the receiver can prove the dishonesty of the signer by revealing an ordinary signature that can be verified by any verifier (or judge). However, the conversion of the signature requires the signer to release one more parameter. This results in a further communication burden. In addition, it may be

unworkable if the signer is uncooperative. Later, Wu and Hsu [18] proposed a convertible authenticated encryption scheme that can easily produce the ordinary signature without the cooperation of the signer, and their scheme is more efficient than Araki et al.'s in terms of the computation complexities and the communication costs. Since then, some similar schemes have been proposed [3, 4, 8, 10, 15, 16, 18, 20, 21].

In the applications for organizations of enterprises, a decisional document is sometimes signed by two or more senior managers. Then, these above mentioned convertible authenticated encryption schemes have a weakness [16]. Their schemes cannot work, when the signers are more than one. In order to improve this weakness, in 2008, Wu et al. first proposed a convertible multi-authenticated encryption scheme [19]. Their scheme provides that the size of generated authenticated ciphertext is independent of the number of the total participating signers and the signature is cooperatively produced by a group of signers instead of a single signer. However, in 2009, Tsai found that the computational complexity of Wu et al.'s scheme is rather high and message redundancy is used. To improve the computational efficiency and remove the message redundancy, Tsai proposed a new convertible multi-authenticated encryption with one-way hash function [16].

With the rapid progress of wireless mobile communication, more and more people need secure transactions by cell phone for the electronic commerce. The security and efficiency are both important requirements for mobile communications. Due to the limitations of bandwidth and computation, it is necessary to construct low-computation and communication for convertible multi-authenticated encryption. Therefore, based on elliptic curve cryptography (ECC) [9] and Schnorr's [14] signature scheme, this article will propose a new efficient convertible multi-authenticated encryption scheme for mobile units or hardware-limited users. Moreover, the proposed scheme provides the following advantages: (1) The size of the generated authenticated ciphertext is independent of the number of total signers. (2) The signature is cooperatively produced by a group of signers instead of a signal signer. (3) Except for the designated recipient, no one can derive the signed message and verify its corresponding signature. (4) In case of a later dispute on repudiation, the receiver has the ability to prove the dishonesty of the signers by revealing an ordinary signature that can be verified by any verifier (or judge) without the cooperation of the signers. (5) The computation costs for the verifier will not significantly increase even if the signer group is expanded. Moreover, we also proposed a convertible multi-authenticated encryption protocol in multi-verifier setting for some applications. It allows a group of verifiers to cooperatively recover and confirm the valid authenticated ciphertext.

This paper is organized as follows. In the next section, it will present the necessary related works of the proposed scheme. In Section 3, we will introduce the proposed convertible multi-authenticated encryption scheme. The security analyses and the performances of the proposed scheme are discussed in Section 4. Some conclusions will be made in the last section.

2 Preliminaries

Before a new dynamic access control in sensor networks based on elliptic curves is proposed, this session first introduces the properties of elliptic curves that will allow us to discuss the security of the proposed scheme in Section 4 [9].

An elliptic curve is generally given by

$$y^2 = x^3 + ax^2 + bx + c. \quad (1)$$

Let q be a prime number larger than 3. An elliptic curve modulo q, E_q is the set of solutions (x,y) satisfying

$$y^2 = x^3 + ax^2 + bx + c \bmod q. \quad (2)$$

Here we take x and y to be in a fixed complete residue system modulo q, so E_q is a finite set. The group law on an elliptic curve is defined when the discriminant is nonzero, where the discriminant of the curve in Equation (2) is

$$\Delta = 27c^2 + 4a^3c + 4b^3 - a^2b^2 - 8abc \bmod q.$$

Again, the point at infinity is O. The rules for addition of points on E_q apply with the interpretation that the reciprocal is the inverse modulo q. When the inverse modulo q does not exist, then the corresponding line is "vertical" modulo q. Suppose that two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$. The rules are as follows.

If $x_1 = x_2 \bmod q$, then $P_1 + P_2 = O$. If $y_1 = 0 \bmod q$, then $P_1 = -P_1$ and $2P_1 = O$. In other cases, the sum $P_1 + P_2$ is obtained by computing $\lambda = \frac{y_1 - y_2}{x_1 - x_2} \bmod q$, if $P_1 \neq P_2$, or $\lambda = \frac{3x_1^2 + 2ax_1 + b}{2y_1} \bmod q$, if $P_1 = P_2$, and then let $x_3 = \lambda^2 - a - x_1 - x_2 \bmod q$.

Hence, $P_1 + P_2 = (x_3, y_3)$, where $y_3 = \lambda(x_1 - x_3) - y_1 \bmod q$. Then, it preserves the addition rules hold for all P, $Q \in E_q$, and O is neutral element. Moreover, if the number of elements on E_q is n, then for every point P on E_q, it has $nP = O \bmod q$.

In the elliptic curve cryptosystems, the elliptic curve discrete logarithm problem in E_q is the following: Given $P \in E_q$ with order n (That is $nP = O$) and Q is a point in the cyclic group $G = \langle P \rangle$. It is intractable to find r such that $Q = rP$. Moreover, according to the Diffie-Hellman algorithm over elliptic curve, it has that $t_2A_1 = t_2(t_1P) = t_1(t_2P) = t_1A_2 = t_1t_2P$ over elliptic curve E_q,

where $A_1 = t_1 P$ and $A_2 = t_2 P$ for any positive integers t_1 and t_2.

3 The Proposed Scheme

In this section, we will propose a convertible multi-authenticated encryption scheme based on the elliptic curve cryptosystem (ECC) [9] and Schnorr's [14] signature scheme. There are three phases in our scheme: the signing encryption, the message recovery and the signature conversion phases. In the signing encryption phase, the group of signers can construct the authenticated ciphertext to some specified recipient. In the message recovery phase, only the specified recipient has the ability to recover the ciphertext and verify the message. When a later dispute on repudiation, in the signature conversion phase, the recipient can reveal the converted multi-signature and then any one (or judge) can prove the dishonesty of the signers without the cooperation of the group of signers. Initially, the system authority (SA) chooses a large prime number q ($q \approx 2^{160}$) and an elliptic curve E_q (the elliptic curve E is over the finite field F_q); a cyclic group $G = \langle P \rangle$ of points over the elliptic curve E_q, where the point P is the generator of the group and has an order n of at least 160 bits. It provides $nP = O$ and the point at infinity is O. SA also selects a secure one-way hash function $h(\ )$. Then, SA publishes the elliptic curve E_q, P, n, and $h(\ )$. Each signer in the system, U_i, owns a secret key x_i over the elliptic curve E_q and computes the corresponding public key $Q_i = x_i P$ of the point over the elliptic curve E_q. Moreover, the recipient V has a secret key x_b and its corresponding public key $B = x_b P$ of the point over the elliptic curve E_q. Without loss of generality, let $SG = \{U_1, U_2, \cdots, U_t\}$ be the signing group, V the recipient, and M the message to be signed. According to the concept of elliptic curves public key cryptosystem and Schnorr's signature scheme, each signer $U_i \in SG$ performs the following steps in the signature encryption phase.

3.1 The Signature Encryption Phase

1. Each signer $U_i \in SG$ selects a random number k_i to computes the point $R_i = k_i P = (R_i^x, R_i^y)$ over the elliptic curve E_q and broadcasts R_i to $U_j \in SG \setminus \{U_i\}$, where R_i^x and R_i^y are the x-component and y-component of point R_i, respectively.
2. Upon receiving R_j from $U_j \in SG \setminus \{U_i\}$, U_i computes two points $R = \sum_{i=1}^{t} R_i$ and $Z = tMP + R = (Z^x, Z^y)$ over the elliptic curve E_q, $r = h(M \| Z^x \| Z^y)$, and $s_i = M + k_i - x_i r$, where t is the number of group signers SG, Z^x and Z^y are the x-component and y-component of point Z, respectively. Next, U_i sends (s_i, R_i) to $U_j \in SG \setminus \{U_i\}$.
3. After receiving (s_j, R_j) from $U_j \in SG \setminus \{U_i\}$, U_i verifies $MP + R_j = s_j P + rQ_j$ over the elliptic curve E_q, where $r = h(M \| Z^x \| Z^y)$, Q_j is the public point of signer U_j, and "//" denotes concatenation. If it holds, proceed to the next step; else s_j is requested to be signed and sent again.
4. When all (s_j, R_j)'s are collected and verified, the clerk, who can be any signer in SG, computes the value $s = \sum_{i=1}^{t} s_i \mod n$, the point $D = tMB = (D^x, D^y)$ over the elliptic curve E_q, and $C = M \oplus D^x$, where D^x is the x-component of point D and "$\oplus$" denotes the exclusive or operator. Note that B is the public point (key) of the designated recipient V. Then, the clerk sends (C, R, s, r) to the recipient V.

Here, the authenticated ciphertext for the message M is (C, R, s, r), which is sent to the verifier V. We first show the correctness of equation $MP + R_j = s_j P + rQ_j$ in the following. It provides that $s_i = M + k_i - x_i r$, then

$$s_i P = MP + k_i P - x_i rP,$$

therefore, $s_i P + rQ_i = MP + R_i$ over the elliptic curve E_q, where $r = h(M \| Z^x \| Z^y)$, $Q_i = x_i P$, and $R_i = k_i P$.

3.2 The Message Recovery Phase

After receiving the signature (C, R, s, r), V performs the following two steps to recover the message M and verify the signature.

1. Compute two points $Z = sP + r\sum_{i=1}^{t} Q_i = (Z^x, Z^y)$ and $D = x_b(Z - R) = (D^x, D^y)$ over the elliptic curve E_q, where x_b is secret key of V.
2. Recover the message M as $M = C \oplus D^x \mod q$.

Then, V can verify the signature with the following equality:

$$r = h(M \| Z^x \| Z^y). \quad (3)$$

If it holds, the signature is valid. Hence, the recipient V confirms this secret message M and its signature were sent by the group signers $SG = \{U_1, U_2, \cdots, U_t\}$. For the security of Schnorr's signature scheme, the random number k_i should not be reused. We show the correctness of

equations $Z = sP + r\sum_{i=1}^{t} Q_i = (Z^x, Z^y)$ and $D = x_b(Z - R) = (D^x, D^y)$ over the elliptic curve E_q in the following.

The proposed scheme has $s = \sum_{i=1}^{t} s_i = \sum_{i=1}^{t} (M + k_i - rx_i)$, then $sP = \sum_{i=1}^{t} (MP + k_i P - rx_i P) = tMP + \sum_{i=1}^{t} R_i - r\sum_{i=1}^{t} Q_i$ over the elliptic curve E_q, it provides that

$$Z = sP + r\sum_{i=1}^{t} Q_i = tMP + R = (Z^x, Z^y), \quad (4)$$

Hence,

$$D = x_b(Z - R) = x_b(tMP) = tMB \text{ over } E_q \quad (5)$$

, and

$$M = C \oplus D^x = (M \oplus D^x) \oplus D^x \quad (6)$$

where $B = x_b P$ is the public point of V *over the elliptic curve E_q.*

3.3 The Signature Conversion Phase

In case of later dispute on repudiation, *V* can prove the dishonesty of the group signers $SG = \{U_1, U_2, \cdots, U_t\}$ by revealing the message *M* for the converted signature (*r*, *s*). With this converted signature, anyone (or judge) can compute $Z = sP + r\sum_{i=1}^{t} Q_i = (Z^x, Z^y)$ and verify its validity from equation $r = h(M \| Z^x \| Z^y)$. This phase is for the specified recipient to convince the judge that a signature is the signers' true one if it is valid.

In our signature conversion phase, only the recipient can reveal the message *M* and the converted signature (*r*, *s*) for any verifier to compute $Z = sP + r\sum_{i=1}^{t} Q_i = (Z^x, Z^y)$ and check whether Equation (3) holds or not. Therefore, the group signers $SG = \{U_1, U_2, \cdots, U_t\}$ cannot repudiate that they ever sent the message *M* to the recipient *V*. It is obvious that our convertible multi-authenticated encryption scheme can easily produce the ordinary signature without the cooperation of the multi-signers. Therefore, it is very convenient for the document's signers to clarify the responsibility.

3.4 Figures and Tables Format

The proposed convertible multi-authenticated encryption can be easily updated into multi-signer and multi-verifier setting for the applications. The system initialization is the same as in this Section 3. Without loss of generality, let $SG = \{U_1, U_2, \cdots, U_t\}$ be the signing group, $VG = \{V_1, V_2, \cdots, V_g\}$ the recipient group, and *M* the message to be signed. Moreover, each recipient V_i in *VG* has a secret key d_i and its corresponding public key $B_i = d_i P$ of the point over the elliptic curve E_q. Each signer in the system, U_i, owns a secret key x_i over the elliptic curve E_q and computes the corresponding public key $Q_i = x_i P$ of the point over the elliptic curve E_q. We depict these three phases for multi-verifier setting as follows.

3.5 The Signature Encryption Phase for Multi-verifier

1. Each signer $U_i \in SG$ selects a random number k_i to computes the point $R_i = k_i P = (R_i^x, R_i^y)$ over the elliptic curve E_q and broadcasts R_i to $U_j \in SG \setminus \{U_i\}$, where R_i^x and R_i^y are the *x*-component and *y*-component of point R_i, respectively.
2. Upon receiving R_j from $U_j \in SG \setminus \{U_i\}$, U_i computes two points $R = \sum_{i=1}^{t} R_i$ and $Z = tMP + R = (Z^x, Z^y)$ over the elliptic curve E_q, $r = h(M \| Z^x \| Z^y)$, and $s_i = M + k_i - x_i r$, where *t* is the number of group signers *SG*, Z^x and Z^y are the *x*-component and *y*-component of point *Z*, respectively. Next, U_i sends (s_i, R_i) to $U_j \in SG \setminus \{U_i\}$.
3. After receiving (s_j, R_j) from $U_j \in SG \setminus \{U_i\}$, U_i verifies $MP + R_j = s_j P + rQ_j$ over the elliptic curve E_q, where $r = h(M \| Z^x \| Z^y)$, Q_j is the public point of signer U_j, and "//" denotes concatenation. If it holds, proceed to the next step; else s_j is requested to be signed and sent again.
4. When all (s_j, R_j)'s are collected and verified, the clerk, who can be any signer in *SG*, computes the value $s = \sum_{i=1}^{t} s_i \bmod n$, the point $D = tM(\sum_{i=1}^{g} B_i) = (D^x, D^y)$ over the elliptic curve E_q, and $C = M \oplus D^x$, where D^x is the *x*-component of point *D* and "$\oplus$" denotes the exclusive or operator. Note that B_i is the public point (key) of the designated recipient V_i of *VG*. Then, the clerk sends (C, R, s, r) to the recipient group *VG*.

It is obvious that $D = tM(\sum_{i=1}^{g} B_i)$

$$= tM(B_1 + B_2 + ... + B_g)$$
$$= tM(d_1 P + d_2 P + ... + d_g P) = (D^x, D^y)$$

Here, the authenticated ciphertext for the message *M* is (C, R, s, r), which is sent to the verifier group *VG*. In the signature encryption phase for multi-verifier setting, the

Steps 1, 2, and 3 are the same as the above signature encryption phase. The only difference is in the Step 4 between the above signature encryption phase and the signature encryption phase for multi-verifier setting.

3.6 The Message Recovery Phase for Multi-Verifier

After receiving the signature (C, R, s, r), *VG* performs the following two steps to recover the message *M* and verify the signature.

1. Each V_i of *VG* computes two points $Z = sP + r\sum_{i=1}^{t} Q_i = (Z^x, Z^y)$ and $D_i = d_i(Z - R)$ over the elliptic curve E_q and broadcasts D_i to $V_j \in VG \setminus \{U_j\}$, where d_i is secret key of V_i.
2. Upon receiving D_j from $V_j \in VG \setminus \{V_i\}$, each V_i of *VG* can compute the point $D = \sum_{i=1}^{g} D_i = (D^x, D^y)$.
3. Recover the message *M* as $M = C \oplus D^x$ mod *q*. Then, each V_i of *VG* can verify the signature with the following equality:

$$r = h(M \| Z^x \| Z^y).$$

If it holds, the signature is valid. Hence, the recipient V_i of *VG* confirms this secret message *M* and its signature were sent by the group signers $SG = \{U_1, U_2, \cdots, U_t\}$. For the security of Schnorr's signature scheme, the random number k_i should not be reused. We show the correctness of equations $Z = sP + r\sum_{i=1}^{t} Q_i = (Z^x, Z^y)$ and

$D = (d_1 + d_2 + ... + d_g)(Z - R) = tM(\sum_{i=1}^{g} B_i) = (D^x, D^y)$ over the elliptic curve E_q in the following.

The proposed scheme has $s = \sum_{i=1}^{t} s_i = \sum_{i=1}^{t} (M + k_i - rx_i)$, then

$sP = \sum_{i=1}^{t} (MP + k_i P - rx_i P) = tMP + \sum_{i=1}^{t} R_i - r\sum_{i=1}^{t} Q_i$ over the elliptic curve E_q, it provides that

$$Z = sP + r\sum_{i=1}^{t} Q_i = tMP + R = (Z^x, Z^y), \quad (7)$$

Hence, $D_i = d_i(Z - R) = d_i(tMP) = tMB_i$ over E_q, and (8)

$$D = (d_1 + d_2 + ... + d_g)(Z - R) = tM(\sum_{i=1}^{g} B_i) = \sum_{i=1}^{g} D_i = (D^x, D^y) \quad (9)$$

$$M = C \oplus D^x = (M \oplus D^x) \oplus D^x, \quad (10)$$

where $B_i = d_i P$ is the public point of *V* over the elliptic curve E_q.

3.7 The Signature Conversion Phase for Multi-verifier

In case of later dispute on repudiation, the verifier group *VG* can prove the dishonesty of the group signers $SG = \{U_1, U_2, \cdots, U_t\}$ by revealing the message *M* for the converted signature (*r*, *s*). With this converted signature, anyone (or judge) can compute $Z = sP + r\sum_{i=1}^{t} Q_i = (Z^x, Z^y)$ and verify its validity from equation $r = h(M \| Z^x \| Z^y)$. This phase is for the specified recipient of *VG* to convince the judge that a signature is the signers' true one if it is valid.

In our signature conversion phase for multi-verifier, only the recipient of verifier group can reveal the message *M* and the converted signature (*r*, *s*) for any verifier to compute $Z = sP + r\sum_{i=1}^{t} Q_i = (Z^x, Z^y)$ and check whether Equation $r = h(M \| Z^x \| Z^y)$ holds or not. Therefore, the group signers $SG = \{U_1, U_2, \cdots, U_t\}$ cannot repudiate that they ever sent the message *M* to the recipient group *VG*. It is obvious that our convertible multi-authenticated encryption scheme for multi-verifier setting can easily produce the ordinary signature without the cooperation of the multi-signers. Therefore, it is very convenient for the document's signers to clarify the responsibility.

4 Discussions

In this section, we are going to explore the securities and the performances of the proposed scheme.

4.1 Security Analyses

In our scheme, both encrypting and signing are based on the ECC and Schnorr's signature scheme, respectively. Thus, the security of proposed scheme is founded in the difficulty of solving the discrete logarithm problem in E_q. We will review some security terms needed for security analysis [5, 9].

Definition 1. A *secure hash function, h( ): $x \to y$, is one-way, if given x, it is easy to compute $h(x) = y$; however, given y, it is hard to compute $h^{-1}(y) = x$.*

Definition 2. *The elliptic curve discrete logarithm problem (ECDLP) in E_q is as follows: Given $P \in E_q$ with order n (That is nP = O) and Q is a point in the cyclic group $G = \langle P \rangle$. It is intractable to find r such that Q = rP.*

Definition 3. *The elliptic curve computational Diffie-Hellman problem (ECDHP) is as follows: Given t_1P and t_2P over elliptic curve E_q, it is hard to compute t_1t_2P for*

any positive integers t_1 *and* t_2 .

In the proposed scheme, any signer U_i 's private key x_i must be kept secret. From public key $Q_i = x_i P$ of the group signer *SG* over the elliptic curve E_q , no one can easily derive the corresponding private key x_i . This security results from the difficulty of solving the elliptic curve discrete logarithm problem (ECDLP). Moreover, in our scheme, the ordinary signature is embedded in the authenticated encryption signature. Thus, the receiver can easily release the converted signature to any verifier (or judge) when the group signers *SG* deny their having signed.

First, we consider the confidentiality in the proposed convertible multi-authenticated encryption scheme, each signer $U_i \in SG$ selects a random number k_i to computes the point $R_i = k_i P = (R_i^x, R_i^y)$ over the elliptic curve E_q and then broadcasts R_i to $U_j \in SG \setminus \{U_i\}$ .Next, each U_i computes two points $R = \sum_{i=1}^{a} R_i$ and $Z = tMP + R = (Z^x, Z^y)$ over E_q , and applies the concept of Schnorr's signature scheme to construct $r = h(M \| Z^x \| Z^y)$ and $s_i = M + k_i - x_i r$. Finally, the clerk of *SG* computes the value $s = \sum_{i=1}^{t} s_i$ and the point $D = tMB = (D^x, D^y)$ over E_q , and then generates the ciphertext *C* of *M* by computing $C = M \oplus D^x$, where $B = x_b P$ is the public point of receiver *V*. Then, the clerk delivers the signature (C, R, s, r) to the specified recipient *V*. After receiving (C, R, s, r) , *V* computes the point $Z = sP + r\sum_{i=1}^{t} Q_i = (Z^x, Z^y)$, and then uses his secret key x_b to derive $D = x_b(Z - R) = x_b tMP = tMB$ and recovers the message $M = C \oplus D^x$. Next, *V* can confirm that the message *M* is sent from signers *SG* by checking $r = h(M \| Z^x \| Z^y)$ holds.

In the proposed scheme, from the information (C, R, s, r) , anyone can derive $Z = sP + r\sum_{i=1}^{t} Q_i = (Z^x, Z^y)$ and compute (*Z*-*R*). However, without knowing *V*'s secret key x_b , no one can easily derive $D = x_b(Z - R) = tMB$ and recover the message $M = C \oplus D^x$. This is the elliptic curve computational Diffie-Hellman problem (ECDHP). For given $tMP = (Z - R)$ and $tB (tB = tx_b P)$, it is very difficult to find $tMB = tx_b MP$. In addition, based on ECDLP, it is intractable to find x_b such that $B = x_b P$. Therefore, it can provide the confidentiality in the proposed convertible multi-authenticated encryption.

For the unforgeability security, in our method, it is very hard to derive k_i from the point $R_i = k_i P$. This security also results from the difficulty of solving the elliptic curve discrete logarithm problem (ECDLP) and Schnorr's signature scheme. Even if the message *M* is known, without k_i , it is not easily for the attacker to obtain signer U_i 's secret key x_i from $s_i = M + k_i - x_i r$. We see that the probability of obtaining x_i and k_i from current s_i , $R_i = k_i P$, and r is equivalent to performing an exhaustive search on x_i and k_i . Thus, the attacker cannot easily to masquerade the signer U_i .

Moreover, the adversary can produce an authenticated ciphertext (C^*, R^*, s^*, r^*) for message M^* under the private key of the designated recipient. If M^* satisfies $r^* = h(M^* \| Z^{*x} \| Z^{*y})$, then the multi-signature (s^*, r^*) can be regarded as a valid multi-signature for the message M^* with respect to the group public key $\sum_{i=1}^{t} Q_i$ of *SG*, where $Z^* = sP + r\sum_{i=1}^{t} Q_i = (Z^{*x}, Z^{\bullet y})$. However, based on the secure hash function *h*( ), it is difficult to find M^* such that $r^* = h(M^* \| Z^{*x} \| Z^{*y})$. The probability of obtaining the exactly $r^* = h(M^* \| Z^{*x} \| Z^{*y})$ is equivalent to performing an exhaustive search on M^* . By applying the Schorr's signature scheme, for $r = h(M \| Z^x \| Z^y)$ and $s_i = M + k_i - x_i r$ ($s = \sum_{i=1}^{t} s_i$), without the group signer's private key x_i , anyone cannot forge the signature (*r*, *s*) for the message *M*, where k_i is a secret random number of the group signer of U_i . It can be resistant the forgery under the chosen-message attacks. Hence, anyone cannot masquerade as a signer U_i or the group signers *SG* to forge the valid signature-ciphertext (C, R, s, r) and send it to a specified recipient *V*. For the security of Schnorr's signature scheme, the secret random number k_i should not be reused for any message.

Next, the proposed convertible multi-authenticated encryption for multi-verifier setting is extension of the convertible multi-authenticated encryption scheme. After receiving (C, R, s, r) , each V_i of *VG* can compute the point $Z = sP + r\sum_{i=1}^{t} Q_i = (Z^x, Z^y)$, and then use his secret key d_i to derive $D_i = d_i(Z - R) = d_i tMP = tMB_i$ and send D_i to other V_j of *VG*. After receiving all D_j of V_j , then each V_i could compute $D = \sum_{i=1}^{g} D_i = (D^x, D^y)$ and recover

the message $M = C \oplus D^x$. Next, each V_i can confirm that the message is sent from signers *SG* by checking $r = h(M \| Z^x \| Z^y)$ holds.

In the proposed method, from the information (C, R, s, r), anyone can derive $Z = sP + r\sum_{i=1}^{t} Q_i = (Z^x, Z^y)$ and compute (*Z*-*R*). However, without knowing V_i 's secret key d_i, no one can easily derive $D_i = d_i(Z - R) = tMB_i$ and recover the message $M = C \oplus D^x$, where $D = \sum_{i=1}^{g} D_i = (D^x, D^y)$. This is the elliptic curve computational Diffie-Hellman problem (ECDHP). For given $tMP = (Z - R)$ and $tB_i (tB_i = td_iP)$, it is very difficult to find $tMB_i = td_iMP$. In addition, based on ECDLP, it is intractable to find d_i such that $B_i = d_iP$. Therefore, it can provide the confidentiality in the proposed convertible multi-authenticated encryption. Therefore, only the verifier group *VG* can recover the message *M* and confirm that the message is sent from signers *SG*. It is obvious that the security of the proposed convertible multi-authenticated encryption for multi-verifier setting is same as the proposed convertible multi-authenticated encryption protocol.

4.2 Performances and Comparisons

The concept of convertible multi-authenticated encryption was first proposed by Wu *et al*. [19]. To improve the computational efficiency and remove the message redundancy for the Wu *et al*.'s scheme, in 2009, Tsai proposed a new convertible multi-authenticated encryption with one-way hash function [16]. For this reason, we only compare our convertible multi-authenticated encryption scheme with Tsai's scheme [16]. For convenience, we define related notations to analyze the computational complexity. The notation Te_m means the time for one multiplication computation over an elliptic curve, Te_a denotes the time for one modular addition computation over an elliptic curve, T_e means the time for one modular exponentiation computation, T_m is the time for performing a modular multiplication computation, and T_h denotes the time for executing the adopted one-way hash function in one's scheme. Here, the modular addition computation Te_a for two points in elliptic curve E_q is similar to the operation that of a modular multiplication computation T_m in Z_q. Note that the times for computing exclusive-or, modular addition, and subtraction are ignored, since they are much smaller than Te_m, Te_a, T_e, T_m, and T_h.

In the proposed method, the most expensive operation is the point multiplication of the form *kP* and *P* is a cyclic group of points over an elliptic curve E_q [9, 11, 17]. Compared to RSA, ECC can achieve the same level of security with smaller key sizes [9, 11]. It has been shown that 160-bit ECC provides comparable security to 1024-bit RSA [13] and 224-bit ECC provides comparable security to 2048-bit RSA [17]. Gura *et al*. [6] evaluated the assembly language implementations of ECC and RSA on the Atmel ATmega128 processor [18], which is popular for sensor platform such as Crossbow MICA Motes. In their implementation, a 160-bit point multiplication of ECC requires only 0.81s, while 1024-bit RSA public key operation and private key operation require about 0.43s and 10.99s, respectively. Therefore, under the same security level, smaller key sizes of ECC could offer faster computation, as well as memory, energy and bandwidth savings. Hence, Te_m is more efficient than a modular exponentiation computation T_e.

Table 1: Comparisons of Tsai's scheme and the proposed scheme in computation costs

	Tsai's scheme	The proposed scheme
Signature encryption (for each signer and the clerk)	$T_h + (2t+1)T_e + 2tT_m$	$T_h + (2t+2)Te_m + 2tTe_a$
Message recovery and verification	$T_h + 3T_e + tT_m$	$T_h + 3Te_m + tTe_a$
Signature conversion	**0**	**0**
Verifying converted signature	$T_h + 2T_e + tT_m$	$T_h + 2Te_m + tTe_a$

Te_m : the time for performing a multiplication computation over an elliptic curve

Te_a : the time for performing a modular addition computation over an elliptic curve

T_e : the time for performing a modular exponentiation computation

T_m : the time for performing a modular multiplication computation

T_h : the time for performing a one-way hash function

We summarize the comparisons of our convertible mulit-authenticated encryption scheme with Tsai's scheme in Table 1. As shown in Table 1, the computational complexity for the **s**ignature encryption phase, message recovery and verification, and verifying converted signature are $T_h + (2t+2)Te_m + tTe_a$, $T_h + 3Te_m + tTe_a$, and $T_h + 2Te_m + tTe_a$, respectively. Therefore, under the same security level, smaller key sizes of ECC could offer faster computation, as well as memory, energy and bandwidth savings. It is obvious that the proposed scheme is more efficient than Tsai's scheme.

5 Conclusions

Based on ECC and Schnorr's signature scheme, we have proposed a convertible multi-authenticated encryption scheme. The proposed scheme allows a group of signers to cooperatively create a valid authenticated ciphertext for the specific recipient. In this way, only the designated recipient

has the ability to recover the message and verify the signature. Once the group signers deny the signature, the specified recipient can convert the authenticated ciphertext into an ordinary one for convincing anyone of the signers' dishonesty. In addition, we also proposed a convertible multi-authenticated encryption for multi-verifier setting. It allows a group of verifiers to cooperatively recover the valid authenticated ciphertext. Comparing with previously proposed schemes, our method is more suitable for hardware-limited users or mobile units. All of them can simultaneously achieve the security requirements of integrity, confidentiality, authenticity, and non-repudiation.

Acknowledgments

This research was partially supported by the National Science Council, Taiwan, under contract no: (101-2221-E-025-017).

References

[1] S. Araki, S. Uehara, and K. Imamura, "Convertible limited verifier signature based on horster's authenticated encryption," 1998 *Symposium on Cryptography and Information Security*.

[2] S. Araki, S. Uehara, and K. Imamura, "The limited verifier signature and its application," *IEICE Transactions on Fundamentals*, vol. E82-A, no.1, pp. 63-68, 1999.

[3] C. C. Chang and C. Y. Lee, "A smart card-based authentication scheme using user identify cryptography," vol. 15, no. 2, pp. 139-147, 2013.

[4] H. Y. Chien, "Convertible authenticated encryption scheme without using one-way hash function," *Informatica*, vol. 14, no. 4, pp. 1-9, 2003.

[5] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, pp. 644-654, 1976.

[6] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Computing elliptic curve cryptography and RSA on bit CPUs," *CHES'04*, 2004.

[7] P. Horster, M. Michels, and H. Petersen, "Authenticated encryption schemes with low communication costs," *Electronics Letters*, vol. 30, no. 15, 1994, pp. 1212-1213.

[8] S. T. Hsu, C. C. Yang, and M. S. Hwang, "A study of public key encryption with keyword search," *International Journal of Network Securiy*, vol. 15, no. 2, pp. 71-79, 2013.

[9] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, pp. 203-209, 1987.

[10] J.Lv, X, Wang, and K. Kim, "Practical convertible authenticated encryption schemes using self-certified public keys," *Applied Mathematics and Computation*, vol. 169, no. 2, pp.1285-1297, 2005.

[11] V. Miller, "Uses of elliptic curves in cryptography," *Advances in Cryptology – Crypto '85*, LNCS 218, pp. 417-426, Springer-Verlag, 1986.

[12] K. Nyberg and R. A. Rueppel, "Message recover for signature schemes based on the discrete logarithm problem," *Advance in Cryptology – Eurocrypt '94*, LNCS 950, pp. 182-193, Springer-Verlag, 1995.

[13] R. L. Rivest, A. Shamir, and L.M. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120-126, Feb. 1978.

[14] C. P. Schnorr, "Efficient identification and signatures for smart cards," *Advances in Cryptology - Crypto '89*, LNCS 435, pp. 339-351, Springer-Verlag**,** 1990.

[15] Z. Tan, "Efficient identity-based authenticated multiple key exchange protocol," *Computers and Electrical Engineering*, vol. 37. pp. 191-198, 2011.

[16] J. L. Tsai, "Convertible multi-authenticated encryption scheme with one-way hash function," *Computer Communications*, vol. 32, pp. 783-786, 2009.

[17] S. Vanstone, "Responses to NIST's proposal," *Communications of the ACM* vol. 35, pp. 50-52, July 1992.

[18] T. S. Wu and C. L. Hsu, "Convertible Authenticated Encryption Scheme," *The Journal of Systems and Software*, vol. 62, 2002, pp. 205-209.

[19] T. S. Wu, C. L. Hsu, K. Y. Tsai, H. Y. Lin, and T. C. Wu, "Convertible multi-authenticated encryption scheme," *Information Sciences*, vol. 178, pp. 256-263, 2008.

[20] J. Zhang and Y. Wang, "On the security of a convertible authenticated encryption scheme," *Applied Mathematics and Computation*, vol. 169, no. 22, pp. 1063-1069, 2005.

[21] W. Zhao, C. Lin, and D. F. Ye, "Provably secure convertible nominative signature scheme," *Information Security and Cryptology*, vol. 5487, pp. 23-40, 2009.

[22] Y. Zheng, "Signcryption and Its Applications in Efficient Public Key Solutions," *Advances in Information Security Workshop (ISW'97)*, pp. 291-312, New York, 1997.

Hui-Feng Huang received her M. S. and Ph.D. degrees in Mathematics from National Taiwan University and Computer Science and Information Engineering from National Chung Cheng University, respectively. Currently, she is a professor at the Department of Computer Science and Information Engineering in National Taichung University of Science and Technology. Her research interests focus on the areas of cryptography and information security, network security, algorithm, and electronic commerce etc.

Pin-Han Lin received the Bachelor of computer science degrees from Department of Computer Science and Information Engineering in National Taichung University

of Science and Technology, Taiwan, ROC in 2011. Currently, he is a master of Computer Science and Information Engineering student in National Taichung University of Science and Technology, Taiwan, ROC. His current research interests are in the area of cryptography, information security, network security and electronic commerce.

Min-Hsuan Tsai received the Bachelor of Art degrees from Department of applied Japanese in National Taichung University of Science and Technology, Taiwan, ROC in 2012. Currently, he is a master of Computer Science and Information Engineering student in National Taichung University of Science and Technology, Taiwan, ROC. His current research interests include cryptography, information security, network security and electronic commerce.

Simulation Study of a Many-to-One Mapping for IPv6 Address Owner Identification in an Enterprise Local Area Network

Nashrul Hakiem[1], Mohammad Umar Siddiqi[2], and Hashum Mohamed Rafiq[3]
(Corresponding author: Nashrul Hakiem)

Department of Informatics Engineering, Faculty of Science and Technology[1]
UIN Syarif Hidayatullah Jakarta, Jl. Ir. H. Juanda 95 Jakarta 15412 Indonesia
Department of Electrical and Computer Engineering, Faculty of Engineering[1,2,3]
International Islamic University Malaysia, Jalan Gombak, Kuala Lumpur 53100, Malaysia
(Email: hakiem@yahoo.com)

(Received Nov. 19, 2012; revised and accepted Aug. 15, 2013)

Abstract

Owner identification is an important aspect of improving network visibility and enhancing network security within local area networks deploying IPv6. This paper presents a simulation study for owner identification in an enterprise local area network from their IPv6 addresses. The study is based around the reverse implementation (many-to-one mapping) of a one-to-many reversible mapping. The paper reviews the many-to-one mechanism and the associated simulation software development, followed by presentation of results obtained from required functional tests. The IPv6 address data can be obtained from the output of any network monitoring software. In addition to a text format for verification, it also uses a checksum for validation which is used during the IPv6 address generation and identification. The simulation software given here can easily identify an IPv6 address owner if the IPv6 address is properly generated by the mechanism and it can display particular verification messages.

Keywords: Checksum, IPv6 address, many-to-one mapping, network monitoring, network visibility, one-to-many mapping, owner identification.

1 Introduction

Identity is one of the most important aspects within the Internet [18]. It facilitates controlling user activity and access to the network in order to improve network visibility and thus improve network security. It plays a central role in the development of the Future Internet [15].

IPv6 represents a considerable improvement compared to the previous version, IPv4. However, some potential security problems still remain and require improvement [3]. Some research work has been carried out to improve IPv6 security [8, 12] and to overcome IP address deficiency and the lack of IP address security [14].

One-to-many reversible mapping [5] is a mechanism to enhance IPv6 address generation in terms of security and privacy. This one-to-many mapping between user space and IPv6 addresses is generated cryptographically using the Cipher Feedback (CFB) mode of operation of the Advanced Encryption Standard (AES).

This paper presents IPv6 address owner identification based on many-to-one mapping, the reverse implementation of a one-to-many reversible mapping. The paper is organized as follows. An overview of related works is given in Section 2. The many-to-one mapping mechanism is detailed in Section 3. Section 4 presents the IPv6 address identification mechanism and presents the results obtained from various functional tests. Conclusions are given in Section 5.

2 Related Works

2.1 Network Monitoring

Network administrators need to be aware of and have a handle on different types of traffic that is traversing their networks. Traffic monitoring and analysis is essential in the sense that it provides a more effective way to troubleshoot and resolve issues when they occur. This helps preventing network services from a state of "stand-still" over extended periods of time [2].

There are several popular network management software packages specifically designed with emphasis on network monitoring, measurement, and analysis which are available from commercial sources and open source vendors [13]. These tools help in monitoring the enterprise network activities in real time and analyzing the network for LAN usage. Thus, these tools not only help to correct network problems on time, but also to prevent network failure, to detect inside and outside threats, and

make good decisions for network planning [26].

2.2 IP Address Identification

An important aspect of network monitoring is to be able to identify who is using the resources within the network. A network administrator may take necessary action against a user who misbehaves or misuses the resources within an enterprise local area network.

Cryptographically Generated Addresses (CGAs) have been designed to solve the so-called IPv6 Address Ownership problem [1]. A CGA is used in SEcure Neighbor Discovery (SEND) [19] to safeguard the address of the sender. SEND has been proposed to improve the security of the Network Discovery (ND) protocol in environments where the physical security of the link is not guaranteed (for example in a wireless environment). However, the use of CGA is expensive and time consuming. There is a mechanism to reduce the generation time by moving most of the computation to the server [25]. Further enhancement has been undertaken to support Multi-key CGA (MCGA) [11] and the multiple hash algorithm in CGA [22].

A proposal has been made to generate the IPv6 address in the stateful mode which introduces a light-weight extension of anonymous communications in IPv6 networks [9]. It generates a changeable address using DHCPv6 which may be imported into onion routing-based anonymous communication systems. The objective of this method is to enhance the overall anonymity of the host [9].

A study on the advantages of interaction of DHCPv6 and CGA has been undertaken in [4, 24], followed by a proposal in which CGA is used to efficiently improve the security of DHCPv6 interaction. CGA may be used to authenticate the DHCPv6 server.

2.3 One-to-Many Reversible Mapping

A one-to-many reversible mapping provides a mechanism to enhance IPv6 address generation in terms of security and privacy. A different IPv6 address is given each time a node tries to access the local area network (LAN). This makes it more difficult for eavesdroppers to identify the owner of an IPv6 address. Thus, it protects user privacy as recommended by IETF [21].

The one-to-many mapping between user space and IPv6 addresses is generated cryptographically using the Cipher Feedback (CFB) mode of operation of the Advanced Encryption Standard (AES) [5]. The required software development for IPv6 address generation (one-to-many mapping) has been presented [7].

The mechanism used to generate the user IPv6 address [5] is able to link the dynamic IPv6 address to a particular user, if needed, to improve network visibility, and hence improve security within an enterprise local area network.

3 Many-to-one Mapping

The one-to-many reversible mapping [5], in the reverse mode (many-to-one), is capable to identify users from their IPv6 addresses to facilitate tracking of network anomalies or violations of policies and to improve network visibility. By the random generation of an IPv6 address, the privacy of the user is protected even though the communication is transparent end-to-end.

Figure 1 shows the proposed Interface ID format comprising of a 6-bit checksum, 2-bit 'u' and 'g', a 48-bit `encryptedUserID`, and an 8-bit `keyIdx`.

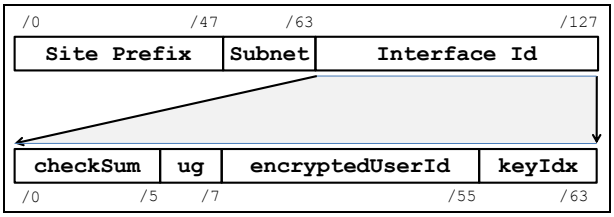


Figure 1: Proposed interface ID format

Figure 2 shows an activity diagram for Interface ID generation which has an 18-bit user ID as input and produces a dynamic 64-bit interface ID.

The 48-bit `encryptedUserId` is generated as per the activity diagram shown in Figure 3 which can be represented as:

$$f(p) \mapsto C_j, j = 1 \ldots n \tag{1}$$

where an 18-bit user ID p is randomly mapped to one of all the n permissible 48-bit encrypted user ID C_j with $n = 2^{48} / 2^{18} = 2^{30}$.

The detailed construction of the user ID encryption can be represented as follows:

$$conc(R, p) = P \tag{2}$$

where the 48-bit concatenated user ID P is a concatenation of a 30-bit R (random number) and an 18-bit p (user ID).

From Equation (2), it can be seen that the same p can generate many P (one-to-many mapping) because of additional randomly generated bits of R. However, the user ID is clearly visible which clashes with one of the objectives to protect user privacy. Encryption is, therefore, performed using CFB-AES which has a higher avalanche effect. Therefore, any change of even a single bit in P will significantly affect many bits of C to produce a pseudo-random value that actually corresponds to the same user ID p.

$$C = E_{CFB-AES}(K, IV, P) \tag{3}$$

where $E_{CFB\text{-}AES}$ denotes the encryption of P under the key K, IV Initialization Vector, and C is the encrypted user ID which is embedded in the Interface ID.

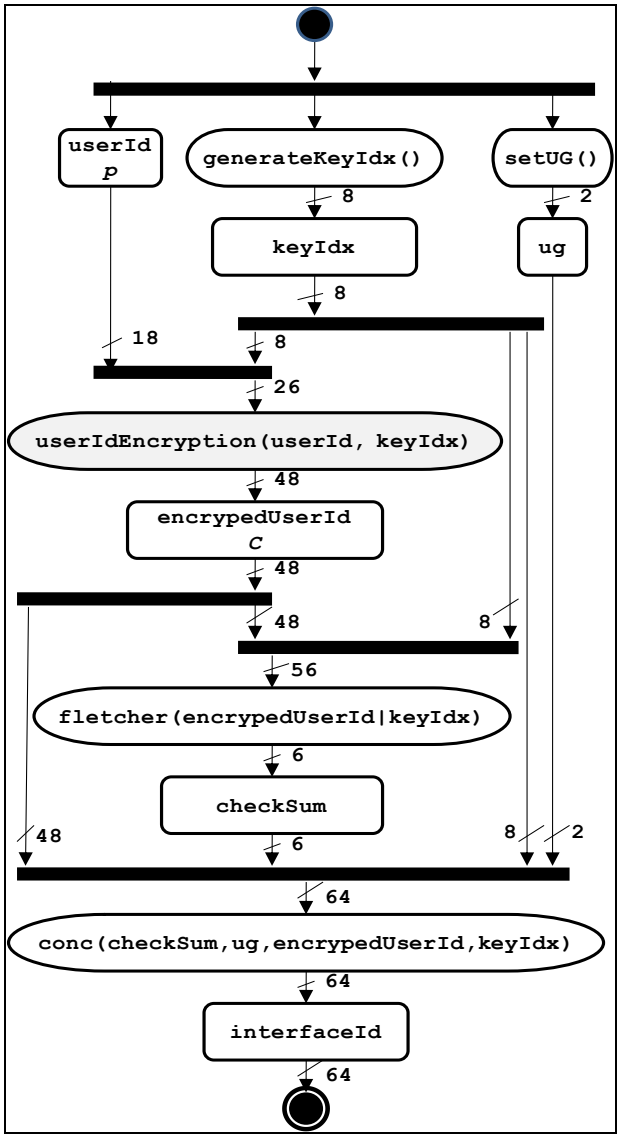


Figure 2: Interface ID generation

Details of the CFB-AES encryption operation are given in Equations (4) and (5) as follows:

$$C_k = P_k \oplus S_s\left[E\left(K, C_{k-1}\right)\right], k = 2 \ldots n \tag{4}$$

where k the sequence of blocks from the second to the last, and the first block encryption also depends on the IV (Initialization Vector) as follows:

$$C_1 = P_1 \oplus S_s\left[E\left(K, IV\right)\right]. \tag{5}$$

4 Results and Discussion

The generated dynamic address can be uniquely linked to a particular user if the need arises. There is a many-to-one mapping between the IPv6 addresses and user space. Figure 4 and Figure 5 show Interface ID owner identification and user ID decryption respectively.

4.1 User ID Identification

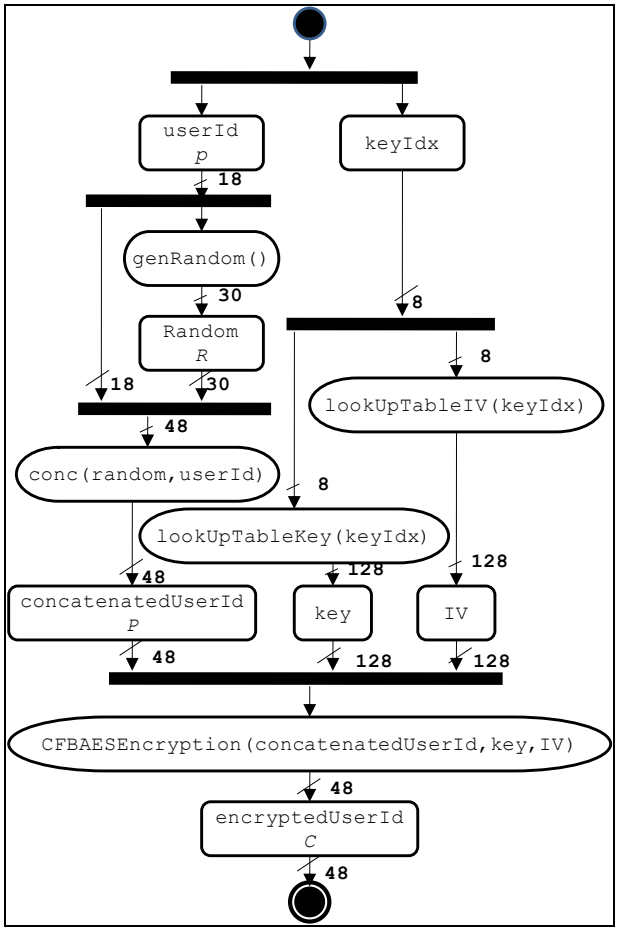


Figure 3: User ID encryption

User ID identification (many-to-one mapping) can be represented as:

$$f\left(C_j\right) \mapsto p, j = 1 \ldots n. \tag{6}$$

To obtain p to identify an 18-bit user ID from a member of C which is part of the Interface ID, the method has to perform validation first as depicted in Figure 4. The `userIdDecryption` process is illustrated in Figure 5 and can be represented as:

$$P = D_{CFB-AES}\left(K, IV, C\right) \tag{7}$$

where $D_{CFB\text{-}AES}$ denotes the decryption of C under the key K and Initialization Vector IV to produce a 48-bit user ID.

Subsequently, simply eliminate the first 30 bits (R) from 48-bit concatenated user ID P.

$$rem\left(P, R\right) = p. \tag{8}$$

This produces a user ID (p) from some P (many-to-one mapping).

For the identification process, the mechanism should yield P from C (Equation (7)). In CFB-AES, this requires encrypting both the first block and the rest of the blocks which can be seen in Equations (9) and (10).

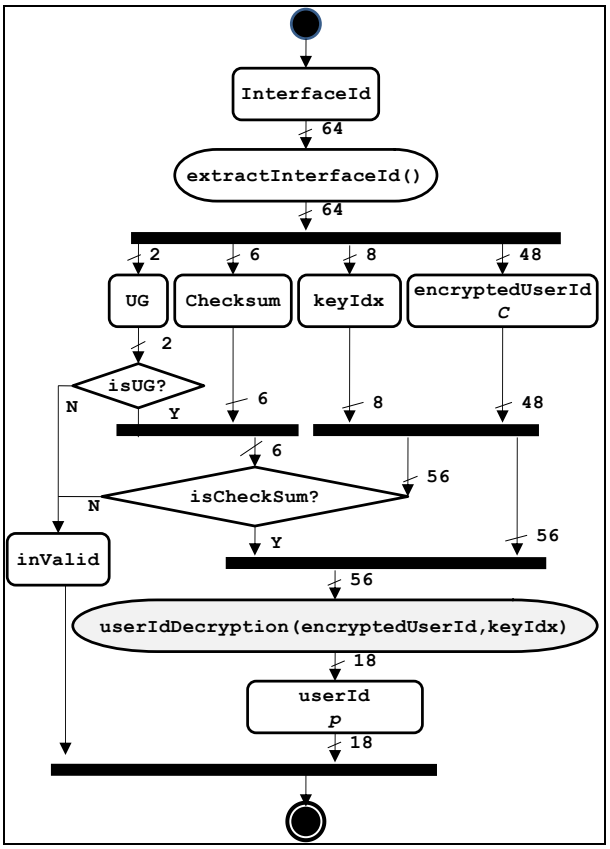


Figure 4: User ID identification

$$P_1 = C_1 \oplus S_s\left[E(K, IV)\right] \tag{9}$$

$$P_k = C_k \oplus S_s\left[E(K, C_{k-1})\right] \tag{10}$$

where k is the second block to the end of the blocks and s is the segment of unit of bits.

4.2 Checksum

A 6-bit checksum is inserted in the proposed Interface ID part of IPv6 address as illustrated in Figure 1 [6] in order to validate the generated Interface IDs.

A modified Fletcher checksum has been used because it is more effective in most situations and has a lower computational cost compared to the Adler checksum [6, 16].

$$Y = \sum_{l=1}^{14}\left(Y_{l-1} + \lambda \times X_l\right) \tag{11}$$

$$Z = \sum_{l=1}^{14}\left(Z_{l-1} + Y_l\right) \tag{12}$$

$$W = conc\left((Y \bmod 8),(Z \bmod 8)\right) \tag{13}$$

where X, Y, and Z are hexadecimal values and W is two octal digits with Y and Z both initialized to 0 (zero). Symbol λ is a parametric constant that can be arbitrarily chosen by the administrator, while l is the number of hexadecimal values.

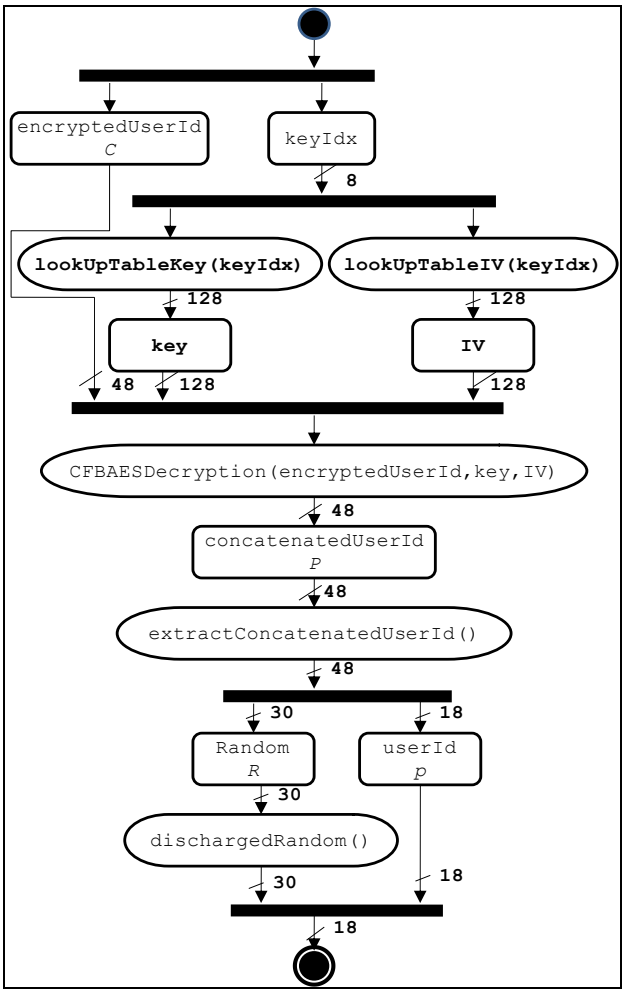


Figure 5: User ID decryption

Figure 6 shows the pseudocode of `function generateChecksum()` which returns a string data type representing the checksum value. It has two parameters which are a string and an integer data type. The string input is a combination of a 48-bit encrypted user ID and an 8-bit key index. This checksum is used for both the address generation and the IPv6 address identification.

```
  function generateChecksum( uid:String,
radix:int ) → String
  {
 c, s, y, z : String
 cInt, yInt, zInt : int = 0
 sumY, sumZ, i  : int = 0
 while ( i < uid.length() )
 {
   c = uid.substring( i, i + 1 )
   cInt = parseInt( c, radix )
   yInt = Constant * cInt
   sumY += yInt
   sumZ += sumY
   i++
 }
 y = toOctalString( sumY )
 z = toOctalString( sumZ )
 s = y + z
 ← s
  }
```

Figure 6: Function generateChecksum() pseudocode

4.3 Software Implementation

The user ID Identification, which is depicted in Figure 4, is implemented as `function userIdIdentification()`, with the pseudo-code shown in Figure 7.

Firstly, the IPv6 address format is verified, and then it takes the leftmost 48 bits to be compared with the current site prefix. After that, it checks the u and g bits as 0 respectively and finally it compares the embedded checksum in the Interface ID with the checksum computation [7].

After the verification process, user ID decryption is performed which is drawn from the activity diagram of Figure 4. User ID decryption is implemented into `function userIdDecryption()` as depicted in Figure 8.

The 128-bit key, 128-bit `initialization Vector`, and 48-bit `encryptedUserId` are used as input and an 18-bit `userId` is produced.

```
function userIdIdentification
(ipv6Address:String)
{
  userId : String
  sitePrefix : String
  interfaceId : String
  checksum : String
  key, encryptedUserId, iv : String
  if (isIpv6Address(ipv6Address) )
  {
    splitIPv6Address(ipv6Address)
    if (isSitePrefix(sitePrefix))
    {
      splitIID(interfaceId)
      if (isUG(interfaceId))
      {
        if (isChecksum(interfaceId))
        {
          userId = userIdDecryption(key,
encryptedUserId, iv)
        }
        else
        {
          message = "Incorrect checksum."
        }
      }
      else
      {
        message = "Incorrect u and g bit
values."
      }
    }
    else
    {
      message = "Incorrect site prefix within
enterprise."
    }
  }
  else
  {
    message = "Incorrect IPv6 address format."
  }
  userId = message
}
```

Figure 7: Pseudo-code for the function userIdIdentification()

```
function userIdDecryption(key: String,
encryptedUserId: String, iv: String)
{
  userId, userId18Bit: String
  cfbAes =  new cfbAes (key,
encryptedUserId, iv)
  cfbAes.decrypts
  userId = cfbAes.getOutStr()
  ← userId18Bit = removeR(userId)
}
```

Figure 8: Pseudo-code for the function userIdDecryption ()

Figure 9 is an example of the output from Wishark network monitoring and analysis [10, 23]. If the analysis shows any anomaly or suspicious activity, the offending IP address is indicated. This IPv6 address then becomes the input to the user ID identification procedure in order to identify the IPv6 address owner within the enterprise local area network.

Figure 10 shows a graphical user interface frame with a text field for the IPv6 address input. The IPv6 address input is from any network monitoring output which has produced an IPv6 address. The 'Identify' button within this frame calls the `function userIdIdentification ()` as depicted in Figure 7.

The IPv6 address owner or an error message is displayed in the user ID text field. Particular error messages are: incorrect IPv6 address format; incorrect site prefix; incorrect u and g bit values; and incorrect checksum.

4.4 Checksum Validation

A checksum is used for validation in the IPv6 address generation and IPv6 address owner identification as per Figure 2 and Figure 4 respectively. For example an IPv6 address is generated for an 18-bit `userId` $(321675)_8$ with an8-bit `keyIdx` $(fd)_{16}$ and a 30-bit random number $(77343\ 67271)_8$.

Based on Table 1, using this particular `keyIdx`, the 128-bit key and the 128-bit IV; the key and the 128-bit IV are $(972635b8\ 56825391\ 997548f7\ 14379866)_{16}$ and $(93348773\ 2882790e\ 58194495\ 8426894a)_{16}$ respectively. This produces 48-bit `encryptedUserId` $(fafa54\ 2ddf06)_{16}$, then it constructs a 6-bit checksum $(07)_8$ with a `keyIdx` and an `encryptedUserId` as parameters.

This results in `1cfa:fa54:2ddf:06fd` as the 64-bit Interface ID. This Interface ID is concatenated with the site prefix and the subnet ID provided by the enterprise local area network to produce the 128-bit IPv6 address [20].

For Interface ID owner identification, primarily it checks the correctness of the IPv6 address format. Then the IPv6 address is split into the site prefix, subnet ID, and Interface ID. If the site prefix matches with the current enterprise site prefix, then it checks the 7th and 8th bit as the 'u' and 'g' bits of the Interface ID [20].

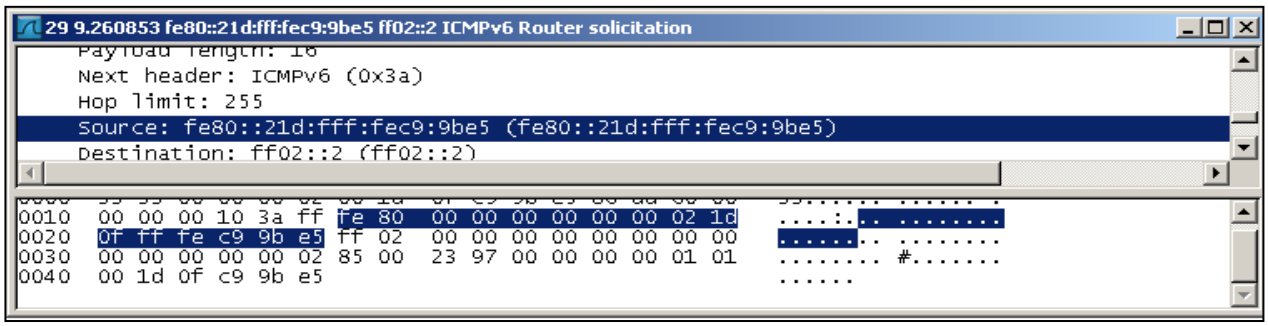


Figure 9: Output example of network monitoring and analysis

Table 1: Key and IV examples

Idx	Key	Initialization Vector
1	719382b603572138744295f461126613	680234479629537e328691705173641a
2	720383b604573139745296f462127614	681235480630538e329692706174642a
3	721384b605574140746297f463128615	682236481631539e330693707175643a
4	722385b606575141747298f464129616	683237482632540e331694708176644a
5	723386b607576142748299f465130617	684238483633541e332695709177645a
...	...	...
128	846509b730699265871422f588253740	807361606756664e455818832300768a
...	...	...
252	970633b854823389995546f712377864	931485730880788e579942956424892a
253	971634b855824390996547f713378865	932486731881789e580943957425893a
254	972635b856825391997548f714379866	933487732882790e581944958426894a
255	973636b857826392998549f715380867	934488733883791e582945959427895a
256	974637b858827393999550f716381868	935489734884792e583946960428896a

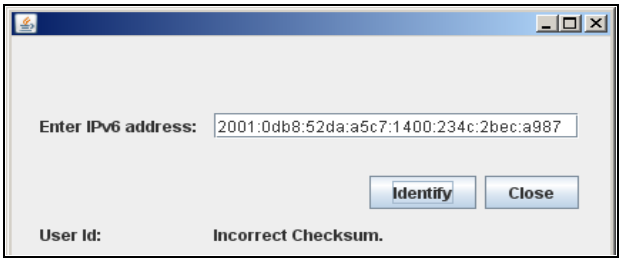


Figure 10: User interface

Table 2: DHCPv6 address generation mechanism

Mechanism	Advantages	Disadvantages
EUI-64 [20]	Unique identifier	Threatens the privacy of users
Random [4, 21]	Easy implementation	Difficult to identify IPv6 address owner
One-to-many reversible mapping [5]	• Unique identifier • Easy implementation • Respect user privacy • Security improvement	Increase processing time

Furthermore, a checksum is computed and compared with the embedded checksum in the Interface ID. If the two are equal, then the identification may proceed to the next stage to obtain a user ID as displayed in Figure 5.

Table 2 shows the relative advantages and disadvantages of standard DHCPv6 address generation mechanisms.

The CFB-AES mechanism is able to generate pseudo-randomly IPv6 address which makes it difficult to identify the owner [5], hence respects the user privacy. However it is possible for administrator to identify IPv6 address owner in the IP address layer in order to improve network security. Although the mechanism reduces processing speed, however it is still practical since it takes less than 100 milliseconds for generating address or identifying the IPv6 address owner [6].

5 Conclusion

This paper presents a method, based on the reverse implementation of an one-to-many reversible mapping, for identification of an IPv6 address owner in an enterprise local area network. The reverse implementation (many-to-one mechanism) has been reviewed and the development of the underlying software development has been given, followed by results of several functional tests. The IPv6 address data may be captured for evaluation from the output of any network monitoring and analysis system and the IPv6 address owner identification scheme may be implemented as a complement of the network monitoring software in order to improve network security. It may be noted that the performance impact of an enterprise wireless local area network, in general improves with improved network security [17].

References

[1] C. Castelluccia, "Cryptographically generated addresses for constrained devices," *Wireless Personal Communications*, vol. 29, pp. 221–232, 2004.

[2] A. Cecil, *A Summary of Network Traffic Monitoring and Analysis Techniques*, Student Paper, ed: Washington University in St. Louis, 2006.

[3] E. Durdağı and A. Buldu, "IPv4/IPv6 security and threat comparisons," *Procedia - Social and Behavioral Sciences*, vol. 2, pp. 5285-5291, 2010.

[4] S. Groat, M. Dunlop, R. Marchany, and J. Tront, "What DHCPv6 says about you," in *2011 World Congress on Internet Security (WorldCIS)*, pp. 146-151, 2011.

[5] N. Hakiem, A. U. Priantoro, M. U. Siddiqi, and T. H. Hasan, "Generation of IPv6 addresses based on one-to-many reversible mapping using AES," in *Recent Progress in Data Engineering and Internet Technology*, vol. 157, pp. 183-189, 2012.

[6] N. Hakiem, M. U. Siddiqi, and S. P. W. Jarot, "Collision probability of one-to-many reversible mapping for IPv6 address generation," in *2012 International Conference on Computer and Communication Engineering (ICCCE)*, pp. 599-602, Kuala Lumpur Malaysia, 2012.

[7] N. Hakiem and M. U. Siddiqi, "One-to-many reversible mapping for IPv6 address generation: simulation software development," *Journal Of Theoretical And Applied Information Technology*, vol. 47, pp. 892-901, Jan 2013.

[8] N. T. Hoa, K. Naoe, and Y. Takefuji, "Simplifed IPSec protocol stack for micro server " *International Journal of Network Security*, vol. 11, pp. 46-54, July 2010.

[9] Z. Jia, D. Haixin, L. Wu, and W. Jianping, "A light-weighted extension of anonymous communications in IPv6 network," in *2010 International Conference on Green Circuits and Systems (ICGCS)*, pp. 404-408, 2010.

[10] S. Kakuru, "Behavior based network traffic analysis tool," in *2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN)*, pp. 649-652, 2011.

[11] J. Kempf, J. Wood, Z. Ramzan, and C. Gentry, "IP address authorization for secure address proxying using Multi-key CGAs and ring signatures," in *Advances in Information and Computer Security*. vol. 4266, pp. 196-211, 2006.

[12] J. Li, P. Zhang, and S. Sampalli, "Improved security mechanism for mobile IPv6," *International Journal of Network Security*, vol. 6, pp. 291–300, May 2008.

[13] B. Li, J. Springer, G. Bebis, and M. H. Gunes, "A survey of network flow applications," *Journal of Network and Computer Applications*, vol. 36, pp. 567-581, 2013.

[14] X. Liu, G. Hu, W. Chen, and K. Xu, "IPv6 protocol simplification for the internet of things," *Qinghua Daxue Xuebao/Journal of Tsinghua University*, vol. 52, pp. 699-703, 2012.

[15] P. Martinez-Julia and A. F. Skarmeta, "A lightweight and Identity-Based network architecture for the internet of things," in *2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*, pp. 711-716, 2012.

[16] T. Maxino, *Revisiting Fletcher and Adler Checksums*, DSN 2006 Student Forum, ed. Pittsburgh: Institute for Software Research, Carnegie Mellon University, 2006.

[17] D. Nayak, D. B. Phatak, and A. Saxena, "Evaluation of security architecture for wireless local area networks by indexed based policy method: a novel approach," *International Journal of Network Security*, vol. 7, pp. 1–14, July 2008.

[18] J. Oltsik, *Identity-Aware Networking*, White Paper, ed: Enterprise Strategy Group, 2010.

[19] RFC3971, *SEcure Neighbor Discovery (SEND)*, Standards Track, IETF Network Working Group, 2005.

[20] RFC4291, *IP Version 6 Addressing Architecture*, Standards Track, IETF Network Working Group, Feb. 2006.

[21] RFC4941, *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*, Standards Track, IETF Network Working Group, Sep. 2007.

[22] RFC4982, *Support for Multiple Hash Algorithms in Cryptographically Generated Addresses (CGAs)*, Standards Track, IETF Network Working Group, 2007.

[23] C. Sanders, *Practical Packet Analysis Using Wireshark to Solve Real-world Network Problems*, 2nd ed. Canada: No Starch Press, 2011.

[24] S. Sean, L. Xiaodong, S. Zhili, and J. Sheng, "Enhance IPv6 dynamic host configuration with cryptographically generated addresses," *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2011 Fifth International Conference on*, pp. 487-490, 2011.

[25] G. Su, *et al.*, "A quick CGA generation method," *Future Computer and Communication (ICFCC), 2010 2nd International Conference on*, pp. V1-769-V1-773, 2010.

[26] C. So-In, *A Survey of Network Traffic Monitoring and Analysis Tools*, Student Paper, ed: Washington University in St. Louis, 2006.

Nashrul Hakiem holds a master degree in Informatics Engineering (Software Engineering) from Institut Teknologi Bandung (ITB), Indonesia as of 2001. Prior to that, he obtained a Bachelor in Computer Science from Universitas Gadjah Mada (UGM), Indonesia in 1996. Currently, he is a PhD candidate in Electrical and Computer Engineering Department of International Islamic University Malaysia (IIUM). The author is a lecturer in the Informatics Engineering Department, Faculty of Science and Technology, Universitas Islam Negeri (UIN) Syarif Hidayatullah Jakarta, Indonesia. His research interests are in software engineering, object oriented technology, cryptography, and IPv6.

Mohammad Umar Siddiqi received his B.Sc. and M.Sc. degrees from Aligarh Muslim University (AMU Aligarh) in

1966 and 1971, respectively, and a Ph.D. degree from the Indian Institute of Technology Kanpur (IIT Kanpur) in 1976, all in Electrical Engineering. He has been in the teaching profession throughout, first at AMU Aligarh, then at IIT Kanpur and Multimedia University Malaysia. Currently, he is a Professor in the Faculty of Engineering at International Islamic University Malaysia. His research interests are in coding, cryptography, and information security.

Hashum Mohamed Rafiq received his B.Sc. degree in Computer Science from University of Dar Es Salaam (UDSM), Tanzania and holds an M.Sc. degree in Computer and Information Engineering from the International Islamic University Malaysia. Currently, he is a PhD candidate in Electrical and Computer Engineering Department of the International Islamic University Malaysia (IIUM). His research interests are in coding, cryptography, and information security.

Semi Random Position Based Steganography for Resisting Statistical Steganalysis

Amitava Nag[1], Sushanta Biswas[2], Debasree Sarkar[2], and ParthaPratim Sarkar[2]
(Corresponding author: Amitava Nag)

Department of Information Technology, Academy of Technology, Hoogly 721212, India[1]
Département of Engineering and Technological studies,University of Kalyani[2]
Kalyani 741 235, India
(Email: amitavanag.09@gmail.com)
(Received Oct. 18, 2012, revised and accepted Feb. 20, 2013)

Abstract

Steganography is the branch of information hiding for secret communication. The simplest and widely used steganography is the LSB based approach due to its visual quality with high embedding capacity. However, LSB based steganography techniques are not secure against statistical steganalysis mainly $\chi 2$ attack and Regular Singular (RS) attack. These two staganalysis can easily estimate the hidden message length. This work propose a LSB based steganography technique where first a location is obtained randomly based on the bit pattern (except LSB) of a cover pixel using linear probing and embed a secret bit into LSB. This technique makes the stego-image completely secure against both $\chi 2$ attack and RS attack.

Keywords: Information hiding, RS attack, statistical steganalysis, steganography, $\chi 2$ attack

1 Introduction

Due to widespread use of internet, the sharing and transmission of images in digital form has become quite easy. However, message transmissions over the Internet still have to face all kinds of security problems. Therefore, finding ways to transmit data secretly through internet has become an important issue. Cryptography [18] is a one procedure to provide a safe way by transforming data into a cipher text via cipher algorithms [1, 15]. Encryption techniques scramble the message so that it cannot be understood by unauthorized users. However, this can naturally raise the curiosity level of an eavesdropper. It would be rather more prudence if the secret message is cleverly embedded in another media such that the secret message is concealed to everyone. This idea forms the basis for steganography [3, 13], which is a branch of information hiding by camouflaging secret information within covert carriers to avoid observation. The word steganography in Greek means "covered writing". Steganography is the art of hiding the presence of communication by embedding secret messages into innocent, innocuous looking cover documents, such as digital images [2, 4, 7, 8, 10, 12, 20, 21], videos [5, 19], sound [10, 14, 16] or document [6, 11, 17]. The stego-medium is the result of embedding the message in cover-medium. Images provide excellent carriers for hidden information. Many different techniques have been introduced to embed messages in images.

The most common approaches for steganography in images are Least Significant Bit (LSB) modification [8, 12] where LSB is substituted by secret bit. This modification create some structural asymmetry [8, 13] and thus sufficient evidence about the existence of secret message inside stego-image is collected. This is known as steganalysis attack [13, 20]. The goal of the proposed method is to avoid detection of steganalysis attack.

2 Related Work

Steganalysis is the science and art of discovering the existence of secret message hidden in stego-image using steganography [3, 13]. Steganalysis can be classified into two classes: signature steganalysis and statistical steganalysis [13, 20]. In statistical steganalysis the existence of the hidden message is discovered by finding statistical abnormality in stego-media caused by message embedding. Two popular statistical steganalysis are Chi-squared ($\chi 2$ detection) [21] and Regular Singular(RS) attack [4].

2.1 $\chi 2$ Detection

In the embedding process of LSB steganography the secret bits replaces the bits of LSB plane of cover image while the higher bit planes are unaltered. Hence, the pixel values of the cover Image are modified. This modification allow us to test Chi-squared (χ^2 detection) on the stego images. In westfeld and Pfitzmann proposed a chi-square detection (χ^2 detection) method using the POV (pair of value) phenomenon of the LSB plane.

The result of the LSB embedding process is the creation of Pairs of Value (POVs). For example, a pixel value of 210 in cover image will either 210 or change to 211. Thus

{210,211} is POV. In general, {2i,2i+1| $0 \le i \le 127$ } form POVs.

LSB embedding techniques creates POVs, the frequencies of 2k and 2k+1 becomes equal or nearly so. χ^2 attack detects these near-equal POVs and calculates the probability of embedding. The χ^2 statistics is calculated as

$$\chi^2 = \sum_{i=0}^{127} \frac{(x_i - z_i)^2}{z_i} where z_i = \frac{x_i + x_{i+1}}{2} \dots\dots\dots (1)$$

z_i is the theoretically expected frequency if a random message has been embedded, and x_i is the actual number of occurrences of color. The embedded rate p is estimated by the equation given below:

$$p = 1 - \frac{1}{2^{\frac{n-1}{2}}\Gamma\left(\frac{n-1}{2}\right)} \int_0^{x_{n-1}^2} e^{-\frac{u}{2}} u^{\frac{n-1}{2}-1} du \dots\dots (2)$$

But the main weakness of Chi-Squared technique is its complete dependency upon the pairs of values. This test fails completely for the any image embedding techniques using an algorithm that does not generate POVs.

2.2 RS Attack

Fridrichet. al. proposed the RS steganalysis technique for detecting embedded messages in a stego-image by LSB steganography. This method is most reliable and accurate method than χ^2 detection to estimate embedding rate for random embedding cases and can easily distinguish stego-image and cover image. The RS attack steganalysis technique perform the following steps

Step 1: Select an m-tuple Mask M with values {-1,0,1}. Here we choose m=4 and select M=[0 1 1 0], -M=[0 -1 -1 0].

Step 2: The grayscale image is divided into non-overlapping groups G_c of n adjacent pixels $x_1, x_2, \dots, x_n \in \{0 \text{ to } 255\}$ and set $G_c = (x_1, x_2, \dots, x_n)$

Step 3: The smoothness of pixel group G_c is determined by using the discrimination function f as

$$f(x_1, x_2, \dots\dots\dots, x_n) = \sum_{0}^{n-1} |x_{i+1} - x_i| \dots\dots\dots (3)$$

Step 4: An invertible mapping F_M, called flipping function is defined on [0 to 255] to flipping the pixel value according to M i.e. F_1 for positive M and F_{-1} for negative M as,

$$F_1(x) = \begin{cases} x-1, & if x \bmod 2 == 1 \\ x+1, & if x \bmod 2 == 0 \end{cases} \dots\dots\dots (4)$$

$$F_{-1}(x) = F_1(x+1) - 1 \dots\dots\dots (5)$$

where F_1: 0←→1, 2←→3, ..., 254 ←→255

and F_{-1}: -1 ←→0, 1 ←→2,3 ←→ 4, ..., 253 ←→ 254, 255←→256

Similarly, define F_0 as, $F_0(x) = x$

Step 5: Let $F_M(G_c)$ be the result of flipping all the pixel value of group G_c by flipping function F_M . Let $f(F_M(G_c))$ be the result of $F_M(G_c)$ input to discrimination function f, define three types of groups R,S,U by the following rules:

Regular Groups: $G_c \in R \Rightarrow f(F_M(G_c)) > f(G_c)$;

Singular Groups: $G_c \in S \Rightarrow f(F_M(G_c)) < f(G_c)$;

Unusable Groups: $G_c \in U \Rightarrow f(F_M(G_c)) = f(G_c)$.

Do this same grouping also for negative Mask i.e. –M.

Step 6:

a) Repeat Step 1 to Step 5 up to half of the total no of pixels of the embedded image. The factor of one half is due to the fact that, assuming the message is a random bit-stream; on average only one half of the pixels will be flipped.

b) Repeat Step 1 to Step 5 up to the total no of pixels of the embedded image.

Step 7: For half of the total no of pixels calculate, $R_M(p/2), S_M(p/2), R_{-M}(p/2), S_{-M}(p/2)$. Similarly for the total no of pixels calculate, $R_M(1-p/2), S_M(1-p/2), R_{-M}(1-p/2), S_{-M}(1-p/2)$, where p is unknown length of message in a stego-image (in percent of pixels).

Step 8: Obtain the value of x from the following quadratic equation,

$$2(d_1 + d_0)x^2 + (d_{-0} - d_{-1} - d_1 - 3d_0)x + d_0 - d_{-0} = 0 \quad \dots (6)$$

$$\text{where} \begin{cases} d_0 = R_M\left(\frac{p}{2}\right) - S_M\left(\frac{P}{2}\right) \\ d_1 = R_M\left(1 - \frac{p}{2}\right) - S_M\left(1 - \frac{P}{2}\right) \\ d_{-0} = R_{-M}\left(\frac{p}{2}\right) - S_{-M}\left(\frac{P}{2}\right) \\ d_{-1} = R_{-M}\left(1 - \frac{p}{2}\right) - S_{-M}\left(1 - \frac{P}{2}\right) \end{cases} \dots\dots\dots (7)$$

Step 9: p is estimated from x as $p = \frac{x}{\left(x - \frac{1}{2}\right)}$

2.3 RHTF-based LSB Steganography

In [11], the authors proposed a reversible histogram transformation functions (RHTF) steganography scheme. In 2011, Lou and Hu discovered two vulnerabilities: "zero points" and "double frequency", by which they distinguished the stego-images from cover images and also they broke the value of the secret key [9] . In [20], Lin and Hu remove "zero points" and "double frequency" from sego-image using the following algorithm:

Embedding Algorithm

Step 1: Divide the cover image I_c into n groups of size $\frac{I_c}{n}$.

Step 2: Generate n number of secret key a_j using following key generation algorithm:

a) Generate key by increasing a_j as $a_j = a_{j-1} + 1$, until $a_j = a_U$.

b) Generate key by decreasing a_j as $a_j = a_{j-1} + 1$, until $a_j = a_L$.

c) Continue Steps 2 (a) and (b) until j = n.
wherea initial value (a_1), upper bound(a_U) and lower bound (a_L) are predefined.

Step 3: Apply the compressing transformation technique to each cover pixel P as follows

$$P_1 = P - \left\lfloor \frac{P}{a_j + 1} \right\rfloor$$

Step 4: Replace the LSB of P_1 by a secret bit and P_2 is obtained.

Step 5: Apply the following formula to produce stego pixel

$$P_s = P_1 - \left\lfloor \frac{P_1}{a_j} \right\rfloor$$

Extracting Algorithm

Step 1: Divide the stego-image I_s into n groups of size $\frac{I_s}{n}$.

Step 2: Generate n number of secret key a_j using following key generation algorithm:

a) Generate key by increasing a_j as $a_j = a_{j-1} + 1$, until $a_j = a_U$.
b) Generate key by decreasing a_j as $a_j = a_{j-1} + 1$, until $a_j = a_L$.
c) Continue Step 2 (a) and (b) until j = n.
wherea initial value (a_1), upper bound(a_U) and lower bound (a_L) are predefined.

Step 3: Apply the compressing transformation technique to each cover pixel P as follows

$$P_1 = P_s - \left\lfloor \frac{P_s}{a_j + 1} \right\rfloor$$

Step 4: Extract the LSB of P_1 as a secret bit.

3 Proposed Technique

Sequential embedding is susceptible to Chi Square Attack [21]. In order to resist this, non-sequential random embedding was proposed. However, as a counter measure RS Attack [4] was developed specifically to detect random embedding. RS attack is based on the fact that image gets very slightly distorted as a result of LSB embedding. This approach groups a collection of pixels based on the effect embedding has on them as Regular, Singular and Unusable groups. Based on certain formulae and the number of Regular and Singular groups, we can deduce the percentage of embedding in terms of a probabilistic result. Here lies the strength of the RS algorithm.

The proposed algorithm takes advantage of the strongest point of the RS algorithm, i.e. it groups collection of pixels into Regular, Singular and Unusable groups. However, we find that only the Regular and Singular groups suffice the needs of the formulae. The proposed algorithm embeds the message bits in such a semi random way that the effects of embedding are cancelled out by each other and as a result the relative numbers of Regular and Singular Groups are minimized. Due to this, formulae render a misleading and impossible probabilistic result. Thus, the proposed algorithm resists both types of statistical steganalysis, namely Chi Square attack and RS Attack.

To insert a secret bit in the proposed technique, we first select a proper position. For position selection, we traverse the image according to the binary bit pattern of a pixel till its LSB is encountered. For traversing from location (x,y), we use the following rules:

Rule 1: If a 1 is encountered, then traverse the matrix by one row in a cyclic format, towards downward as $(x_{new}, y_{new}) = (((x mod M) + 1), y) \ldots\ldots (8)$.

Rule 2: If a 0 is encountered, then traverse the matrix by one column in a cyclic format, towards right side as $(x_{new}, y_{new}) = (x, (y\ mod N) + 1)) \ldots\ldots (9)$.

When a position of embedding $(x_{new}, y_{new})$is selected using above traversal, we check whether a collision occurs i.e. any bit is already embedded in that position. If collision occurs, then linear probing is used in row major order to select a collision free position for embedding a secret bit. After the selection of final position in cover image, the secret bit is directly embedded in the LSB of that selected cover pixel. To detect collision a binary flag matrix of same size of cover image is used whose elements are initialized to zero. When a secret bit is embedded in the cover image, the value in the corresponding position of the flag matrix is set to 1. During embedding in selected position of the cover image, if the value of corresponding position of flag matrix is 1, collision is detected and linear probing is applied until a position whose flag value is 0.

Algorithm 1:Embedding of secret bit stream

Input: Cover Image I of size M×N and Secret bits sequence S = {s1,s2,……,sL}, where si Є {0,1}
Output: Stego Image Is
1: Begin
2: Transformation of pixel value to even number: Change pixel I(x,y) as

$$I(x,y) = \begin{cases} I(x,y) - 1 & \text{if} I(x,y) \bmod 2 == 0 \\ I(x,y) & \text{Otherwise} \end{cases} \quad \ldots\ldots (10)$$

3: Binary pattern generation: Obtain binary value of I(x,y) as I(x,y)=(b7b6b5b4b3b2b1b0) where bi Є {0,1}.
4: Declaration and Initialization of Flag matrix: Declare a flag matrix F of size M×N and initialize its value with 0.
5: Image matrix traversal: Traverse the image matrix I according to the binary bit pattern of pixel I(x,y) starting from location (x,y) till the 2nd least significant bit (Here b1) using the following rules:
(a) If bi = = 1, (x1, y1) = (((x mod M)+1), y);
(b) If bi = =0, (x1, y1) = (x, ((y mod N)+1)).
Where bi represents the current working bit of I(x,y) and i ≠ 0.

6: Collision detection and insertion of secret bits: If (x1, y1) is the selected position for insertion obtained in step 3 and sj is a secret bit, check whether I(x1, y1) is collision free by examining value of f(x1, y1). If f(x1, y1) is 0, then I(x1, y1) is collision free and embed si at LSB of I(x1, y1). On the other hand if f(x1, y1) is 1, perform a linear probe using equation (11) on the image matrix I starting from (x1, y1) till (x2, y2) for which f(x2, y2) is 0 and embed si into the LSB of I(x2, y2) as described below:

Case 1: $f(x_1, y_1) = = 0$

$I'(x_1, y_1) = (b_7b_6b_5b_4b_3b_2b_1s_j)$ and $f(x_1, y_1) = =1$.

Case 2: f(x1, y1) = = 1

New position is computed using linear probing as

$$(x_{new}, y_{new}) = \begin{cases} (x_1, (y_1 + 1)) \text{ify} < N \\ ((x_1 \text{mod} M) + 1, (y_1 \text{mod} N) + 1) \text{ify} == N \end{cases} \dots (11)$$

till $(x_{new}, y_{new}) = (x_2, y_2)$ for which f(x2, y2) = 0 and $I'(x_2, y_2) = ((b_7b_6b_5b_4b_3b_2b_1s_j)$ and $f(x_2, y_2) = 1$.

7: End

Let us apply the embedding algorithm on a 4 × 4 image matrix I given below:

I =

105	115	112	94
109	115	152	107
121	131	119	6
138	114	22	37

After converting all pixels of the above image matrix into even numbers, the new image matrix

I =

104	114	112	94
108	114	152	106
120	130	118	6
138	114	22	36

and a flag matrix f of size 4 × 4 is defined and initialized to 0 as

f =

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

Let the secret message to be embedded be **1111010100101011**. The message embedding is started from the location (1, 1) whose pixel value is 104. The binary bit Sequence of 104 is 01101000. Now traverse the matrix according to the bit sequence till the 2nd LSB is encountered using Equations (8) and (9) as:

0 1 1 0 1 0 0

I(1,1)→I(1, 2)→I(2, 2)→I(3, 2)→I(3, 3)→I(4, 3)→I(4, 4)→I(4, 1).

After reaching to the position (4, 1), the same position of flag matrix f is examined and found that f(4, 1) is 0, i.e. I(4, 1) is collision free. Thus embed the 1st message bit (here 1) in I(4, 1) which change the pixel value 138 to 139. After embedding f(4, 1) is also changed to 1 as given below

I =

104	114	112	94
108	114	152	106
120	130	118	6
139	114	22	36

and f =

0	0	0	0
0	0	0	0
0	0	0	0
1	0	0	0

This process continues to embed all secret bits and at the same time the value at the corresponding position in the flag matrix is also changed to 1. Now let us give an example to detect collision and resolve it using flag matrix. For this purpose choose the last message bit. After the insertion of the 15 bits, the flag matrix looks like as

f =

1	1	1	1
1	1	1	1
1	0	1	1
1	1	1	1

To insert the last message bit (16th bit) into the cover image, the traversal will be started from the pixel 36 of position (4, 4) into the cover image. According to the bit pattern (first 7 bits) of 36 (here 0010010), the traversal will be stopped in the position (2, 2) and collision occurs as in (2, 2) location of the flag matrix is set as 1. To find the collision free location, apply linear probing in row major order by Equation (11) as

1 1 1 1 0

f(2, 2)→ f(2, 3)→ f(2, 4)→ f(3, 1)→ f(3, 2)→ Stop

As (3, 2) location of flag was set to 0, embed last secret bit (here 1) in the cover pixel 130 of location (3, 2) as given in the last row of Table 1. After embedding the secret bit sequence using above algorithm, the stego-image I' and flag matrix f is

I' =

105	114	112	94
109	115	153	106
121	131	119	6
139	115	23	36

and f=

1	1	1	1
1	1	1	1
1	1	1	1
1	1	1	1

Table 1: Example details of the embedding procedure

Start Coordinate (x,y)	I(x,y)	$b_7b_6b_5b_4b_3b_2b_1b_0$	Final coordinate (x_1,y_1)	$I(x_1, y_1)$	s_i	$I'(x_1,y_1)$
(1,1)	104	01101000	(4,1)	138	1	139
(1,2)	114	01110010	(1,1)	104	1	105
(1,3)	112	01110000	(4,3)	22	1	23
(1,4)	94	01011110	(2,2)	114	1	115
(2,1)	108	01101100	(2,4)	106	0	106
(2,2)	114	01110010	(2,1)	108	1	109
(2,3)	152	10011000	(1,3)	112	0	112
(2,4)	106	01101010	(2,3)	152	1	153
(3,1)	120	01111000	(3,4)	6	0	6
(3, 2)	130	10000010	(1,4)	94	0	94
(3,3)	118	01110110	(4,2)	114	1	115
(3,4)	6	00000110	(1,2)	114	0	114
(4,1)	138	10001010	(3,1)	120	1	121
(4,2)	114	01110010	(4,4)	36	0	36
(4,3)	22	00010110	(3,3)	118	1	119
(4,4)	36	00100100	(3, 2)	130	1	131

3.1 Retrieval Technique

The message retrieval is just the reverse procedure of the embedding process as given in the extraction algorithm.

Algorithm 2:Extraction of secret bits from Stego-imageI'

Input: Stego-image I'

Output: Secret bit stream S

1: Begin

2: Binary pattern generation: Obtain binary value of $I'(x,y)$ as $I'(x,y)=(b_7b_6b_5b_4b_3b_2b_1s_i)$ where $b_i \in \{0,1\}$

3: Declaration and Initialization of Flag matrix: Declare a flag matrix F of size M×N and set its all elements to 0.

4: Image matrix traversal: Traverse the image matrix I according to the binary bit pattern of pixel $I'(x,y)$ starting from location (x,y) till the 2nd least significant bit (Here b_1) using the following rules:

(a) If $b_i == 1$, $(x_1, y_1) = ((x + 1) \bmod M, y)$

(b) If $b_i == 0$, $(x_1, y_1) = (x, (y + 1) \bmod N)$

Where b_i represents the current working bit of $I'(x,y)$ and $i \neq 0$

5: Collision detection and extraction of secret bits: If (x_1, y_1) is the selected in step 3, check whether $I'(x_1, y_1)$ is collision free by examining value of $f(x_1, y_1)$. If $f(x_1, y_1)$ is 0, then $I'(x_1, y_1)$ is collision free and extract the LSB s_i of $I'(x_1, y_1)$ and is added into secret bit stream. On the other hand if $f(x_1, y_1)$ is 1, perform a linear probe using Equation (11) on the image matrix I' starting from (x_1, y_1) till (x_2, y_2) for which $f(x_2, y_2)$ is 0 and embed s_i into the LSB of $I'(x_2, y_2)$ as described below:

case 1: $f(x_1, y_1) = = 0$

extract the LSB s_i from $I'(x_1, y_1) = (b_7b_6b_5b_4b_3b_2b_1s_j)$ and set $f(x_1, y_1) = 1$

case 2: $f(x_1, y_1) = = 1$

Linear probing is applied using Equation (11) till $(x_{new}, y_{new}) = (x_2, y_2)$ for which $f(x_2, y_2) = = 0$ and extract the LSB s_i from $I'(x_2, y_2) = ((b_7b_6b_5b_4b_3b_2b_1s_j)$ and set $f(x_2, y_2) = 1$

6: End

To illustrate message retrieval technique first define a flag matrix f of size 4 × 4 as

f =

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

Traversal will start from location (1, 1) in stego-image with the pixel 104, whose corresponding Binary Bit Sequence = 01101001. From the binary sequence of 105 it is observed that first seven bits are unchanged. Only the last bit is changed in worst case (if s_j and b_0 are not matched). Thus traversed path remain same as to the traversed path during embedding. Now traverse the matrix according to the bit sequence till the 2nd LSB is encountered using Equations (8) and (9) as:

0 1 1 0 1 0 0

I(1, 1)→I(1, 2)→I(2, 2)→I(3, 2)→I(3, 3)→I(4, 3)→I(4, 4)→I(4, 1)

After reaching to the position (4, 1), the same position of flag matrix f is examined and found that f(4, 1) is 0, i.e. I(4, 1) is collision free. Thus extract the 1st message bit (here 1) from the LSB of $I'(4, 1)$ whose value is 139. After extracting secret bit s_j from the location (4, 1) of I', f(4, 1) is changed to 1 as given below

f =

0	0	0	0
0	0	0	0
0	0	0	0
1	0	0	0

This process continues to extract the secret bits and at the same time the corresponding bit in the flag matrix is also changed. Now let us give an example to detect collision and resolve it using flag matrix during extraction. For this purpose choose the last bit. After the insertion of the 15 bits, the flag matrix looks like as

f =

1	1	1	1
1	1	1	1
1	0	1	1
1	1	1	1

To extract the last secret bit(16th bit) from the cover image, the traversal will be started from the pixel 36 of position (4, 4) into the cover image. According to the bit pattern (first 7 bits) of 36 (here 0010010), the traversal will be stopped in the position (2, 2) and collision is found as in location (2, 2) in the flag matrix is set as 1. To find the collision free location, apply linear probing by Equation (11) as

1 1 1 1 0

f(2, 2)→ f(2, 3)→ f(2, 4)→ f(3, 1)→ f(3, 2)→ Stop

As location (3, 2) of the flag matrix is set to 0, extract the secret bit (here 1) from the LSB of the pixel 131 at location (3, 2) in stego-image I'as given in the last row of

Table 2. After extracting the secret bit sequence using above algorithm flag matrix f is

f =

1	1	1	1
1	1	1	1
1	0	1	1
1	1	1	1

Table 2: Example details of extracting procedure

Start Coordinate (x,y)	I' (x,y)	$b_7b_6b_5b_4b_3b_2b_1b_0$	Final coordinate (x_1,y_1)	I' (x_1,y_1)	Extracted bits (s_i)
(1,1)	104	01101000	(4,1)	139	1
(1,2)	114	01110010	(1,1)	105	1
(1,3)	112	01110000	(4,3)	23	1
(1,4)	94	01011110	(2,2)	115	1
(2,1)	109	01101100	(2,4)	106	0
(2,2)	115	01110010	(2,1)	109	1
(2,3)	153	10011000	(1,3)	112	0
(2,4)	106	01101010	((2,3)	153	1
(3,1)	121	01111000	(3,4)	6	0
(3, 2)	131	10000010	(1,4)	94	0
(3,3)	119	01110110	(4,2)	115	1
(3,4)	6	00000110	(1,2)	114	0
(4,1)	139	10001010	(3,1)	121	1
(4,2)	115	01110010	(4,4)	36	0
(4,3)	23	00010110	(3,3)	119	1
(4,4)	36	00100100	(3, 2)	131	1

3.2 Security Analysis

In this section, we will explain

Mask= [0 1 1 0];

r_1 = no. of regular groups for M;

Negative mask= [0 -1 -1 0];

r_2 = no. of regular groups for (–M).

Here we assume, N=4, initially set $r_i = s_i = 0$, $1 <= i <= 2$ s_1 = no. of singular groups for M:

s_2 = no. of regular groups for (–M)

$$I' = \begin{bmatrix} 105 & 114 & 112 & 94 \\ 109 & 115 & 153 & 106 \\ 121 & 131 & 119 & 6 \\ 139 & 115 & 23 & 36 \end{bmatrix}$$

For total group/2:
In iteration-1, G_c={105,114,112,94} and $f(G_C)$ = 29;
$F_M(G_C)$ = {105,115,113,94} and $f(F_M(G_C))$=31.
Therefor $f(F_M(G_C)) > f(G_C)$;
Hence, **Regular Group** set $\mathbf{r_1=1.}$
Again $F_{-M}(G_c)$= {105,113,111,94} and $f(F_{-M}(G_c))$ = 27.
Therefore $f(F_{-M}(G_c)) < f(G_C)$
Hence, **Singular Group** set $\mathbf{s_2 = 1.}$

In iteration 2, G_c={109,115,153,106} and $f(G_C)$ = 91,
$F_M(G_C)$ = {109,114,152,106}, and $f(F_M(G_C))$ = 89.
Therefore $f(F_M(G_C)) < f(G_C)$.
Hence, **Singular Group** set $\mathbf{s_1 = 1.}$
Again $F_{-M}(G_c)$ = {109,116,154,106} and $f(F_{-M}(G_c))$ = 93.
Therefore $f(F_{-M}(G_c)) > f(G_C)$.
Hence, **Regular Group**set $\mathbf{r_2=1.}$

RM = r_1/total group = 1/2;
RM' = r_2/total group = 1/2;
SM = s_1/total group = 1/2;
SM'= s_2/total group = 1/2;
d_0 = (RM – SM) = (1/2 – 1/2) = 0;
d_{-0}= (RM' – SM') = (1/2 – 1/2) = 0.

For total group:-
From Iteration 1, $r_1 = 1, s_2 = 1$;
From Iteration 2, $s_1 = 1$, $r_2 = 1$;
In iteration 3, G_c={121,131,119, 6} and $f(G_C)$ = 135,
$F_M(G_C)$ = {121,130,118,6}, and $f(F_M(G_C))$ = 133.
Therefore $f(F_M(G_C)) < f(G_C)$.
Hence, **Singular Group** set $\mathbf{s_1 = 2}$.
Again $F_{-M}(G_c)$ = {121,132,120,6} and $f(F_{-M}(G_c))$ = 137.
Therefore $f(F_{-M}(G_c)) > f(G_C)$.
Hence, **Regular Group**set $\mathbf{r_2=2.}$

In iteration 4, G_c={139,115,23,36} and $f(G_C)$ = 129,
$F_M(G_C)$ = {139,114,22,36}, and $f(F_M(G_C))$ = 131.
Therefore $f(F_M(G_C)) > f(G_C)$.
Hence, **Regular Group**set $\mathbf{r_1=2.}$
Again $F_{-M}(G_c)$ = {1391162436} and $f(F_{-M}(G_c))$ = 127.
Therefore $f(F_{-M}(G_c)) < f(G_C)$.
Hence, **Singular Group**set $\mathbf{s_2 = 2.}$

RM = r_1/total group = 2/4 = 1/2;
RM' = r_2/total group = 2/4=1/2;
SM = s_1/total group = 2/4 = 1/2;
SM'= s_2/total group = 2/4 = 1/2;
d_1 = (RM – SM) = (1/2 – 1/2) = 0;
d_{-1}= (RM' – SM') = (1/2 – 1/2) = 0.

$$2(d_1 + d_0)x^2 + (d_{-0} - d_{-1} - d_1 - 3d_0)x + d_0 - d_{-0} = 0$$
$$2(0+0)x^2 + (0+0-0-3*0)x + 0 - 0 = 0.$$

$$\boldsymbol{x_1 = x_2 = 0.}$$

Hence Probability of embedding,

$$\boldsymbol{P = x/(x - 0.5) = 0/(0 - 0.5) = 0.}$$

4 Experimental Results

Huffman encoding is a lossless compression technique, which can also encode message and produce binary bit stream. Secret data are encoded and compressed by Huffman encoding and secret bit sequence. Table 3 shows 521×512 grayscale 10 cover images: Airplane, Baboon, Barbara, Boat, Couple, Goldhill, Lena, Man, Peppers and Stream. The Peak Signal to Noise Ratio (PSNR) is applied to compare visual quality between the cover image and stego-image. The definition of PSNR is given below

$$PSNR(dB) = 20\log_{10}\frac{255}{\sqrt{MSE}} \dots\dots\dots (12)$$

MSE is the mean squared error between the original image and the modified image which is defined as

$$MSE = \frac{1}{M \times N}\sum_{x=1}^{M}\sum_{y=1}^{N}\left(I(x,y) - I'(x,y)\right)^2 \ldots\ldots\ldots \quad (13)$$

where M and N denotes the width and height of the cover and stego image respectively. Table 3 shows the PSNR values of LSB, RHTF based LSB and our scheme for 90% embedding. In Table 3, we see that the average PSNR is better than LSB and RHTF method.

Table 3: PSNR result for embedding same message

Cover-images (512×512)	LSB	RHTF based LSB	Our method
	PSNR (dB)	PSNR (dB)	PSNR (dB)
Airplane	50.2441	50.2273	50.2938
Baboon	49.9268	49.9983	50.2771
Barbara	50.7814	50.1712	50.8807
Boat	51.1182	51.1892	51.2400
Couple	51.1192	51.1715	51.0477
Goldhill	50.4200	50.5482	50.4287
Lena	51.1189	50.7136	50.7930
Man	50.6599	50.3456	50.8573
Peppers	50.2590	50.2675	50.2300
Stream	50.9532	51.0419	51.4591
Average	50.6600	50.5674	50.7513

4.1 Statistical Attack

In this section, we employ two statistical attacks to evaluate the security of our proposed method, LSB method and RHTF based LSB.

4.1.1 Resisting the Chi Square Attack

We have already discussed that our proposed algorithm is completely based on random embedding of messages on the LSB plane of the cover image. The most interesting thing while resisting the Chi Square is that Chi Square is completely unable to detect the existence of message if embedding is done at a random basis. So it fails to detect the message embedded by our proposed algorithm. After applying the Chi Square Attack on the stego image of Lena obtained by our algorithm we have got the graph shown in Figure 1(b) which proves the inability of detection by Chi Square Steganalysis Technique. On the other hand from Figure 1(a), it is clearly observed that Chi Square Steganalysis technique is very effective at detecting the stego-images using LSB method.

Figures 1 and 2 show a comparison among LSB and our scheme in terms of resistance performance against Chi Square and RS attacks. From the figure it is clear that, any stego-image generated by LSB scheme is detectable by this attack i.e. no stego-image is identified as cover image for 90% embedding. But RHTF based LSB is secured against Chi Square. Figure 1 shows that even for the 90% embedding, 90.52% stego-images generated by RHTF based LSB are identified as cover image when Chi Square attack is applied. On the other hand, our proposed method can produce 96.3% stego-images as cover image for 90% embedding. Accordingly, we can say that our proposed scheme is more secured than LSB and RHTF based LSB against this attack.

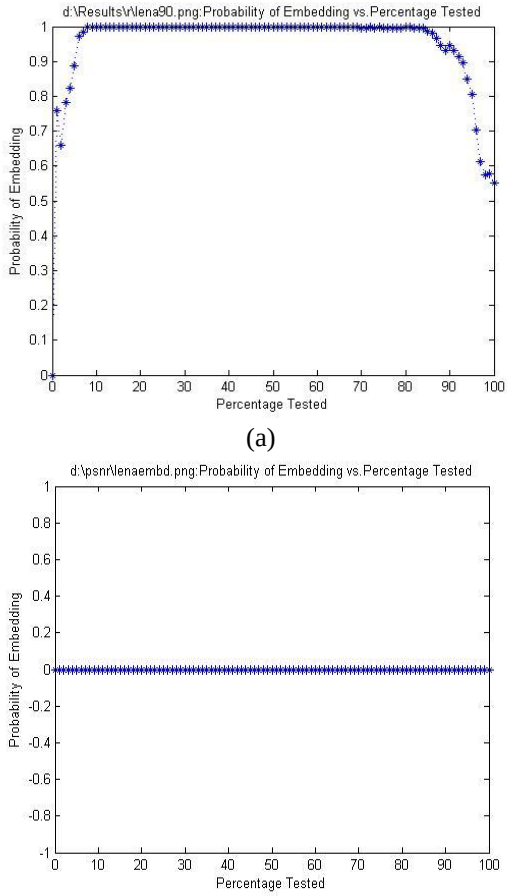


Figure 1: Results of Chi Square Attack on stego image obtained by applying (a) LSB technique and (b) Proposed algorithm with 90% embedding

4.1.2 RS-Attack

Figure 2 shows RS-attack result of gray stego-Lena image with size of 512×512 using our proposed method. The X-axis represents the percentage of embedding and Y-axis represents relative percentage of the regular and singular groups with masks M =[0 1 1 0] and –M =[0 -1 -1 0]. Figure 2 shows that expected value of R_m is almost equal to the value of R_{-m} and S_m is equal to S_{-m}. The other stego-images generated by our proposed method are also tested and produce same results as what Figure 2 represents. Thus we can conclude that our proposed method is secured against the RS-steganalysis.

5 Conclusions

In this paper, we propose a novel technique to produce a better stego-image that is secured against both χ^2 attack and RS attack compared to LSB substitution method and RHTF based LSB approach due to location selection using linear probing. Besides the experimental results shown that the

produced stego-image is totally indistinguishable from the cover image by human eye.

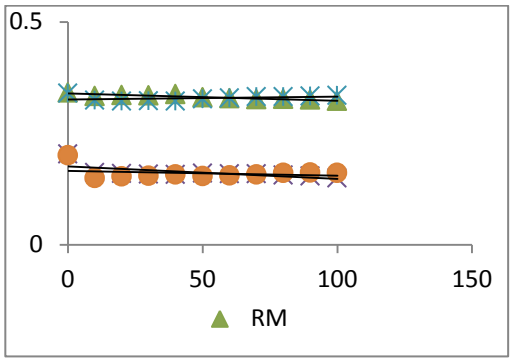


Figure 2: RS diagram of graystego-Lena image with size of 512×512 using our proposed method, where X-axis represents percentage(%) of Embedding and Y-axis represents relative number of Regular and Singular Groups.

References

[1] National Bureau of Standard (U.S), *Data Encryption Standard (DES)*, Federal Information Processing Technical Information Service, Springfield, VA, 1997.

[2] C.C. Chang and H. W. Tseng, "A steganographic method for digital images using side match," *Pattern Recognition Letters*, pp. 1431-1437, 2004.

[3] A. Chedded, J. Condell, K. Curran, and P. M. Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, pp. 727-752, 2010.

[4] J. Fridrich, M. Goljan, and R. Du, "Reliable detection of LSB steganography in color and grayscale images," in *Proceedings ACM Workshop Multimedia and Security*, pp. 27-30, 2001.

[5] A. A. Hanafy, G. I. Salama, and Y. Z. Mohasseb, "A secure covert communication model based on video steganography," in *Proceedings of the 2008 IEEE Military Communications Conference*, pp. 1–6, 2008.

[6] T. Y. Liu and W. H. Tsai, "A new steganographic method for data hiding in Microsoft Word documents by a change tracking technique," *IEEE Transaction on Information Forensics and Security*, vol. 2 no. 1, pp. 24-30, 2007.

[7] H. Luo, F. X. Yu, H. Chen, Z. L. Huang, H. Li, and P. H. Wang, "Reversible data hiding based on block median preservation," *Information Science*, vol. 181, no. 2, pp. 308-328, 2011.

[8] W. Luo, F. Huang, and J. Huang, "Edge adaptive image steganography based on LSB matching revisited," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 201-214, 2010.

[9] D. C. Lou and C. H. Hu, "LSB steganographic method based on reversible histogram transformation function for resisting statistical steganalysis," *Information Science*, doi:10.1016/j.ins.2011.06.003, 2011.

[10] B. Karthikeyan, S. Ramakrishnan, V. Vaithiyanathan, S. Sruti, and M. Gomathymeenakshi, **"**An improved steganographic technique using LSB replacement on a scanned path image**,"** *International Journal of Network Security*, vol. 15, no. 1, pp. 314-318, Jan. 2013

[11] A. R. S. Marçal and P. R. Pereira, "A steganographic method for digital images robust to RS steganalysis," in *International Conference on Image Analysis and Recognition*, LNCS 3656, pp. 1192-1199, 2005.

[12] J. Mielikainen, "LSB matching revisited," *IEEE Signal Processing Letters*, vol. 13, no. 5, pp. 285-287, 2006.

[13] A. Nissar and A. H. Mir, "Classification of steganalysis techniques: A study," *Digital Signal Processing*, vol. 20, pp. 1758-1770, 2010.

[14] R. Petrovic, J. M. Winograd, K. Jemili, and E. Metois, "Data hiding within audio signals," in *Proceedings of the 4th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services*, pp. 88-95, 1999.

[15] R. Rivest, A. Shamir, and Adleman, "A method for obtaining digital signetures and public-key cryptosystems," *Communication of ACM*, vol. 120-126, 1978.

[16] P. Shah, P. Choudhari, and S. Sivaraman, "Adaptive wavelet packet based audio steganography using data history," in *Proceedings of the 2008 IEEE Region 10 and the 3rd International Conference on Industrial and Information Systems*, pp. 1-5, 2008.

[17] M. H. Shirali-Shahreza and M. Shirali-Shahreza, "A new approach to Persian/Arbic text steganography," in *Proceedings of Fifth IEEE/ACIS International Conference on Computer and Information Science*, pp. 310-315, 2006.

[18] W. Stallings, *Cryptography and Network Security – Principles and Practice*, 4th ed. Pearson Education Pvt. Ltd., Indian, 2004.

[19] B. Wang and J. Feng, "A chaos-based steganography algorithm for H.264 standard video sequences," in *Proceedings of the 2008 International Conference Communications, Circuits and Systems*, pp. 750-753, 2008.

[20] H. Wang and S. Wang, "Cyber warfare: steganography vs. steganalysis," *Communication of the ACM*, vol. 47, no. 10, pp. 76-82, 2004.

[21] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," in *Proceedings of the 3rd International Workshop on Information Hiding*, Dresden,Germany, pp. 61-76, 1999.

Amitava Nag obtained his M.Tech from University of Calcutta in the year 2005. He earned his B.Techfrom Dept. of Engineering & Technological Studies, University of Kalyani in the year 2003. He is presently working as an Assistant Professor in Academy of Technology, India and

also working towards his PhD at the Dept. of Engineering & Technological Studies, University of Kalyani. He is a member of IEEE and CSI,India.His area of interest includes Cryptography and steganography.

S. Biswas obtained his Ph.D in engineering from Jadavpur University in the year 2004. He obtained his M.E from Jadavpur University and B.E from Bengal Engineering College (Presently known as Bengal Engineering and Science University, Shibpur) in the year 1994 and 1990 respectively. He is presently working as Scientific Officer (Associate Professor Rank) at the Dept. of Engineering & Technological Studies, University of Kalyani. He has more than 14 years of teaching experience. His area of interest includes, Artificial Neural Network, Image Processing, Frequency Selective Surfaces, Microstrip Antennas.

D. Sarkar has obtained her Ph.D degree in Engineering from Jadavpur University in the year 2005. She has obtained her M.E and B.E from Bengal Engineering College (presently known as Bengal Engineering and Science University, Shibpur) in the year 1994 and 1991 respectively. She is presently working as Scientific Officer (Associate Professor Rank) at Dept. of Engineering & Technological Studies, University of Kalyani. She has more than 14 years of teaching experience. Her area of research includes Artificial Neural Network, Microstrip Antenna, Frequency Selective Surfaces, and Embedded Systems.

Partha Pratim Sarkar obtained his Ph.D in engineering from Jadavpur University in the year 2002. He has obtained his M.E from Jadavpur University in the year 1994. He earned his B.E degree in Electronics and Telecommunication Engineering from Bengal Engineering College (Presently known as Bengal Engineering and Science University, Shibpur) in the year 1991. He is presently working as Senior Scientific Officer (Professor Rank) at the Dept. of Engineering & Technological Studies, University of Kalyani. His area of research includes, Microstrip Antenna, Microstrip Filter, Frequency Selective Surfaces, and Artificial Neural Network. He has contributed to numerous research articles in various journals and conferences of repute. He is also a life Fellow of IETE.

Automated Analysis of Internet Key Exchange Protocol v2 for Denial of Service Attacks

Hasmukh Patel[1] and Devesh C. Jinwala[2]
(Corresponding author: Hasmukh Patel)

Department of Computer Science & Engineering, L. C. Institute of Technology[1]
Mehsana-Unjha Highway, Bhandu, Mehsana, Gujarat, India
Department of Computer Engineering, Sardar Vallabhbhai National Institute of Technology[2]
Ichchhanath, Surat, Gujarat, India
(Email: hasu.patel@gmail.com)
(Received Nov. 24, 2012; revised and accepted July 17, 2013)

Abstract

The Denial of service (DoS) and Distributed Denial of Service (DDoS) attacks are aimed at maliciously consuming the available resources in computing systems to prevent genuine users from legitimately accessing them. These attacks can easily interrupt or disable targeted systems, so it is important for the system to detect and filter bogus connection requests as early as possible. Many common protocols TCP, HIP, SSL, etc., are vulnerable to DoS attacks. Until now, there has been no fit for all, generic solution to resist a DoS/DDoS attacks presented. An attractive alternative therefore is to investigate the approaches by which one can at least reduce the impact of the DoS/DDoS attacks. Our research work presented here focuses on the same.

We develop a formal model of Internet Key Exchange version 2 (IKEv2) protocol using formal specification language of Colored Petri Nets (CPNs) to analyze the protocol for DoS attacks. IKEv2 is a member of the IPSec protocol suite and establishes a security association that includes secret information between source and destination. IPSec provides security services to applications viz. VPN, remote login, email, file transfer etc. Till date no automatic formal analysis of IKEv2 protocol is attempted for DoS attacks, hence we choose IKEv2 protocol to illustrate automatic analysis for DoS attacks. We use simulation approach of CPNs to analyze the protocol for DoS attacks. We analyze the processing cost and memory cost to carry out DoS attacks in IKEv2. In addition, we measure the strength of the protocol against DoS attacks using different experiments in CPNs.

Keywords: Colored petri nets, denial of service attacks, Internet key exchange protocol version2

1 Introduction

With the rapid growth of the Internet and the consequent proliferation of the Web-enabled services in every aspect of human activities, it has become all the more challenging to ensure the security as well as availability of the services offered. One of the potent threats to the security and availability of the Web Services is a Denial of Service (DoS) attack that can be orchestrated by an adversary even without any significant and sophisticated armory and skills. Hence, it is essential to investigate the means and technologies by which such attacks can be thwarted. In case such attacks cannot be thwarted then it is necessary to investigate how the consequences thereof can be minimized to the extent possible. Our research work described herein focuses on the issues associated with the analysis of the DoS attacks and minimizing the consequences thereof.

DoS attacks can broadly classified into logical attacks and resource exhaustion attacks. The logical attacks are kind of smart attacks. To mount logical attacks, the attacker should find out the vulnerabilities in an application installed on or protocols use by targeted system/service provider. In resource exhaustion attacks, an attacker tries to exhaust the resources viz. CPU, memory or network bandwidth of a service provider [1, 14]. The ultimate goal of the attacker is to prevent a genuine user from using the services. Hence, DoS attacks are dangerous and devastating attacks.

The key exchange protocols used to establish a shared key to make secure communication possible. They use expensive cryptographic operations to derive the shared key and to transfer it securely. Hence, the key exchange protocols are vulnerable to DoS attacks. Therefore, it is very crucial to verify the key exchange protocols for availability property. Our focus is to analyze the strength of key exchange protocols against DoS attacks.

2 Motivation

When we design computer systems to pursue security, availability should not be compromised. One of the ways to compromise availability is DoS attacks. Protocols viz. HIP [16], SSL [17], JFK [11, 15] etc. were designed very carefully, even though they are found vulnerable to DoS attacks. Hence, we emphasize that the formal analysis

should model and verify confidentiality, integrity as well as availability property of the protocols.

Designing protocols to withstand DoS attacks is a very complex task [15]. To the best of our knowledge, still there is no guaranteed technique to differentiate attacker's bogus request from genuine user request. Authentication has been used to authenticate the user and allow them to connect to the service provider. However, authentication itself is very resource expensive operation. An attacker may take advantage of this and fire many requests to mount a resource exhaustion attack. Gradual authentication [12] can be applied to increase the level of authentication at each step of the protocol. Even though, the protocols with the gradual authentication need to analyze formally for DoS attacks.

The framework pursued to analyze protocols for DoS attacks is Meadows cost-based framework [12]. It is a basic framework and there is a scope for an improvement. Tritilanunt et al. improved the Meadows framework with refinement in cost calculation [16, 17]. They also model and analyze the HIP protocol for DoS attacks using CPNs. However, they only use computational cost to analyze the protocol.

Internet Key Exchange version 2 (IKEv2) is a simple, efficient and secure key exchange protocol [10]. IPSec provides security services to applications viz. VPN, remote login, email, file transfer etc. Hence, it is very crucial to verify the IKEv2 protocol for DoS attacks. Rui Jiang et al. proposed efficient and secure key exchange protocol to overcome the security shortage of IKE protocol [9]. Cas Cremers presented modeling and analysis of IKEv1 and IKEv2 protocols using Scyther, a security protocol verifier tool, for secrecy and authentication properties only [4]. However, to the best of our knowledge, till date there has been no automatic and formal analysis of IKEv2 for DoS attacks is attempted. Hence, it is very essential to verify IKEv2 protocol for DoS attacks. Therefore, in this paper, we analyze IKEv2 protocol and examine processing and memory cost that leads to resource exhaustion attacks.

The tools viz. Scyther, Proverif, Avispa/Avantssar, NRL, Colored Petri Nets (CPNs) etc. developed for analyzing security protocols using formal methods. CPNs, general-purpose verification tool, is more suitable and beneficial in the analysis and verification of cryptographic protocols [7, 8]. It can be used to analyze the behavior of the modelled system using simulation, state space methods and model checking [7]. In this paper, by adopting idea of Tritilanunt's [16] refined processing cost calculation of Meadows framework [12], we develop a formal model of IKEv2 protocol using CPNs to analyze for DoS attacks. We use a simulation approach provided in CPN Tools to achieve a formal analysis. Our simulation provides an accurate cost estimation of processing as well as memory of protocol execution comparing among principals. In addition to that, we measure the tolerance of IKEv2 protocol under DoS attacks.

The contributions of this paper are.

- Formal modeling and automatic analysis of IKEv2 protocol using CPNs (Section 3 and Section 4);
- Identification of three types of attackers to analyze IKEv2 protocol (Section 3);
- As per idea of Meadows framework, processing and memory cost analysis at each step of protocol (Section 4);
- Performance measure to check tolerance of IKEv2 protocol under DoS attacks (Section 4).

The remaining paper is organized as follow. In Section 3, we discuss modeling of IKEv2 protocol and types of attackers considered for analysis. In Section 4, we analyze the IKEv2 protocol for computational and memory cost. In Section 5, we describe related work to verification of protocols for DoS attacks using CPNs. We conclude our work in Section 6.

3 Modeling

In this section, we model the IKEv2 protocol to analyze for DoS attacks using CPN Tools. We describe the types of attackers identified for analysis of IKEv2 protocol. Table 1 gives the message sequence of IKE v2 protocol.

Table 1: IKEv2 protocol

$$A \rightarrow B: HDR_1, SA_{a1}, g^{XA}, N_A$$
$$B \rightarrow A: HDR_2, SA_{b1}, g^{XB}, N_B$$
$$A \rightarrow B: HDR_3, \{ID_A, ID_B, AUTH_A, SA_{a2}, TS_a, TS_b\}_{SK}$$
$$B \rightarrow A: HDR_4, \{ID_B, AUTH_b, SA_{b2}, TS_a, TS_b\}_{SK}$$

Where

$$AUTH_a = \{SA_{a1}, g^{XA}, N_A, N_B, prf_{SK_{pa}}(ID_A)\}_{SK(A)}$$
$$AUTH_b = \{SA_{b1}, g^{XB}, N_B, N_A, prf_{SK_{pb}}(ID_B)\}_{SK(B)}$$

We describe IKEv2 protocol in the annotated Alice-Bob specification in Table 2. The purpose of Alice-Bob specification is to give the details of operations in execution of protocol on initiator as well as responder side. Table 3 presents the cost of some specific cryptographic algorithms, which are part of IKEv2 protocol. The costs of operations are from the cryptographic protocol benchmarks by Wei Dai [5].

3.1 Attacker Types

By adopting idea of Tritilanunt's [16], we identify three types of attackers to analyze IKEv2 protocol that follow the protocol execution and have a limited capability to spoof the messages.

Attacker Type 1: Attacker Type 1 randomly chooses the components of first message, and then takes no further action. The intention of this type of attacker is to flood the responder using spoofed IP addresses.

Table 2: Annotated Alice-Bob specification of IKEv2

$A \rightarrow B$	$\text{createexp}_1(g^X A), \text{computenonce}_1(N_A) \parallel g^{XA}, N_A \parallel$ $\text{verifygroup}(g^X A), \text{accept}_1$
$B \rightarrow A$	$\text{createexp}_2(g^X B), \text{computenonce}_2(N_B) \parallel g^{XB}, N_B \parallel$ $\text{verifygroup}(g^X B), \text{accept}_2$
$A \rightarrow B$	$S_1 = \text{generatesign}_1(N_A, N_B, g^{XB}, g^{XB}, ID_A, SA_a 1)$, $Enc_1 = \text{encrypt}_1(K, \{ID_A, S_1, SA_{a1}\})$, $D_1 = \text{generatemac}_1(K, Enc_1) \parallel Enc_1, D_1 \parallel$ $\text{generatedh}_2(g^{AB}), K = \text{computekey}_2(N_A, N_B, g^{AB})$, $\text{verify}_1(D_1 = \text{generatemac}_2(K, Enc_1)), \text{decrypt}_1(K, Enc_1)$, $\text{verifysign}_1(S_1), \text{accept}_3$
$B \rightarrow A$	$S_2 = \text{generatesign}_2(N_A, N_B, g^{XA}, g^{XB}, ID_B, SA_{b2})$, $Enc_2 = \text{encrypt}_2(K, \{ID_B, S_2, SA_{b2}\})$, $D_2 = \text{generatemac}_3(K, Enc_2)$ $\parallel Enc_2, D_2 \parallel \text{verify}_2(D_2 = \text{generatemac}_4(K, Enc_2))$, $\text{decrypt}_1(K, Enc_2), \text{verifysign}_1(S_2), \text{accept}_4$

Table 3: Computational cost of CPU usage of specific algorithm

Key Exchange	**Megacycle/ Operation**	**Symmetric Crypto**	**Cycles/ Bock**
Diffie-Hellman Key pair generation	1.51	DES	15320
Diffie-Hellman Key Agreement	2.16	AES/CBC (128-bit key)	1041
Public Key Crypto	**Megacycle/ Operation**	**Hash**	**Cycles/ Bock**
RSA Signature	2.71	HMAC/MD5	932
RSA Verification	0.13		

Attacker Type 2: Attacker Type 2 follow the protocol for first message. Randomly chooses the components to create the third message. The intention of this type of attacker is to make responder to consume resources for expensive operations like Diffie-Hellman key generation and encryption.

Attacker Type 3: Follow the protocol up to third message and then takes no further action. Computation includes generation of encryption and authentication key, signature generation and encrypting the message. The intention of this type of attacker is to make responder to verify the signature and sign the message to generate the response of third message.

3.2 Modeling using Colored Petri Nets for IKEv2 protocol

We use CPNs to model IKEv2 protocol. Figure 1 shows the main page of hierarchical CPNs for IKEv2 protocol. The model consists of three main components. They are initiator, network and responder. There is a subpage for generation and processing of each message from the main page. Figure 2 shows responder subpage to process the received message 1 and generate message 2. The color of token contains three kinds of data includes name of component, processing cost and memory cost.

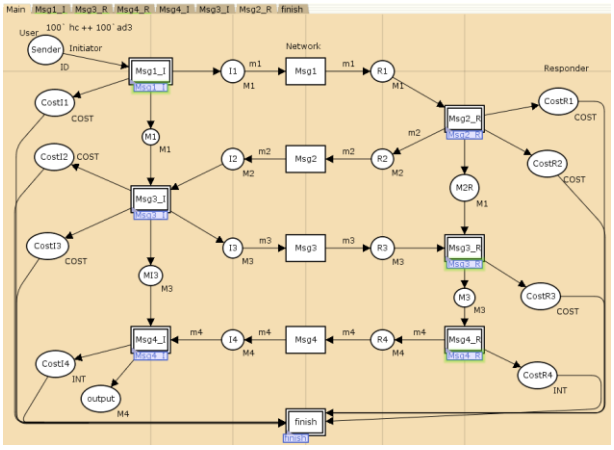


Figure 1: Main page of hierarchical Coloured Petri Nets of IKEv2

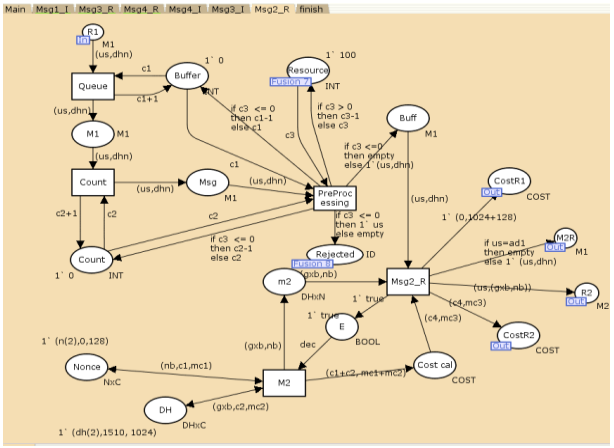


Figure 2: Responder sub page - processing message 1 and generate message2

4 Analysis

In this section, we analyze the IKEv2 protocol. We consider three parameters for analysis. First is processing cost of cryptographic operations involved in protocol execution. Second is memory cost for components of protocol require to store in memory as part of protocol execution. We measure and analyze unbalanced computation and memory cost. Third is to measure the tolerance of IKEv2 protocol under different DoS attacks scenarios.

4.1 Processing Cost Analysis

We simulate the model of IKEv2 protocol for honest client and three types of attackers identified in Section 3. Table 4 shows the computational cost incurred between different

types of attackers and responder. In case of honest client and attacker Type 1, the cost of initiator and responder are same.

Table 4: Comparison of Initiator and Responder computational cost for IKE v2

Protocol	Initiators	Initiator Cost	Responder Cost
IKE v2	Honest Client	6544	6544
	Attacker Type1	1510	1510
	Attacker Type2	1511	3673
	Attacker Type3	6398	6544

Table 5: Comparison of Initiator and Responder memory-cost for IKE v2 protocol

Protocol	Initiators	Initiator Cost(bits)	Responder Cost(bits)
IKE v2	Honest Client	3744	3744
	Attacker Type1	1152	2304
	Attacker Type2	1152	3744
	Attacker Type3	3744	3744

IKEv2 protocol uses cookie when it encounter more than pre-configured number of half-open request packets. If many IP-spoofed requests are received in a short time, IKE v2 protocol send cookie require message to one of the sender and ignore other messages [10]. This prevents flooding attacks at message1.

Attacker Type 2 randomly chooses the message component hence the cost of creating the message is almost negligible. On the other side the responder has to perform expensive operations to calculate Diffie-Hellman key and other required keys before checking the message correctness. Hence, attacker Type 2 may lead to resource exhaustion at responder. Attacker Type 3 consuming highest amount of resource among all, but the ratio of the resource consumption of responder to the attacker is less than attacker Type 2. Hence, we conclude that attacker Type 2 is most effective attacker compare to other types of attackers.

4.2 Memory Cost Analysis

Table 5 shows the memory requirement of the IKEv2 protocol in execution for honest client and three types of identified attackers in Section 3. As per the recommendation of IKEv2 specification [10] minimum nonce size is 128 bits, Diffie-Hellman key size is 1024 bits, encryption key and MAC key size are 256 bits and 160 bits respectively. Diffie-Hellman key size depends on the group selected to establish a security association. The key size of an algorithm depends on the selection of cryptographic suite in process to establish a security association. We consider the minimum key size for components of protocol in analysis.

Stateless connection [3] and gradual authentication [12] are techniques proposed to prevent the memory exhaustion attacks. However, the responder cannot be a complete stateless. Components like nonces, encryption keys etc. need to be stored at responder for authentication of connection.

Table 5 show that attacker Type 1 may lead to memory exhaust; however, IKEv2 use cookie when number of half-open connection request exceeds pre-configured number.

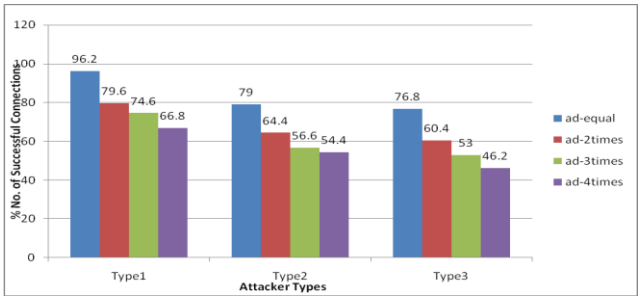


Figure 3: DoS attack tolerance of IKEv2 protocol

Once first message is received correctly and response to the message generated, half-open connection counter decremented and state is created at responder side. We can see from Table 5 that there is a large difference in memory requirement of attacker Type 2 and responder. There is no way to detect that a message received is spoofed until Diffie-Hellman key and other required keys are calculated to authenticate the request, hence it may lead to a memory exhaust. Attacker Type 2 spoofs the message components; hence, it does not require to store the message components. Memory requirements of attacker Type 3 and responder are same. Therefore, Attacker Type 2 is most effective attacker among all.

4.3 DoS Attack Tolerance of IKEv2 Protocol

We set up an experiment to measure the tolerance of IKEv2 protocol for DoS attacks under different scenarios. We make a pair of honest client with each type of attacker. We measure the number of successful connections of the honest client in case of DoS attacks by each type of attacker. To measure the tolerance of IKEv2 protocol under DoS attacks, we increase number of requests of attacker by two times, three times and four times and note the number of successful requests of the honest client in each case. The overall result is shown in Figure 3.

From Figure 3, we note that, number of successful requests of the honest client decreasing as we go from attacker Type 1 to Type 3. In case of attacker Type 3, number of successful connections of honest client is least. This is because the requests from attacker Type 3 consume the highest amount of resources of responder among all attackers. The ratio of resource consumption of responder to resource consumption of attacker Type 2 is higher than that of attacker Type 3. Table 4 and Table 5 confirm the same. Figure 3 shows the percentage number of successful connections of honest client in twelve different experiments. We conclude from Figure 3 that attacker Type 3 is most effective to interrupt the performance of the responder.

5 Related Work

The purpose of this section is to provide work related to the analysis of security protocol for DoS attacks using CPN Tools.

CPNs has been used for modeling and analysis of security protocols since many years. CPNs is very effective in the analysis and verification of cryptographic protocols [6, 7, 8]. Yang et al. analyzed Andrew secure RPC protocol for secrecy and authentication using CPNs [19, 20]. Issam Al-Azzoni et al. presented technique to model and analyze protocol using CPNs with implementation of TMN protocol [2]. The authors have also integrated generic intruder model and introduced techniques to reduce size of occurrence graph.

There are also efforts to analyze the protocol for DoS attacks using CPN Tools. Jin et al. has used CPN Tools for modeling and analysis of JFK protocol for DoS attacks [18]. Tritilanunt et al. [16, 17] have developed timed CPNs model by adopting the key idea of Meadows framework [12, 13] and incorporating refined cost calculation for SSL and HIP protocols to analyze for DoS attacks. The authors have also calculated the number of successful connections of legitimate user under different attacks strategies.

To the best of our knowledge, there is no implementation of IKEv2 protocol model using CPNs to analyze for DoS attacks. Therefore, we model the IKEv2 protocol using hierarchical CPNs and analyze for processing cost as well as memory cost. In addition to that, we measure the strength of protocol against DoS attacks under different scenarios of DoS attacks.

6 Conclusion and Future Work

When we design computer systems to pursue security, availability should not be compromised. One of the ways to compromise availability is DoS attacks. It is essential to investigate a formal analysis technique that can at least reduce the impact of the DoS attacks.

In this paper, we have developed formal specification of IKEv2 protocol in CPNs. We analyzed IKEv2 protocol for processing and memory cost. We use simulation approach of CPN Tools to measure the tolerance of the protocol against DoS attacks under different scenarios.

In future work, we plan to extend the protocol model by integrating more powerful intruder model. The main issue is to identify the attacker actions and to assign the cost to those actions. Another area to explore is to design and implement a generic model to verify protocols for availability property with goal to improve protocol against DoS attacks. Our eventual goal of this work is to analyze protocols for DoS attacks and strengthen protocols against DoS attacks.

References

[1] CERT, *Denial of Service Attacks*, 3 May 2010. (www.cert.org/tech_tips/denial_of_service.html)

[2] I. Al-Azzoni, D. G. Down, and R. Khedri. "Modeling and verification of cryptographic protocols using coloured petri nets and design/CPN," *Nordic Journal of Computing*, vol. 12, no. 13, pp. 201-228, June 2005.

[3] T. Aura and P. Nikander. "Stateless connections," in *Proceedings of the First International Conference on Information and Communication Security (ICICS '97)*, LNCS 1334, pp. 87-97, Springer-Verlag, 1997.

[4] C. Cremers, "Key exchange in IPsec revisited: Formal analysis of IKEv1 and IKEv2," in *16th European Symposium on Research in Computer Security (ESORICS-2011)*, pp. 315-334, Leuven, Belgium, Sep. 12-14, 2011.

[5] W. Dai, Crypto++ 5.2.1 Benchmarks, 2009. (http://www.cryptopp.com/benchmarks.html)

[6] E. M. Doyle, *Automated Security Analysis of Cryptographic Protocols using Coloured Petri Net Specification*, Master of Science Thesis, Department of Electrical and Computer Engineering, Queen's University, Ontario, Canada, 1996.

[7] K. Jensen, L. M. Kristensen, L. Wells. "Coloured petri nets and CPN tools for modeling and validation of concurrent System," *International Journal Software Tools Technology Transfer*, vol. 9, pp. 213-254, 2007.

[8] K. Jensen, "An introduction to the theoretical aspects of colored petri nets," in *Workshop on the Applicability of Formal Models*, pp. 230-272, 1994.

[9] R. Jiang, A. Hu, and J. Li, "Formal protocol design of ESIKE based on authentication tests," *International Journal of Network Security*, vol. 6, no. 3, pp. 246-254, 2008.

[10] C. Kaufman, P. Homan, Y. Nir, P. Eronen, *Internet Key Exchange Protocol Version 2 (IKEv2)*, RFC 5996, Sep. 2010. (http://www.rfc-editor.org/info/rfc5996)

[11] L. Kuppusamy, J. Rangasamy, D. Stebila, C. Boyd, and J. N. Gonzalez. "Towards a provably secure DoS-Resilientkey exchange protocol with perfect forward secrecy," in *Indocrypt*, pp.379-398, Springer-Verlag, Chennai, India, 2011.

[12] C. Meadows. "A cost-based framework for analysis of denial of service networks," *Journal of Computer Security*, vol. 9, no. 1, pp. 143-164, 2001.

[13] C. Meadows. "A formal framework and evaluation method for network denial of service," in *Proceedings of 12th IEEE Computer Security Foundations Workshop (CSFW)*, pp. 4-13, 1999.

[14] J. Smith, S. Tritilanunt, C. Boyd, J. Gonzalez Nieto, and E. Foo. "Denial of service resistance in key establishment." *International Journal of Wireless and Mobile Computing*, vol. 2, no. 1, pp. 59-71, 2007.

[15] J. Smith, J. M. Gonzalez Nieto, and C. Boyd. "Modeling denial of service attacks on JFK with Meadows's cost-based framework," in *4th Australasian Information Security Workshop*, vol. 54, pp. 125-134, 2006.

[16] S. Tritilanunt, C. Boyd, J. M. Gonzalez Nieto, and E. Foo. "Cost-based and time-based analysis of DoS-

resistance in HIP," in *Proceedings of the Thirteeth Australasian Computer Science Conference*, pp. 191-200, Ballarat, Australia, 2007.

[17] S. Tritilanunt, C. Boyd, E. Foo, and N. Gonzalez Juan. "Using coloured petri nets to simulate DoS-resistant protocols," in *7th Workshop and Tutorial on Practical Use of Coloured Petri Nets and the CPN Tools*, Denmark, Aarhus, 2006.

[18] J. Wei, G. Su, and M. Xu. "An Integrated Model to Analyze Cryptographic Protocols with Colored Petri Nets," *11th IEEE High Assurance Systems Engineering Symposium*, IEEE, pp. 457 -460, 2008.

[19] Y. Xu and X. Xie. "Modeling and analysis of security protocols using colored petri nets," *Journal of Computers*, vol. 6, vo. 1, Academy Publisher, Jan. 2011.

[20] Y. Xu and X. Xie. "Modeling and analysis of authentication protocols using coloured petri nets," in *3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication*, pp. 443-448, 2009.

Hasmukh Patel is serving as an Assistant Professor in Computer Science & Engineering Department with Laljibhai Chaturbhai Institute of Technology, Bhandu (India). His major areas of interests are verification of security protocols, Information and Network Security.

Dr. Devesh Jinwala is serving as an Associate Professor in Computer Engineering with Sardar Vallabhbhai National Institute of Technology, Surat (India). His major research areas of interests are Information Security in general and that in Resource Constrained Environments, specifically; Algorithms & Computational Complexity and Using Ontologies in Software Requirements and Specifications.

Energy Characterization of a Security Module in ARM Processor

Felipe dos Anjos Lima, Edward David Moreno, Dellano Oliveira D. dos Santos, and Wanderson Roger Azevedo Dias
(Corresponding author: Edward David Moreno)

DCOMP/UFS - Department of Computer Science, Federal University of Sergipe
Aracaju, Sergipe, Brazil
(E-mail:{felipes1474, edwdavid, dellano.lelo, wradias}@gmail.com)
(Received Apr. 26, 2013; revised and accepted Nov. 26, 2013)

Abstract

This article shows the results obtained during simulations that measured runtime and energy consumption of a security module (SEMO) when it executes in ARM processor. For the simulations, we considered the impacts of four algorithms (i.e. RSA, SHA-1, Random Numbers Generator and AES). We have used the Sim-Panalyzer simulator and obtained an average energy consumption (x2 Joules) and runtime (x26000 cycles). We also show the impact of some compiler optimizations in the energy consumption of the AES algorithm.

Keywords: AES, ARM, energy, RSA, security

1 Introduction

In the Knowledge era, information is increasingly spreading around the world. This is very substantial, owing to the fact that people are able to easily access the information they want. It only takes a few clicks on the internet, and everything is within reach. Therefore, this easiness brings some problems which need to be carefully analyzed, for instance, we know many people could act maliciously and try to gather information from others without proper permission.

By the time internet was created, people started to use it to perform several tasks, which cost long to be accomplished. For example, a bank transfer can be properly done with just a few clicks, without even leaving home. However, in order to accomplish a safe transaction, some password protection methods and information security mechanisms are needed, so that the site is reliable. If some computer hacker were able to intercept the users passwords, the damages to the user account could be irreparable. Furthermore, it is fundamentally important that the access, to the kind of system discussed above, is classified. For this purpose, some security mechanisms like password usage may be utilized. However, due to security reasons, these passwords may not be generated without any technique [5]., they must be created by reliable software so that they cannot be decrypted by unauthorized people.

Thus, security is a fundamental requirement at any serious computational system. Therefore, by the last years, several algorithms that aim to mask password keys, texts or any kind of confidential information were developed. Also, several security modules still being created trying to guarantee reliability at transactions performed by electronic devices, and the safety of the information stored. These modules can be implemented in hardware or software. In case they were implemented in hardware, they are expected to be embedded on chips, performing several security mechanisms.

The implementation of security modules in software follows the same philosophy, and also presents software components that protect data. Thus, the major objective of a security model is to provide a supervised system to execute its tasks independently, without having to deal with security issues. Therefore, in this article, we present a software implementation of a security module, called SEMO which is similar to one TPM (Trusted Platform Module) [3], which proved to be promising on the information security field. Then, we present analysis of our security module, making usage of the architectural simulation tool Sim-Panalyzer [1], in that we have obtained performance values by measuring runtime and energy consumption from our SEMO.

This article is divided in six sections. In Section 2 we present the SEMO module and its components; in Section 3 we depict one software implementation of the SEMO (TPM in software); Section 4 shows the simulations and analysis of the module; Section 5 presents the impact of the key seize on the energy consumption of AES algorithm, and finally, in Section 6 we present conclusions and ideas for future works.

2 SEMO - A Security Module

Our security module (SEMO) is similar to a TPM since it is a security module composed by a set of components with the intention of protecting the information stored on the device in that a TPM is coupled. This module can be developed on both hardware and software. In case it is implemented directly in hardware is known as TPM (Trusted Platform Module).

Every key generated by a cryptography process is encapsulated in the TPM so that it is not possible to access it from external models. Thus, external attacks aiming to discover passwords or stealing information may not succeed. In addition, the security module can also guarantee safety on both web browsers and email boxes. Figure 1 shows an example of a TPM. As we can observe on Figure 1, a TPM module holds a set of components which allows the execution of a set of security tasks. Its main units are described as follows:

- **I/O**: manages the information flow on the bus, directing messages to the appropriate components;
- **Cryptographic Processor**: executes cryptographic asymmetric operation and hashing utilizing well-known algorithms by the security community, like RSA, AES or SHA-1;
- **Key Generation**: creates pair of keys for asymmetric algorithms and symmetric keys;
- **Random Number Generation**: it is the source of randomness of a TPM. The TPM uses these random values on key generation and randomness on signatures;
- **SHA-1**: it is the hash function which is primarily used by a TPM, because he is a trustful implementation of a hash algorithm;
- **Opt-In**: provide protection mechanisms that allow the TPM to be turned on/off, or enabled/disabled;
- **Execution Engine**: execute programs according to the commands received by the TPM, using the values from I/O;
- **Non-Volatile Memory**: utilized for storing persistent identity and the state associated to the TPM;
- **Platform Configuration Register**: it is a local storage with 160 bits for measuring the discrete identity.

3 Software Implementation of the SEMO

In this section, we describe our contribution, in other words, a TPM implementation in software, with some

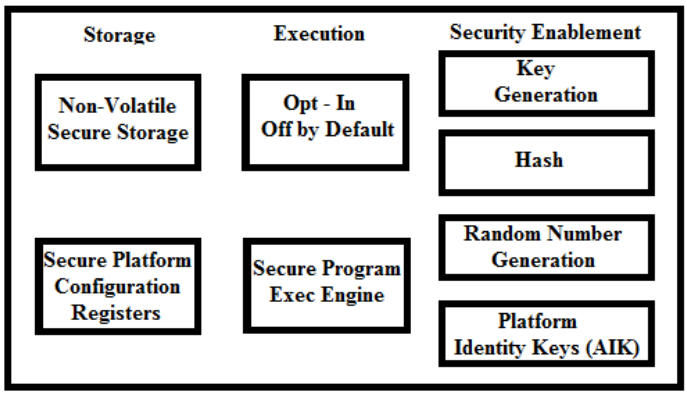


Figure 1: Components of a TPM

security components: namely, AES Engine, SHA-1 Engine, Random Number Generator and RSA Engine. Every component was implemented using C as its programming language. Figure 2 depicts the architecture from the SEMO module we have developed.

3.1 AES Engine

The AES Engine (AES - Advanced Encryption Standard) component that was implemented in our SEMO provides data encryption utilizing 128, 192 and 256-bit keys. The AES algorithm performs, during the encryption process, some operations over the data blocks received as input. Next, we shall present the operations performed by this component.

- **SubByte**: the bytes of the state variable are replaced utiizing a substitution table (S-BOX);
- **ShiftRow**: the bytes from each line of the state variable are rotated;
- **MixColumn**: each column from the state variable is transformed in another column through a modular multiplication;
- **AddRoundKey**: the key of the round is added to the state variable using XOR operation.

The four operations above can be inverted. In this manner, in order to perform the decryption of an encrypted text, the operation SubBytes, ShiftRow, MixColumn and AddRoundKey need to be inverted. The operations InvSubBytes, InvShiftRow, InvMixColumn and InvAddRoundKey operate over the encrypted data block.

3.2 SHA-1 Engine

The SHA-1 (Secure Hash Algorithm) Engine component increments an important document authentication function to the TPM, due to the fact that keys generated by the hash function from this algorithm are unique, in other words, two distinct documents do not own the same

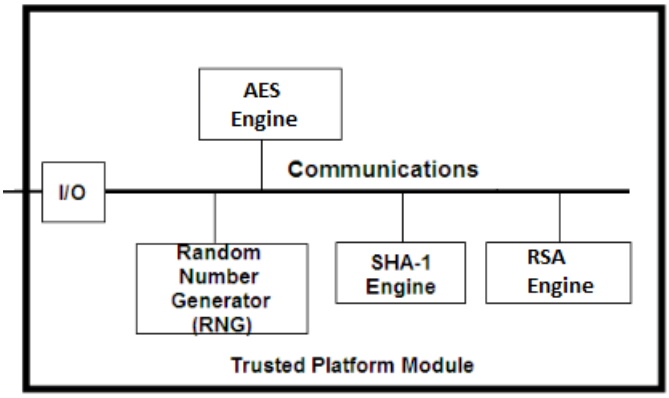


Figure 2: Components of our security module SEMO

representation. Therefore, during some transaction that demands a digital signature from the document, any modification on it would be perceived by the SEMO, and the authentication shall not be done.

3.3 Random Number Generator

The Random Number Generator (RNG) we implemented generates random values that are utilized by the RSA Engine Component for the encryption processes of data [5]. These values remain encapsulated inside the SEMO. However, the algorithm executed by the RSA Engine Component uses a random choice of prime numbers as a stop of the encryption process.

3.4 RSA Engine

The RSA (Random Scheduling Algorithm) Engine Component runs an encryption algorithm of public key, in that, every participant in the data transfer holds a public and a private key. These keys are pairs of integer numbers.

With the RSA Engine Component embedded on the architecture of the SEMO, our module inherited a new component that helps in the security process of information.

4 Simulation and Analysis of SEMO

In this section we present the simulation tool Sim-Panalyzer. We also present the analysis and simulations and their results, considering the impacts on energy consumption and performance at each one of the SEMO components.

4.1 Sim-Panalizer Simulator

Sim-Panalyzer is an energy consumption simulation tool, based on the SimpleScalar which simulates processors [2].

Table 1: Architectural components of Sim-Panalyzer

Architectural Component	Description
aio	Address bar of the input/output units
dio	Data bar of the input/output units
irf	Integer registers
fprf	Floating point registers
*il*1	Level 1 instruction caches
*dl*1	Level 1 data caches
*il*2	Level 2 instruction caches
*dl*2	Level 2 data caches
itlb	TLB instruction table
dtlb	TLB data table
btb	Branch Target Buffer
bimod	Switch Predictor
ras	Address stack result
logic	Random logic circuit
clock	System clock generator
uarch	Microarchitecture (the way USA is implemented in a processor)
fpu	Floating point unit
mult	Multiplication unit
alu	Arithmetic logic unit

SimpleScalar [1] simulates the computational architecture of a CPU platform, cache and memory hierarchy, and based on this model, it manages to simulate real programs over the specified platform. The processor utilized in this article comes from the ARM (Advanced RISC Machine) family [1].

Sim-Panalyzer was built based on the ISA (Instruction Set Architecture) from the families ARM [7] and Alpha of processors, obtaining great results on this kind of simulations [6]. Sim-Panalyzer has several components that altogether generate the total of energy consumption for the architecture [4]. Each one of these components plays an important role on measuring the total consumption of energy spent by the algorithms. Table 1 shows the components of Sim-Panalyzer that consume energy. The parameters for generating those vital parts of the computer were set as input for the Sim-Panalyzer simulator, which altogether generate the patterns of measurement of performance and energy consumption.

4.2 Analysis

While the simulations were performed on the Sim-Panalyzer tool, we have observed that SEMO obtained an average value of energy consumption of 2 Joules when a 1Kb File was subject to an encryption process. On Figure 3, we present the energy consumption of the components AES Engine, SHA-1 Engine, RNG and RSA Engine from our SEMO implementation, and then we detail the architectural elements which obtained the highest energy consumption values. On Figure 4 we present the runtime values per cycles from each one of these components.

As we can observe on Figure 4, the Component AES Engine presented the lowest consumption, this happens because the number of operations executed by the AES algorithm in this component is smaller than in the other ones. Also, the AES was designed to be utilized by embedded systems, which work with a lesser energy consumption. The RSA engine was the one that presented the largest energy consumption values in our SEMO. The components AES and RSA utilized 128-bit keys.

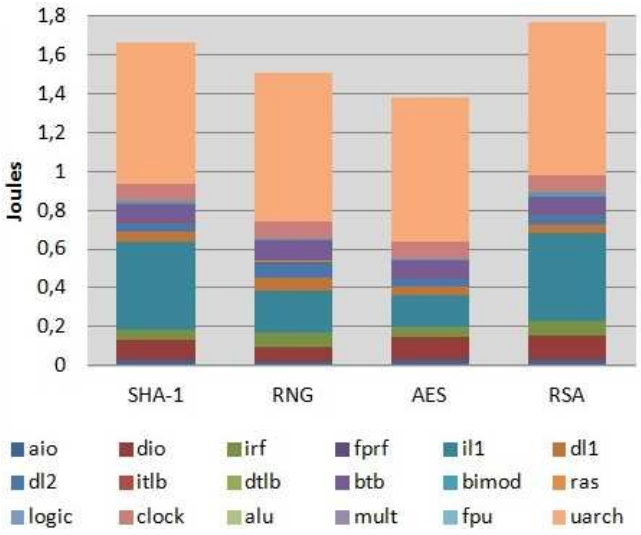


Figure 3: Energy consumption from SEMO components

Regarding the architectural components that are present on the ARM platform we utilized in the simulations, it is possible to perceive that the architectural elements uarch (microarchitecture - the way that ISA is implemented on a processor) and ill (instruction cache level L1) have obtained the highest energy consumption values.

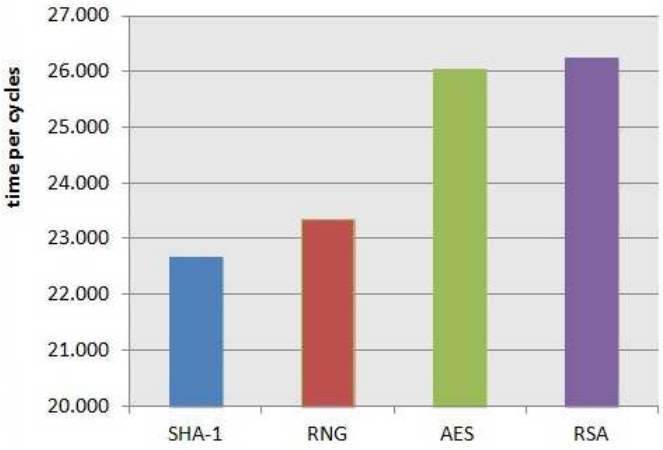


Figure 4: Performance of SEMO components

On Figure 5, we can observe that the components SHA-1 Engine and RNG presented very similar performance measurements, as well as AES Engine and RSA Engine. The simulations were performed in a netbook, with an Athon94 1.66GHz processor, and 2GB of RAM, running a Linux Ubuntu v11.04 operational system.

The SEMO can be implemented on several devices whether they are large or mobile ones. Considering the increasing miniaturization of computer devices, it is important that the existing software could run rapidly, without exhausting the energy available, because is not always possible to recharge batteries. Considering that a device that implements a SEMO could utilized all of its components to perform just one task, we present on Figure 5 the total energy consumption from our module.

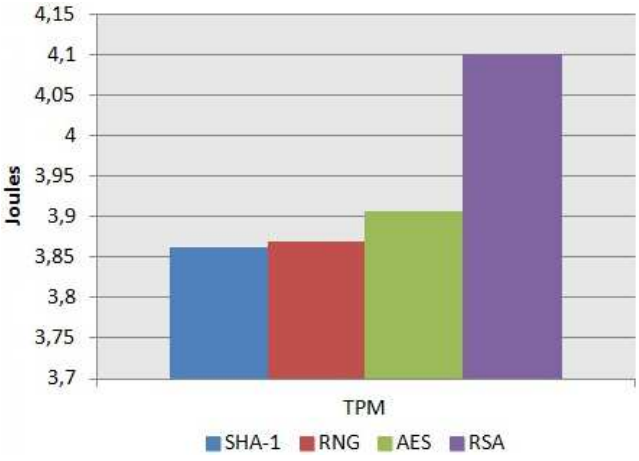


Figure 5: Energy consumption from the SEMO components

5 Detailed Analysis of the AES Component

In this section we make an analysis of the AES encryption algorithm, showing the impact the length of the keys provokes on the algorithms energy consumption and runtime.

5.1 Compiler Optimization

The executable codes generated by the optimizations are semantically equivalent to the original ones. In brief, they behave the same as the original codes given the same input [7]. With the increase in the utilization of embedded systems, the demand for code optimization has been stimulated so that energy consumption can be reduced [8]. In this article, we used gcc version 4.4.5 applying the following optimizations: -O0, -O1, -O2, -O3 and -Ip when compiling MiBenchs. The effects of each type of optimization are described hereafter:

- **-O0**: represents the default compilation, in other words, without any optimizations;

- **-O1**: this type of optimization enable some specific functions, for instance: (i) - Elimination of common subexpressions; (ii) - Global registry allocation;
- **-O2**: these are own specific functions, namely: (i) freorder-blocks: this function records blocks to be compiled in order so that algorithm processing costs can be reduced; (ii) falign-functions: this function reduces the information loading of compiling informations;
- **-O3**: these types of optimization also have specific functions, for example: (i) frename-registers: this function utilizes the maximum of all registers in a minimized way, thus avoiding false dependencies in the code; (ii) finline-functions: this function heuristically decides the simpler functions in order to declare them as static;
- **-Ip**: enables some optimizations like, for instance, dead-code elimination.

5.2 Key Size Impact on Energy Consumption

During the simulations we have utilized a 1Mb text file, which was encrypted and decrypted. We have also used 128, 192 and 256-bit keys (see Figure 6).

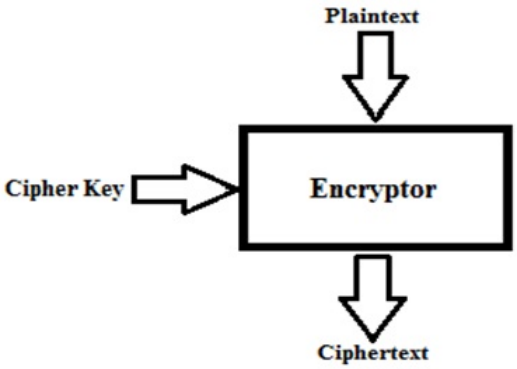


Figure 6: AES input and output

The file used as input for the simulations is handled in blocks by the algorithm. At each step, a 128-bit block is encrypted. The quantity of necessary operations to encrypt and decrypt each block depends on the length of the key used by the process. Table 2 presents the number of rounds executed by the AES algorithm for each cryptography key.

In this section, we present the impact key length has, highlighting the consumption of all architectural components of an ARM processor. As we can see on Figure 7, almost every architectural component obtained similar energy consumption value, therefore we highlight the dio component, which presented an average reduction of 23% when the key length increases. The simulation performed on Sim-Panalyzer showed that the O2 optimization presented a better performance when compared to other optimizations. The average gain was 10% for 128-bit keys when compared to other key lengths. Furthermore, it is possible to observe that the optimization flag Ip could not provoke any significant reduction on runtime, presenting similar results to the O0 which does not enable any greater impact optimizations (see Figure 8). Compiler optimizations are processes of improving the output of a compiler, which is an executable file, according to [7]. By means of switches, substitutions and even exclusion of structures, the compiler can return a faster program executable, consuming less memory.

Table 2: Number of rounds for encrypting/decrypting

Key Length	Number of Rounds
128 bits	10
192 bits	12
256 bits	14

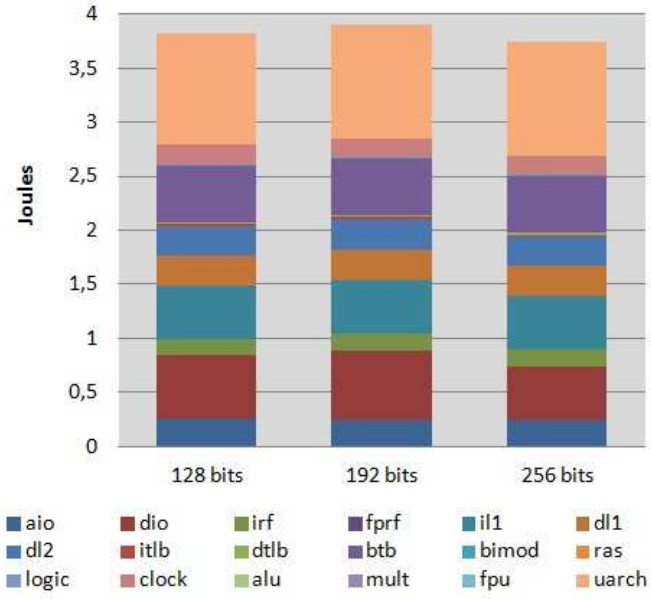


Figure 7: Characterization of energy consumption of AES

5.3 GCC Compiler Optimization Impacts on Energy Consumption

The analysis of the results show us that if the AES code is compiled utilizing O3 optimization, the average total consumption of all components is lower, when compared to the other optimization flags (see Figure 9).

The main optimizations enabled by the O3 flag are:

- **Inline-functions**: replaces every function call by the body of the function itself.

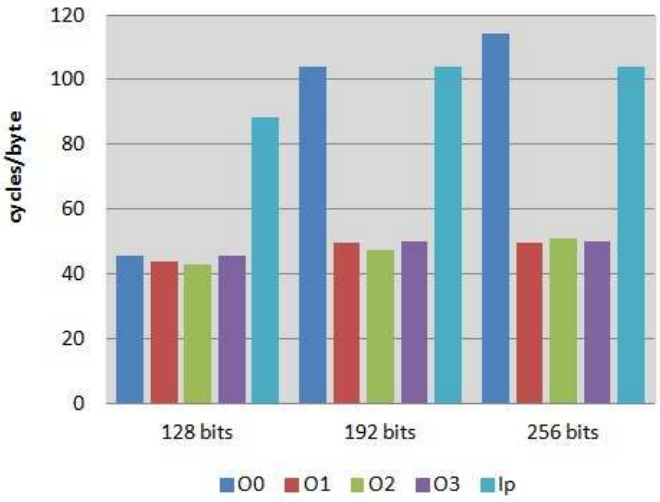


Figure 8: AES runtime measurements

- **Rename-register**: eliminates the dependencies between registers by reorganizing the stored values.

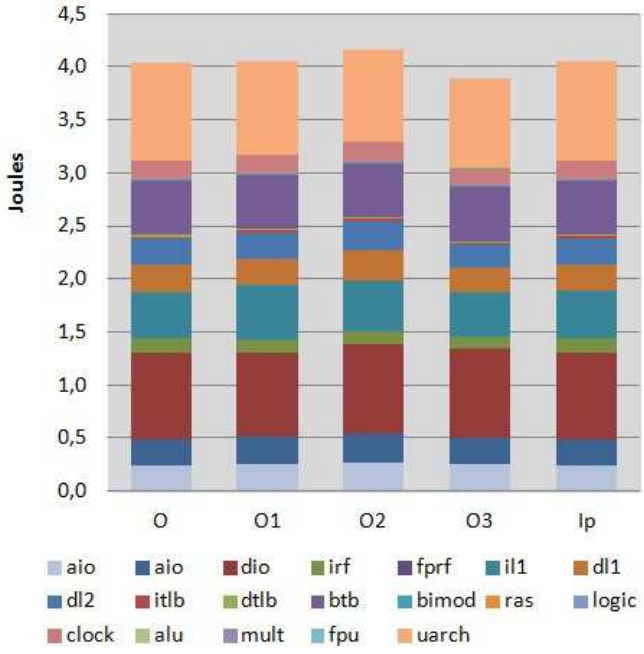


Figure 9: AES energy consumption

By activating the inline-functions optimization during the compilation step, every function present on the main program is replaced by the code that appears in the function body In this manner, the overhead on function call can be highly reduced. This explains why the energy consumption on AES is reduced, because even though the algorithm is compounded by just four functions, they a called at least 40 to 56 times, depending on the key used on encryption or decryption of data.

6 Conclusions and Future Works

In this work, firstly, we present the characteristics and functionalities of the SEMO (SEcurity MOdule). Secondly, we show its software implementation. And finally we present the simulation and analysis of this module, using the Sim-Panalyzer, where we concluded that our module had an average consumption of 2 joules and runtime of approximately 26 thousands cycles.

In addition, we have done a detailed analysis of the AES component, which is an algorithm people have given much attention to in the latest years. Several simulations were performed which had very satisfactory results, due to the fact that they could evidence the impact that key length caused on runtime and energy consumption of each component. Those results we obtained are now able to be used as a baseline for the implementation of security devices that demand less energy consumption.

As a future work, we plan to add more security components to the SEMO, as well as using it in a cellphone emulator. We also plan to develop a hardware implementation of the SEMO, and embedded it in a micro-controller and design an IP core in VHDL/Verilog and so that it can be used in several devices as notebooks, smartphones, ATMs and others.

References

[1] "The simplescalar-arm power modeling project,", June 2012. http://web.eecs.umich.edu/ panalyzer/.

[2] D. Burger and T. M. Austin, "The simplescalar tool set, version 2.0," *ACM SIGARCH Computer Architecture News*, vol. 25, pp. 13–25, June 1997.

[3] Trusted Computing Group, June 2012.

[4] E. D. Moreno, F. M. R. Junior, F. A. Lima, and W. R. A. Dias, "Computer architecture under energy consumption vision," *International Journal of Computer Architecture Education*, vol. 2, pp. 5–8, Dec. 2013.

[5] E. D. Moreno, F. D. Pereira, and R. B. Chiaramonte, *Criptografia em software e hardware*. Novatec: São Paulo, Brazil, 2005.

[6] F. D. Pereira, E. D. M. Ordonez, and R. B. Chiaramonte, "Vliw cryptoprocessor: Architecture and performance in FPGAs," *International Journal of Computer Science and Network Security*, vol. 6, pp. 151–160, Aug. 2006.

[7] D. Seal, *ARM architecture reference manual*. Addison-Wesley Professional, 2nd edition edition, 2001.

[8] J. S. Seng and D. M. Tullsen, "The effect of compiler optimizations on pentium 4 power consumption," in *Proceedings of the Seventh Workshop on Interaction between Compilers and Computer Architectures*, p. 51, Sep. 2003.

Felipe dos Anjos Lima received his B. S. in Computer Science from Universidade Federal de Sergipe (UFS) in 2013. His areas of research interest include embedded

systems, distributed computing and information security.

Edward David Moreno received the M.Sc. and Ph.D. degrees in Electrical Engineering from USP (University of So Paulo), SP, Brazil, in 1994 and 1998. During 1996 and 1997 he stayed as invited researcher at University of Toronto, Canada, and Chalmers University of Technology, Sweden. He is teacher at the UFS (Federal University of Sergipe), Aracaju, Sergipe, Brazil. Moreno has participated on 100 events as International Program Committee and he is editorial board of 4 important Journals: JUCS - Journal Universal on Computer Science, Springer Transactions on Computational Science and IJCSNS International Journal of Computer Science and Network Security and JCP - Journal of Computers. He has published five books about digital systems, FPGAs, Microcontrollers, Reconfigurable Computing and Hardware Security. The research areas are: computer architecture, reconfigurable computing, embedded systems, hardware security, power aware computing and performance evaluation.

Dellano Oliveira D. Santos received his B. S. in Computer Science from Universidade Federal de Sergipe (UFS) in 2013. His areas of research interest include embedded systems, distributed computing and information security.

Wanderson Roger Azevedo Dias received the B.S. in Computer Information Systems (2004), specialist in Software Development for Web (2007), M.Sc. and Ph.D. degrees in Computer Science by UFAM (Federal University of Amazonas), Manaus, Amazonas, Brazil, in 2009 and 2013. He is teacher at the IFS (Federal Institute of Sergipe), Aracaju, Sergipe, Brazil. The researches of teacher Roger are in the areas of: computer architecture, embedded systems, code compression, simulation architecture, hardware security, power aware computing, performance evaluation and FPGAs.

An Efficient and Distortion-controllable Information Hiding Algorithm for 3D Polygonal Models with Adaptation

Yuan-Yu Tsai, Wen-Ching Huang, and Bo-Feng Peng
(Corresponding author: Yuan-Yu Tsai)

Department of Applied Informatics and Multimedia, Asia University,
No. 500, Lioufeng Rd., Wufeng Dist., Taichung City 41354, Taiwan
(Email: yytsai@asia.edu.tw)

(Received Apr. 18, 2013; revised and accepted Oct. 6, 2013)

Abstract

We present an efficient information hiding algorithm for polygonal models. The decision to referencing neighbors for each embeddable vertex is based on a modified breadth first search, starting from the initial polygon determining by principal component analysis. The surface complexity is then estimated by the distance between the embedding vertex and the center of its referencing neighbors. Different amounts of secret messages are adaptively embedded according to the surface properties of each vertex. A constant threshold is employed to control the maximum embedding capacity for each vertex and decrease the model distortion simultaneously. The experimental results show the proposed algorithm is efficient and can provide higher robustness, higher embedding capacity, and lower model distortion than previous work, with acceptable estimation accuracy. The proposed technique is feasible in 3D adaptive information hiding.

Keywords: Adaptation, breadth first search, controllable distortion, information hiding, polygonal models

1 Introduction

3D information hiding algorithms [1, 5, 9] hide the secret message in a cover model to produce a stego model which is undetectable to all expect the legitimate receiver. According to different operation domains for the cover models, different embedding manners are used for data embedding. Generally, the algorithms in the spatial domain [6] are efficient and suitable for the covert communication; whereas the algorithms in the transform domains [10] are of higher robustness and appropriate for copyright protection.

Adaptive information hiding algorithms [2, 3, 8] embed different amounts of secret message into the embedding vertex according to its surface complexity. The main reason is that a vertex located on a rough surface can generally tolerate more positional changes than one on a smooth surface. Thus, the majority of the secret message is embedded into rougher regions to avoid causing visible model distortion on smoother regions.

However, only two information hiding algorithms consider adaptation for the purpose of covert communication. Cheng and Wang [3] proposed an adaptive algorithm utilizing the correlation between neighboring polygons to estimate the amount of message for the embedding vertex. The algorithm first employs a contagious diffusion scheme to efficiently traverse each mesh. Thereafter, an adaptive minimum-distortion estimation procedure is employed to embed the secret message into extending, sliding, and rotating levels of the embedding vertex. However, their proposed algorithm only uses two of the other vertices within the same polygon containing the embedding vertex. This may lead to inaccurate estimation results. To raise the estimation accuracy for surface complexity, Tsai [8] introduced a vertex decimation process to determine the referencing neighbors for each embedding vertex. A quantization index modulation concept is then employed to embed different amounts of secret message into each embedding vertex according its surface complexity. Although the estimation accuracy can be significantly raised from 34.11% to 65.51%, on average, the time complexity for the vertex decimation process is higher and the performance of the algorithm is seriously affected.

In this study, a modified breadth first search (BFS) scheme is developed to improve the performance of determining the referencing neighbors for each embedding vertex. The proposed algorithm can efficiently resolve the referencing neighbors but slightly decrease the estimation accuracy. The proposed algorithm introduces a constant threshold *CT* to control the maximum embedding capacity of each vertex and to lower model distortion. Finally, the proposed algorithm can be robust against similarity transformation and vertex reordering attacks.

This rest of this study is organized as follows; Section 2 illustrates the proposed scheme; Section 3 presents a discussion of the experimental results; and finally, Section 4 offers a conclusion of this work.

2 The Proposed Algorithm

This section illustrates the proposed algorithm, including the data embedding and data extraction procedure. The flowchart of the proposed algorithm is shown in Figure 1.

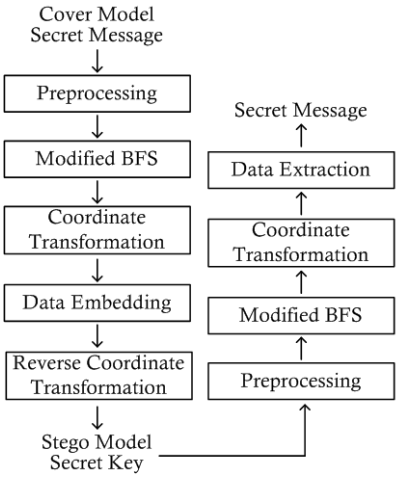


Figure 1: The flowchart of the proposed algorithm

2.1 The Data Embedding Procedure

The data embedding procedure begins by preprocessing the topological information of the input model. To efficiently derive the referencing neighbors for each embedding vertex in the modified BFS process, a vertex neighboring table records the indices of the actual neighbors based on the polygonal information appearing in the model file. Furthermore, the model information, including the diagonal length of the bounding volume, the number of vertices, and the number of faces, can be also derived in this process.

The breadth first search is a search method that begins from the root node of a graph and explores all its neighboring nodes. For each neighboring node, the algorithm explores unexplored neighboring nodes iteratively. The algorithm stops after all nodes have been traversed. All neighboring nodes derived by expanding a node are added to a queue with a first-in-first-out (FIFO) property. However, the breadth first search may not only have a unique search result for a graph. The search results depend on how the user chooses the neighboring nodes of each node. In the proposed technique, the search order is based on the sequence appearing in the vertex neighboring table for each corresponding vertex. This vertex neighboring table is robust against similarity transformation and vertex ordering attacks. Thus, the same search order can be derived in the data extraction procedure.

The modified BFS process determines the referencing neighbors for complexity estimation and data embedding. Each vertex can have three different statuses "NS," "SS," and "S," representing the corresponding vertex as being unsearched, semi-searched, and searched. Each vertex is initialized as "NS." The initial vertex for performing this process is resolved by the first index of the polygon intersected by the principal axis and regarded as the root node for performing the BFS algorithm. In the first iteration, the process enqueues the initial vertex, dequeues it, and then enqueues its unsearched neighbors. Note that, the order of the enqueued neighbors is not arbitrary, but based on the sequence appearing in the vertex neighboring table for each corresponding vertex. When the vertex is enqueued, its status is modified to "SS," whereas the status is modified to "S" when the corresponding vertex is dequeued. In the second iteration, the process dequeues one vertex from the queue and euqueues its unsearched neighbors. The order of the enqueued neighbors is still based on the sequence appearing in the vertex neighboring table. This iteration is repeated until the queue is empty. The algorithm then proceeds until all vertices are searched. In each iteration, the neighbors with the status "NS" or "SS" are included in the referencing list for each dequeued vertex.

To be robust against similarity transformation attacks, the coordinate transformation process collects the vertex whose referencing list is empty. Thereafter, principal component analysis [7] is performed again on these vertices to produce a coordinate system. All vertices of the 3D cover model are then transformed from the Cartesian coordinate system to the new one. Because the coordinate values of these vertices are never modified, the constructed coordinate system can be used for model registration under rotation and translation attacks. This process also derives the diagonal length *DL* of the bounding volume of the vertex whose referencing list is empty. This diagonal length is the key point making the proposed algorithm robust against scaling attacks.

For each embeddable vertex, the data embedding process acquires the referencing neighbors from the referencing list. Next, the embedding capacity is proportional to the distance *d* between the embedding vertex and the center of its referencing neighbors [8]. The quantization index modulation concept is then employed for data embedding with the embedding threshold *ET*. To control the maximum embedding capacity for each vertex and lower model distortion, a constant threshold σ_{EC} is introduced in Equation (1). Thus, the maximum distortion for each embedding capacity can be reduced from $2^{EC_1} \times ET$ to $2^{\sigma_{EC}} \times ET$. Equation (2) shows the derivation for the data-embedded distance *d'*. When the calculated embedding capacity EC_1 is smaller than σ_{EC}, secret message SM_2 with length EC_1 is extracted from the stream of secret message with binary form and SM_{10} is the decimal value from a binary-to-decimal format transformation of SM_2. Figure 2 shows a graphical representation of this type of data embedding. However, for a calculated embedding capacity EC_1 larger than σ_{EC}, the final embedding capacity is limited to $EC_2 = \sigma_{EC}$ (see Equation (2)). Figure 3 is a graphical representation of the data embedding process with limited embedding capacity. To lower model distortion, we first calculate the proper embedding interval

Table 1: The model information, the embedding capacity, and the model distortion for our proposed algorithn

Model Name	N_V	N_F	DL_{BV}	DL_{V^N}	N_{V^N}	Capacity	BitsPV	BitsPEV	NHD
Armadillo	172974	345944	228.80	226.51	440	2784917	16.10	16.14	0.1142%
Brain	294012	588032	10.03	9.84	572	3494908	11.89	11.91	0.1789%
Cow	46433	92864	30.49	29.04	49	644982	13.89	13.91	0.1075%
Golfball	122882	245760	1.73	1.73	1219	1181227	9.61	9.71	0.0543%
Lucy	262909	525814	1918.29	1913.97	4050	4858167	18.48	18.77	0.1608%
Maxplanck	49132	98260	697.49	624.28	55	922368	18.77	18.79	0.1490%
Dragon	437645	871414	26.69	26.62	10422	5321934	12.16	12.46	0.1260%
Hand	327323	654666	8.41	8.28	1555	3501159	10.70	10.75	0.0789%

m based on the σ_{EC} and SM_{10} is finally embedded into the distance between the embedding vertex and the center of its referencing neighbors. Obviously, SM_{10} is a decimal value from a binary-to-decimal format transformation of SM_2 with length σ_{EC}.

$$EC = \begin{cases} EC_1 = \log_2\left(d/ET\right) \\ EC_2 = \min\left(\left\lfloor \log_2\left(d/ET\right)\right\rfloor, \sigma_{EC}\right) \end{cases} \quad (1)$$

$$d' = \begin{cases} \left(2^{EC_1} + \mathrm{SM}_{10}\right) \times ET \\ \left(\left\lfloor \left(d/ET - 2^{EC_1}\right) / 2^{\sigma_{EC}} \right\rfloor \times 2^{\sigma_{EC}} + 2^{EC_1} + \mathrm{SM}_{10}\right) \times ET \end{cases} \quad (2)$$

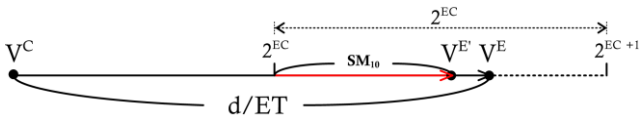


Figure 2: A graphical representation of the data embedding

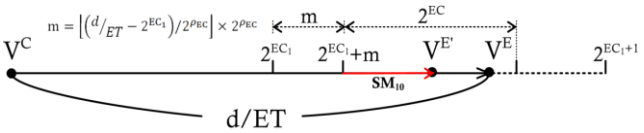


Figure 3: A graphical representation of the data embedding

After the data-embedding process is complete, the algorithm transforms all the vertices from the PCA coordinate system back to the Cartesian system. This produces a stego model that is then delivered to the receiver. To ensure robustness against scaling attacks, a secret key is then calculated by dividing the embedding threshold ET by the diagonal length DL of the bounding volume of the vertices with no referencing neighbors.

2.2 The Data Extraction Procedure

During the data extraction procedure, the following processes are performed sequentially. First, the preprocessing process deals with the topological information of the input model. A vertex neighboring table is then constructed. As mentioned before, the construction of this table is based on the topological property of each vertex. However, the topological information is never modified in the data embedding procedure. Therefore, this table can be correctly reconstructed according to the same processes in the data embedding procedure. Second, the modified BFS process iteratively determines the referencing neighbors for each embedding vertex of the stego model. Third, we collect all the vertices whose referencing list is an empty set. Thereafter, a principal component analysis is performed on the above vertices to produce a coordinate system and transform all vertices of the stego model from the Cartesian coordinate system to the new one. Fourth, the embedding threshold can be also derived in this process based on the secret key and the diagonal length DL of the bounding volume of the vertices with no referencing neighbors. Finally, the data-embedded distance d' can be calculated. The secret message with a binary format can be easily derived based on the embedding capacity and decimal-to-binary format transformation of SM_{10} derived from Equation (3).

$$SM_{10} = \begin{cases} \left\lfloor d'/ET \right\rfloor - 2^{EC_1} \\ \left\lfloor d'/ET \right\rfloor - 2^{EC_1} - \left\lfloor \left(d'/ET - 2^{EC_1}\right) / 2^{\sigma_{EC}} \right\rfloor \times 2^{\sigma_{EC}} \end{cases} \quad (3)$$

3 Experimental Results

This section presents the experimental results obtained from eight 3D common polygonal models: “Armadillo,” “Brain,” “Cow,” “Golfball,” “Lucy,” “Maxplanck,” “Dragon,” and “Hand.” The proposed algorithm was implemented in Microsoft Visual C++ programming language on a personal computer with an Intel Core i7 2.67 GHz processor and 3 GB of memory. Table 1 shows the model information, including the number of vertices N_V, the number of faces N_F, and model size (represented by the diagonal length DL_{BV} of the bounding volume) of each model. Figure 4 shows the visual effect of each cover polygonal model. The embedded secret message is a 0/1 bit string randomly generated. The distortion between the cover model and the stego model was measured using normalized Hausdorff distance (NHD) [4], which is derived from dividing the Hausdorff distance by DL_{BV}. The number precision of the cover model and the stego model

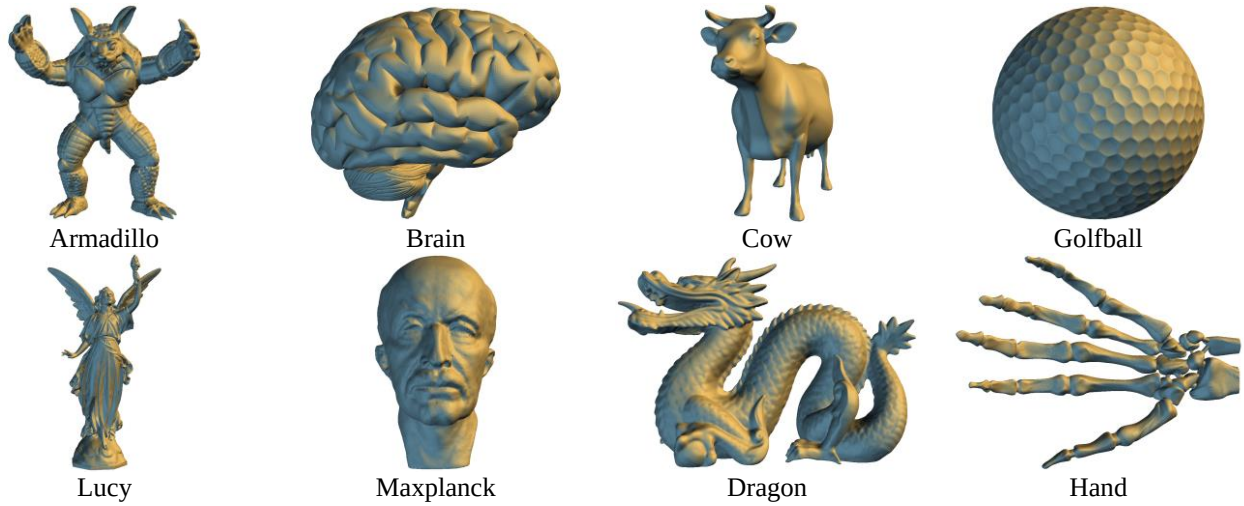


Figure 4: The visual effects of the cover models

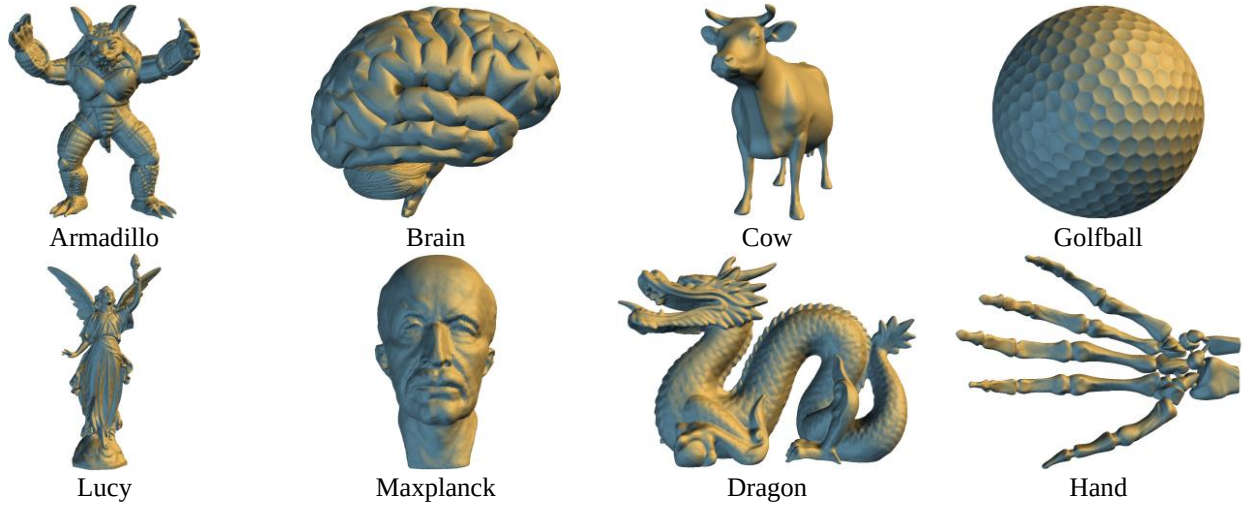


Figure 5: The visual effects of the stego model with an embedded secret message

are both precise to six decimal places. The experimental results show there is no error in the extracted secret message under the similarity transformation and vertex reordering attacks.

This section first presents the experimental results of the proposed algorithm, including its embedding capacity and the visual distortion of the different input models. Second, this section also presents the embedding capacity and model distortion of the Armadillo and Lucy models under different constant thresholds. Finally, this section compares the proposed algorithm with existing adaptive information hiding algorithms to demonstrate the feasibility of the proposed method.

Table 1 shows the results of the embedding capacity and the model distortion under the given embedding threshold $ET = 3\times10^{-6}$. For the maximum embedding capacity, no restriction is performed on the parameter σ_{EC}. The embedding capacity can achieve 9.61 to 18.77 bits per vertex and 9.71 to 18.79 bits per effective vertex, which is the vertex with the embedded secret message. The difference between the value of BitsPV and BitsPEV is small because only 0.1 to 2.4 percent of the total number of vertices cannot have the secret message embedded. The model distortion is acceptable, ranging only from 0.05% to 0.18% of the value DL_{BV} . Figure 5 shows the shading effects with insignificant distortion of the stego models.

This section presents the embedding capacity and model distortion of the Armadillo and Lucy models under different constant thresholds (Table 2). Other test models have similar results. When the constant threshold is smaller, indicating each vertex can only convey a reduced amount of secret message, the total embedding capacity is apparently lower and the model distortion is less. With an increasing constant threshold, both the embedding capacity and the model distortion are increased. From Table 2, our proposed algorithm is superior to previous algorithms with higher embedding capacity and lower model distortion for

the Armadillo model and the Lucy model under the threshold value 15 and 17 separately.

Table 2: The capacity and distortion comparison under different embedding thresholds

Model \ *CT*		5	10	15	17	∞	[8]
Armadillo	Capacity	862670	1725331	2581163	2784917	2784917	2220480
	NHD	0.0001%	0.0024%	0.0666%	0.1406%	0.1142%	0.0963%
Lucy	Capacity	1294295	2588590	3882815	4395901	4858167	4101995
	NHD	0.0000%	0.0003%	0.0091%	0.0337%	0.1608%	0.0555%

Table 3: A comparison of the adaptive methods of [3], [8], and the current method

Algorithm	[3]	[8]	Current Method
Capacity	3.00~6.00 bpv	7.76~18.00 bpv	9.71~18.79 bpv
Robustness	Similarity Transformation	Similarity Transformation	Similarity Transformation Vertex Reordering
Complexity	$O(N_F)$	$O(N_V^2)$	$O(N_E)$
Referencing Ratio	34.11%	64.51%	49.67%

Finally, this section compares the proposed algorithm with existing adaptive information hiding algorithms to demonstrate the feasibility of the proposed method. Table 3 shows that the proposed technique can convey the maximum embedding capacity within the current adaptive algorithms. The robustness is also superior to other two algorithms because of the vertex reordering attack. For the complexity comparison, Cheng and Wang's algorithm employs a new contagious diffusion technique with the time complexity $O(N_F)$ to generate a traversal path for each polygon; whereas our previous work introduces a vertex decimation process with the time complexity $O(N_V^2)$ for determining the referencing neighbors for each embedding vertex. The proposed algorithm adopts a modified breadth first search scheme that explores all edges of the polygonal model to determine the referencing neighbors. Thus, the complexity is only $O(N_E)$, whether N_E is the number of edges in the cover model. However, the proposed technique lowers the number of the referencing neighbors for each embedding vertex at approximately half of the actual neighbors. Despite this, the referencing ratio is still superior to that of Cheng and Wang's algorithm.

4 Conclusions

This study proposes an adaptive information hiding algorithm for polygonal models. The main point of this algorithm is to use a modified BFS method to efficiently derive the referencing neighbors for each embeddable vertex. Thereafter, the surface complexity of the embedding vertex is then estimated by the distance from the center of the referencing neighbors. Different amounts of secret messages are embedded according to the surface properties of each vertex. To decrease the model distortion caused by a large embedding capacity, a constant threshold is employed to control the maximum embedding capacity for each vertex. The proposed algorithm can provide a higher embedding capacity, higher robustness, and a lower model distortion under acceptable estimation accuracy. Most importantly, the performance for determining the referencing neighbors of each embeddable vertex can be significantly improved. With the help of experimental results, this study demonstrates the feasibility of this technique for 3D adaptive information hiding.

Acknowledgments

We thank Dr. Timothy Williams for his assistance in improving the clarity of this article. The authors also thank the anonymous reviewers for their constructive comments. This work was supported by the National Science Council under the grant numbers NSC 101-2221-E-468-026 and NSC 102-2221-E-468-025.

References

[1] M. W. Chao, C. H. Lin, C. W. Yu, and T. Y. Lee, "A high capacity 3D steganography algorithm," *IEEE Transactions on Visualization and Computer Graphics*, vol. 15, pp. 274-284, 2009.

[2] T. Y. Chen, M. S. Hwang, and J. K. Jan, "Adaptive authentication schemes for 3D mesh models," *International Journal of Innovative Computing, Information and Control*, vol. 5, pp. 4561-4572, 2009.

[3] Y. M. Cheng and C. M. Wang, "An adaptive steganographic algorithm for 3D polygonal meshes," *The Visual Computer*, vol. 23, pp. 721-732, 2007.

[4] P. Cignoni, C. Rocchini, and R. Scopigno, "Metro: measuring error on simplified surfaces," *Computer Graphics Forum*, vol. 17, pp. 167-174, 1998.

[5] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*, Second Edition, Morgan Kaufmann, Burlington, 2008.

[6] L. C. Huang, L. Y. Tseng, and M. S. Hwang, "The study of data hiding in medical images," *IJNS* 14, pp. 301-309, Springer-Verlag, 2012.

[7] A. C. Rencher, *Methods of Multivariate Analysis*, Second Edition, Wiley, New York, 2002.

[8] Y. Y. Tsai, "An adaptive steganographic algorithm for 3D polygonal models using vertex decimation," *Multimedia Tools and Applications*, in press, DOI: 10.1007/s11042-012-1135-8.

[9] C. M. Wang and Y. M. Cheng, "An efficient information hiding algorithm for polygon models," *Computer Graphics Forum*, vol. 24, pp. 591-600, 2005.

[10] K. Wang, G. Lavoué, F. Denis, and A. Baskurt, "A comprehensive survey on three-dimensional mesh watermarking," *IEEE Transactions on Multimedia*, vol. 10, pp. 1513-1527, 2008.

Yuan-Yu Tsai received a B.S. degree in Department of Computer Science and Information Engineering from National Central University, Taiwan, in 2000, and his Ph.D. degree from the Institute of Computer Science at National Chung Hsing University, Taiwan, in 2006. He is currently an assistant professor at the Department of Applied Informatics and Multimedia, Asia University, Taichung, Taiwan. His research interests include computer graphics and information hiding algorithms for three-dimensional models and images. He is a member of the ACM and the IEEE Computer Society.

Wen-Ching Huang is a third-year student at the Department of Applied Informatics and Multimedia, Asia University, Taichung, Taiwan. Her research interests include information hiding algorithms for three-dimensional models and images.

Bo-Feng Peng is currently a Master's student. He received his B.S. degree in Applied Informatics and Multimedia from Asia University, Taiwan, in 2012. His research interests include information hiding algorithms for three-dimensional models and images.

Unequal Protection Mechanism for Digital Speech Transimission Based on Turbo Codes

Boqing Xu[1], Qun Xiao[1], Zhenxing Qian[2], and Chuan Qin[1]
(Corresponding author: Chuan Qin)

School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology[1]
No. 516 Jungong Rd., Shanghai 200093, China
School of Communication and Information Engineering, Shanghai University[2]
No. 149 Yanchang Rd., Shanghai 200072, China
(Email: qin@usst.edu.cn)

(Received Aug. 6, 2013; revised and accepted Oct. 16, 2013)

Abstract

In this paper, the Turbo-based unequal protection mechanism for reliable transmission of speech signal is studied. In order to obtain the hierarchical importance regularity of information bits for each sampling point, the changing value caused by the variation of each bit in 8-bit folded code of pulse-code modulation is first calculated. According to the obtained hierarchical importance of information bits, two unequal error protection (UEP) schemes of 3-level and 8-level are proposed based on Turbo codes. In order to achieve the satisfactory error protection capability for the global speech signal, the non-uniform puncturing is utilized in these two schemes, which can adaptively assign more parity bits for error protection to more important information bits. Compared with the traditional equal error protection (EEP) scheme, our schemes not only have greater coding rate, but also have generally better quality of the decoded speech signal on the receiver side, especially in poor channel condition. Experimental results demonstrate the effectiveness of the proposed schemes.

Keywords: Hierarchical importance, speech transmission, turbo codes, unequal protection

1 Introduction

Digital signal is usually interfered during the transmission in wireless channel, which may lead to the degradation of signal quality after decoding on the receiver side [13]. Thus, in order to decrease the error probability of information transmission, a large number of error-correcting codes (ECC), such as BCH code and Turbo code, have been proposed and used as the channel coding. Channel coding is one of the key techniques in digital communication. As a kind of channel coding, Turbo codes can be used to improve the communication quality effectively. Turbo codes provide a concatenated coding scheme and a sub-optimal iterative decoding method, which achieve excellent performances under the condition of the low channel SNR. There are many design components of Turbo codes including different encoders, input/output ratios, interleavers, and puncturing patterns. Recently, Turbo codes have been widely applied in various communication systems, such as mobile communication [11], digital video broadcasting (DVB), terrestrial wireless communication over long distances, and satellite communications (SATCOM). However, the traditional ECC can only provide the equal error protection (EEP) for each information bit. In other words, the numbers of the allocated parity bits for all information bits are the same. Actually, after the quantization and encoding for digital signals, different information bits may have different degrees of importance, and the allocation manner of parity bits for EEP may not have the global optimal performance of error protection. Therefore, the unequal error protection (UEP) for digital signals using ECC has been widely studied in recent years [3, 4, 5].

Many researchers have designed the UEP schemes using the different codes and techniques. Convolutional codes were utilized for UEP according to an algebraic theoretical viewpoint in [9]. UEP extensions of low density parity check accumulate (UEP-LDPCA) codes were discussed and several potential applications were also given in [7]. Due to the excellent performance of Turbo codes [2], there are many reported UEP schemes that were designed based on Turbo codes. Zhang *et al.* investigated the impact of different puncturing patterns on the resulting UEP properties through examining the bit error rate (BER) at various positions of a Turbo coded data block [15], and then they applied the UEP properties of Turbo codes in the transmission of JPEG2000 images. Thomos *et al.* proposed an image transmission scheme using Turbo codes for the SPIHT image streams over wireless channels [8], in which an algorithm for the optimal UEP of the compressed bit stream was also presented. An UEP method for the streaming media was proposed in [12]. In this method, besides a hierarchical coding graph, the low-complexity encoding and decoding operations were included, and the

decoding probability and priority were also characterized to show the advantages of the UEP rateless codes. Morcos and Elshabrawy proposed a four-level UEP scheme for H.264 scalable video coding using discrete wavelet transform (DWT) [6], in which I-frames were provided with higher priority than P-frames. An UEP scheme based on the hierarchical quadrature amplitude modulation for the three-dimensional video transmission was presented by Alajel *et al.* [1]. In this scheme, the color sequence was assigned with more protection bits than the depth map in order to achieve the high quality of 3D video.

However, most of the reported UEP schemes were used for the transmission of digital images or videos. Speech signal is also a commonly used type of digital signals transmitted in different kinds of channel. Since the characteristics of speech signal are quite different with the signals of image and video, the corresponding coding method of speech signal is different with those of other kinds of signals. Thus, the UEP schemes in [1, 6, 8, 12] that are used for other types of signals, i.e., images and videos, can not be directly applied on the transmission protection of digital speech signal. The representative lossless coding for speech signal is the PCM coding. In computer applications, PCM coding is a commonly used method to achieve the top level of fidelity, which is widely used in audio digitization and music appreciation for CD, DVD, and audio files. On the other hand, in order to save storage space, the loss coding, such as MP3, focuses on achieving the satisfactory compression performance and the acceptable audible quality simultaneously. Although some research works were conducted on the UEP methods for the compressed speech signal [14], in this paper, we mainly focus on the error protection for uncompressed speech signals with PCM coding. Also, to the best of our knowledge, the currently reported UEP schemes are not suitable to the protection for the transmission of digital speech signal encoded by the PCM method. In this work, we propose two novel UEP schemes with three and eight protection levels for the digital speech transmission over the additive white Gaussian noise [10] (AWGN) channel. We first analyze the hierarchical importance degrees of information bits for digital speech signal after the pulse-code modulation (PCM). Then, according to the obtained rule of hierarchical importance, a new puncturing mechanism using Turbo codes is presented to achieve the capability of unequal protection for digital speech signal.

The rest of this paper is organized as follows. In Section 2, the analysis of hierarchical importance degrees of information bits after PCM speech coding is given. In Section 3, two UEP puncturing schemes based on Turbo codes are proposed. Experimental results and comparisons are presented in Section 4. Finally, conclusions are drawn in Section 5.

2 Hierarchical Importance Analysis

According to the PCM coding rule, each sampling value x of the input digital speech sequence is transformed into 8-bit folded binary code, i.e., $\{b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8\}$. $\{b_1\}$ is the sign bit. The three bits $\{b_2, b_3, b_4\}$ are called the paragraph code, which represent eight kinds of slopes for the encoded paragraphs. The decimal value of the paragraph code varies from $2^{4b_2+2b_3+b_4+3}$ to $2^{4b_2+2b_3+b_4+4}$. Here, the paragraph code $\{0, 0, 0\}$ is an exception. The four bits $\{b_5, b_6, b_7, b_8\}$ are called the segment code, which represent 16 kinds of quantization levels for each encoded paragraph. Note that the sampling value x can be calculated by using its corresponding 8-bit folded binary code, i.e., $\{b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8\}$, see Equation (1).

$$x = (2b_1 - 1) \times \left[2^{\sum_{i=2}^{4} 2^{4-i} b_i + 3} + \frac{2^{\sum_{i=2}^{4} 2^{4-i} b_i + 4} - 2^{\sum_{i=2}^{4} 2^{4-i} b_i + 3}}{2^4} \times \sum_{i=5}^{8} 2^{8-i} b_i \right]. \quad (1)$$

For simplicity of the following description, we denote $2^{\sum_{i=2}^{4} 2^{4-i} b_i}$ and $\sum_{i=5}^{8} 2^{8-i} b_i$ as A and B, respectively. Clearly, A is determined by $\{b_2, b_3, b_4\}$ and B is determined by $\{b_5, b_6, b_7, b_8\}$. Thus, the sampling value x can also be represented as: $x = 8A + \frac{AB}{2}$.

During the transmission of the input speech sequence in the AWGN channel, b_i (i =1, 2, …, 8) of each sampling value x may occur errors caused by the channel noises. Therefore, before we present the UEP scheme for digital speech signal, the hierarchical importance analysis for b_i (i = 1, 2, …, 8) should be first conducted.

2.1 Analysis of the sign bit b_1

If errors occur in the sign bit b_1, the polarity of the sampling value x is inverted, and the original sampling value x is changed to $x_1 = -x = -(8A + \frac{AB}{2})$. Thus, due to the error in the sign bit b_1, the change to the sampling value x is:

$$\Delta x_1 = |x - x_1| = \left| (8A + \frac{AB}{2}) - (-8A - \frac{AB}{2}) \right| = 16A + AB. \quad (2)$$

2.2 Analysis of paragraph code $\{b_2, b_3, b_4\}$

If errors occur in b_2, the original b_2 is changed to $1 - b_2$. Thus, due to the error in b_2, the original sampling value x is changed to:

$$x_2 = 2^{2^2(1-b_2)+\sum_{i=3}^{4} 2^{4-i} b_i + 3} + \left[\frac{2^{2^2(1-b_2)+\sum_{i=3}^{4} 2^{4-i} b_i + 4} - 2^{2^2(1-b_2)+\sum_{i=3}^{4} 2^{4-i} b_i + 3}}{2^4} \times \sum_{i=5}^{8} 2^{8-i} b_i \right] \quad (3)$$

$$= 8A \times 2^{4-8b_2} + \frac{2^{4-8b_2} \times AB}{2}.$$

Similarly, when errors occur in b_3 and b_4, the original sampling value x is changed to $x_3 = 8A \times 2^{2-4b_3} + \frac{2^{2-4b_3} \times AB}{2}$ and $x_4 = 8A \times 2^{1-2b_4} + \frac{2^{1-2b_4} \times AB}{2}$, respectively.

When errors occur in b_2, b_3, and b_4 separately, the changes brought to the original sampling value x can be written as Δx_2, Δx_3, and Δx_4, see Equations (4-6).

$$\Delta x_2 = |x - x_2| = \left|(8A + \frac{AB}{2}) - (8A \times 2^{4-8b_2} + \frac{2^{4-8b_2} \times AB}{2})\right| \quad (4)$$
$$= (2^{7-8b_2} - 8)A + (2^{3-8b_2} - \frac{1}{2})AB.$$

$$\Delta x_3 = |x - x_3| = \left|(8A + \frac{AB}{2}) - (8A \times 2^{2-4b_3} + \frac{2^{2-4b_3} \times AB}{2})\right| \quad (5)$$
$$= (2^{5-4b_3} - 8)A + (2^{1-4b_3} - \frac{1}{2})AB.$$

$$\Delta x_4 = |x - x_4| = \left|(8A + \frac{AB}{2}) - (8A \times 2^{1-2b_4} + \frac{2^{1-4b_4} \times AB}{2})\right| \quad (6)$$
$$= (2^{4-2b_4} - 8)A + (2^{-2b_4} - \frac{1}{2})AB.$$

Based on all possible cases of $\{b_2, b_3, b_4\}$, we can calculate the corresponding absolute differences, i.e., Δx_1, Δx_2, Δx_3, Δx_4, between the original sampling value x and the values after changing, i.e., x_1, x_2, x_3, x_4, according to Equations (2-6). It can be observed from Table 1 that, when $\{b_2, b_3, b_4\}$ belongs to {0, 0, 0}, {0, 0, 1}, {0, 1, 0}, or {0, 1, 1}, Δx_2 is greater than Δx_1, Δx_3, and Δx_4. Similarly, when $\{b_2, b_3, b_4\}$ belongs to {1, 0, 0} or {1, 0, 1}, Δx_3 become larger; and when $\{b_2, b_3, b_4\}$ belongs to {1, 1, 0} or {1, 1, 1}, Δx_1 become larger.

Table 1: Results of hierarchical importance analysis for $\{b_1, b_2, b_3, b_4\}$

$\{b_2, b_3, b_4\}$	A	Δx_1	Δx_2	Δx_3	Δx_4	*Relationship*
{0, 0, 0}	1	2B	128+7B	32+B	16	$\Delta x_2 > \Delta x_3 > \Delta x_1 > \Delta x_4$
{0, 0, 1}	2	32+2B	240+15B	48+3B	16	$\Delta x_2 > \Delta x_3 > \Delta x_1 > \Delta x_4$
{0, 1, 0}	4	64+4B	480+30B	32+B	32+2B	$\Delta x_2 > \Delta x_1 > \Delta x_4 > \Delta x_3$
{0, 1, 1}	8	128+8B	960+60B	48+3B	32+2B	$\Delta x_2 > \Delta x_1 > \Delta x_3 > \Delta x_4$
{1, 0, 0}	16	256+16B	128+7B	384+24B	128+8B	$\Delta x_3 > \Delta x_1 > \Delta x_4 > \Delta x_2$
{1, 0, 1}	32	512+32B	240+15B	768+48B	128+8B	$\Delta x_3 > \Delta x_1 > \Delta x_2 > \Delta x_4$
{1, 1, 0}	64	1024+64B	480+30B	384+24B	512+32B	$\Delta x_1 > \Delta x_4 > \Delta x_2 > \Delta x_3$
{1, 1, 1}	128	2048+128B	960+60B	768+48B	512+32B	$\Delta x_1 > \Delta x_2 > \Delta x_3 > \Delta x_4$

In general, the statistical distribution of amplitude for the long-term speech signal (more than dozens of seconds) is close to Gamma distribution, while the statistical distribution of amplitude for the short-term speech signal (several to dozens of milliseconds) is close to Gaussian distribution. Whether the duration of the speech signal is long or short, the occurrence probability of the small amplitude is greater than that of the large one, see Figure 1. In other words, the probability for $\{b_2, b_3, b_4\}$ belonging to {0, 0, 0}, {0, 0, 1}, {0, 1, 0}, and {0, 1, 1} is greater than that belonging to {1, 0, 0}, {1, 0, 1}, {1, 1, 0}, and {1, 1, 1}. Therefore, from a statistical point of view, we can conclude that the regularity of the hierarchical importance for $\{b_1, b_2, b_3, b_4\}$ is: $I(b_2) > I(b_1) > I(b_3) > I(b_4)$, where $I(\cdot)$ denotes the function of importance degree.

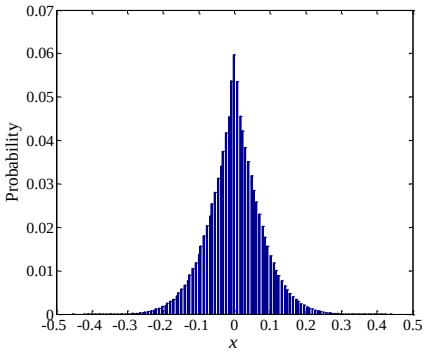


Figure 1: The statistical distribution of amplitude for one digital speech signal

2.3 Analysis of segment code $\{b_5, b_6, b_7, b_8\}$

In order to analyze the importance degree of $\{b_5, b_6, b_7, b_8\}$, the sampling value x in Equation (1) can be represented in the form of Equation (7).

$$x = (8 + \sum_{i=5}^{8} 2^{7-i} b_i)A. \quad (7)$$

If errors occur in b_5, $(1 - b_5)$ is just the changed value of b_5. Consequently, the changed sampling value due to the variation of b_5 is:

$$x_5 = \left[4(1-b_5) + \sum_{i=6}^{8} 2^{7-i} b_i + 8\right]A = (-4b_5 + \sum_{i=6}^{8} 2^{7-i} b_i + 12)A. \quad (8)$$

In the same way, when errors occur in b_6, b_7, and b_8, the changed sampling values x_6, x_7, and x_8 can be calculated using Equations (9-11), respectively.

$$x_6 = (-2b_6 + \sum_{i=5,7,8} 2^{7-i} b_i + 10)A. \quad (9)$$

$$x_7 = (-b_7 + \sum_{i=5,6,8} 2^{7-i} b_i + 9)A. \quad (10)$$

$$x_8 = (-\frac{1}{2} b_8 + \sum_{i=5}^{7} 2^{7-i} b_i + \frac{17}{2})A. \quad (11)$$

When the channel errors occur in b_5, b_6, b_7, and b_8 separately, the corresponding absolute differences, i.e., Δx_5,

Δx_6, Δx_6, Δx_8, between the original sampling value x and the values after changing, i.e., x_5, x_6, x_7, x_8, can be calculated according to Equations (12-15).

$$\Delta x_5 = |x - x_5| = \left|(8 + \sum_{i=5}^{8} 2^{7-i} b_i)A - (-4b_5 + \sum_{i=6}^{8} 2^{7-i} b_i + 12)A\right| = |8b_5 - 4|A. \quad (12)$$

$$\Delta x_6 = |x - x_6| = \left|(8 + \sum_{i=5}^{8} 2^{7-i} b_i)A - (-2b_6 + \sum_{i=5,7,8} 2^{7-i} b_i + 10)A\right| = |4b_6 - 2|A. \quad (13)$$

$$\Delta x_7 = |x - x_7| = \left|(8 + \sum_{i=5}^{8} 2^{7-i} b_i)A - (-b_7 + \sum_{i=5,6,8} 2^{7-i} b_i + 9)A\right| = |2b_7 - 1|A. \quad (14)$$

$$\Delta x_8 = |x - x_8| = \left|(8 + \sum_{i=5}^{8} 2^{7-i} b_i)A - (-\frac{1}{2} b_8 + \sum_{i=5}^{7} 2^{7-i} b_i + \frac{17}{2})A\right| = \left|b_8 - \frac{1}{2}\right|A. \quad (15)$$

Since the binary bits b_5, b_6, b_7, b_8 are either 0 or 1, thus, Δx_5, Δx_6, Δx_7, and Δx_8 in Equations (12-15) can be written as: $\Delta x_5 = 4A$, $\Delta x_6 = 2A$, $\Delta x_7 = A$, $\Delta x_8 = 1/2A$. It can be clearly found that, when errors occur in $\{b_5, b_6, b_7, b_8\}$ separately, the absolute differences between the original sampling value and the corresponding values after changing show a decreasing trend. In other words, the regularity of the hierarchical importance for $\{b_5, b_6, b_7, b_8\}$ is: $I(b_5) > I(b_6) > I(b_7) > I(b_8)$.

Because Δx_5 is equal to $4A$, we can observe from Table 1 that, Δx_4 is always greater than Δx_5 with all possible values of A. Therefore, based on the above analysis, for the 8-bit folded binary code $\{b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8\}$ of each sampling point x in the speech signal, the two bits b_2 and b_1 have the first and the second highest importance degree, and the whole regularity of the hierarchical importance is: $I(b_2) > I(b_1) > I(b_3) > I(b_4) > I(b_5) > I(b_6) > I(b_7) > I(b_8)$.

3 Proposed UEP Schemes Using Turbo Codes

Based on the results of hierarchical importance analysis in Section 2, a novel unequal protection mechanism for digital speech signal using Turbo codes is presented. The framework diagram of the Turbo-based unequal protection mechanism is illustrated in Figure 2.

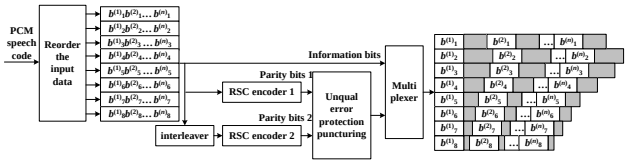


Figure 2: The framework diagram of the Turbo-based unequal protection mechanism

Suppose that the digital speech signal **X** for protection is $x^{(1)}, x^{(2)}, \ldots, x^{(n)}$, where n denotes the length of the signal, i.e., the number of sampling points. During the PCM coding, each sampling point $x^{(i)}$ of **X** is encoded to a string of 8-bit folded binary code, i.e., $b^{(i)}_1, b^{(i)}_2, \ldots, b^{(i)}_8$, $i = 1, 2, \ldots, n$. Thus, the total number of the concentrated binary bits after PCM coding for the speech signal **X** is $8n$. Before conducting the unequal protection by Turbo codes, we first divide the total $8n$-bit binary sequence of **X** into eight groups, and the j^{th} group $\mathbf{G}_j$ consists of the n elements: $\{b^{(1)}_j, b^{(2)}_j, \ldots, b^{(n)}_j\}$, $j = 1, 2, \ldots, 8$. Then, we concentrate the $8n$ bits in these eight groups sequentially and feed them into the Turbo encoder. In the procedure of Turbo encoding, one copy of the $8n$ bits is inputted into the first recursive systemic convolutional (RSC) encoder, and the output is treated as the first group of $8n$ parity bits. The second copy of the $8n$ bits is first messed up by the interleaver and then inputted into the second RSC encoder, and the output is treated as the second group of $8n$ parity bits. The two groups of parity bits outputted from RSC encoders are utilized to provide the error protection for the information bits. Different with traditional Turbo codes of EEP, in order to achieve the UEP capability, we adopt the non-uniform puncturing for the two groups of parity bits. The punctured parity bits are sent to the multiplexer together with the $8n$ information bits, and the output of the multiplexer is the final encoded bits with the unequal protection, which can be transmitted in the channel. The shaded parts in Figure 2 represent the assigned parity bits for the information bits after puncturing. The longer the shaded parts are, the higher protection level they provide. Because the hierarchical importance degrees of information bits are considered, the global error protection performance of UEP is better than that of EEP under the same coding rate.

Note that the puncturing method is the key of the framework in Figure 2, and the different puncturing methods correspond to different error protection schemes. In the following, we propose two non-uniform puncturing methods that can achieve 3-level and 8-level protection for the digital speech signal, respectively.

3.1 3-Level Protection Scheme

The traditional uniform puncturing method can only achieve the EEP capability. In other words, the uniform puncturing of EEP considers that the total information bits have the equal importance degree. Detailedly, in the uniform puncturing of EEP, each information bit has two parity bits, i.e., $p^{(i)}_{j,1}$ and $p^{(i)}_{j,2}$, initially ($i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, 8$). If the information bit locates in the odd position j, its second parity bit $p^{(i)}_{j,2}$ is removed and its first parity bit $p^{(i)}_{j,1}$ is kept as its unique parity bit, while if the information bit locates in the even position j, its first parity bit $p^{(i)}_{j,1}$ is removed and its second parity bit $p^{(i)}_{j,2}$ is kept as its unique parity bit, see Figure 3. Thus, after the uniform puncturing of EEP, each information bit has only one parity bit, and the coding rate is 1/2 consequently. However, only one protection level can be provided by the uniform puncturing

of EEP, which can not meet the practical requirement. A UEP scheme with 3-level protection through the non-uniform puncturing is given as follows, which can also improve the performance of coding rate.

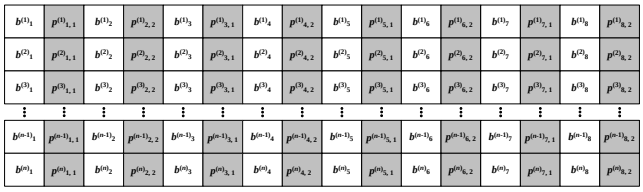


Figure 3: The result of the uniform puncturing of EEP

According to the results of the hierarchical importance analysis in Section 2, the second bit $b^{(i)}{}_2$ of the 8-bit folded binary code for each sampling point $x^{(i)}$ in **X** has the highest importance degree, and the eighth bit $b^{(i)}{}_8$ has the lowest importance degree (i = 1, 2, …, n). Therefore, in the proposed 3-level protection scheme, we define that the n bits of $b^{(i)}{}_2$ for all n sampling points in **X** are provided with the highest protection level, i.e., level 1, while the n bits of $b^{(i)}{}_8$ are provided with the lowest protection level, i.e., level 3. The remaining 6n information bits including $b^{(i)}{}_1$, $b^{(i)}{}_3$, $b^{(i)}{}_4$, $b^{(i)}{}_5$, $b^{(i)}{}_6$, and $b^{(i)}{}_7$, are considered as a whole and provided with the middle protection level, i.e., level 2.

During the non-uniform puncturing process, each of the n bits $b^{(i)}{}_2$ for all n sampling points in **X** is always assigned with two parity bits, i.e., $p^{(i)}{}_{2,1}$ and $p^{(i)}{}_{2,2}$, for error protection (i = 1, 2, …, n), see Part 1 in Figure 4, and each of the n bits $b^{(i)}{}_8$ is always assigned with no parity bits, see Part 3 in Figure 4. For the 6n information bits belonging to level 2, 6n – m parity bits are assigned randomly ($0 \le m < 6n$), and each bit belonging to level 2 is assigned with no more than one parity bit, see Part 2 in Figure 4. That is to say, after puncturing, m information bits belonging to level 2 have no parity bits, and each of the other 6n – m information bits has one parity bit. Statistically, each information bit belonging to level 1, 2, and 3 is assigned with 2, (6n – m)/6n, and 0 parity bits for error protection, respectively. Thus, more important the information bit is, more parity bits are assigned for error protection.

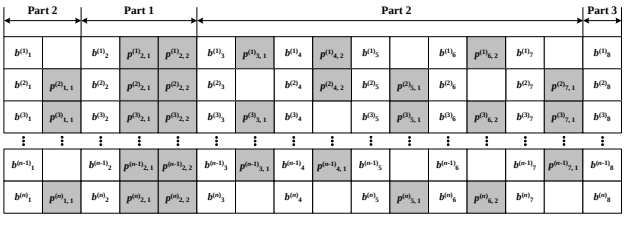


Figure 4: The result of the non-uniform puncturing of UEP with 3-level protection

In the proposed 3-level protection scheme, there are totally 8n – m parity bits assigned to the 8n information bits of three protection levels. Clearly, the coding rate is 8n/(16n – m) after this non-uniform puncturing of UEP with 3-level protection, which is always not smaller than that of the EEP scheme.

3.2 8-Level Protection Scheme

In this subsection, we propose a UEP scheme with 8-level protection for the speech signal **X**, which can achieve more hierarchical protection than the 3-level scheme. As stated in Section 2, the hierarchical importance of the 8-bit folded binary code for each sampling point $x^{(i)}$ in **X** is: I($b^{(i)}{}_2$) > I($b^{(i)}{}_1$) > I($b^{(i)}{}_3$) > I($b^{(i)}{}_4$) > I($b^{(i)}{}_5$) > I($b^{(i)}{}_6$) > I($b^{(i)}{}_7$) > I($b^{(i)}{}_8$), (i = 1, 2, …, n). Thus, similar with the 3-level scheme, in the proposed 8-level protection scheme, we define that the n bits of $b^{(i)}{}_2$ for all n sampling points in **X** have the highest protection level, i.e., level 1, and the n bits of $b^{(i)}{}_8$ have the lowest protection level, i.e., level 8. The n bits of $b^{(i)}{}_1$ are defined to belong to level 2, and the n bits of $b^{(i)}{}_j$ are defined to belong to level j (j = 3, 4, 5, 6, 7). Therefore, totally 8 protection levels are defined, and each protection level has n information bits.

During the non-uniform puncturing process, each of the n bits $b^{(i)}{}_2$ belonging to level 1 is always assigned with two parity bits, i.e., $p^{(i)}{}_{2,1}$ and $p^{(i)}{}_{2,2}$, for error protection (i = 1, 2, …, n), see Part 1 in Figure 5, and each of the n bits $b^{(i)}{}_8$ belonging to level 8 is always assigned with no parity bits, see Part 8 in Figure 5. For the n bits $b^{(i)}{}_1$ belonging to level 2, n – m_1 parity bits are assigned randomly, and each bit belonging to level 2 is assigned with no more than one parity bit, see Part 2 in Figure 5. Similarly, for the n bits $b^{(i)}{}_j$ belonging to level j (j = 3, 4, 5, 6, 7), n – m_j parity bits are assigned randomly, and each bit belonging to level j is assigned with no more than one parity bit, see Part 3-7 in Figure 5. That is to say, after puncturing, m_1 information bits belonging to level 2 have no parity bits, and each of the other n – m_1 bits has one parity bit; m_j information bits belonging to level j have no parity bits, and each of the other n – m_j bits has one parity bit (j = 3, 4, 5, 6, 7). Note that the following relationship should be satisfied to achieve the UEP capability and be consistent with the result of hierarchical importance analysis in Section 2.

$$0 \le m_1 \le m_3 \le m_4 \le m_5 \le m_6 \le m_7 < n. \qquad (16)$$

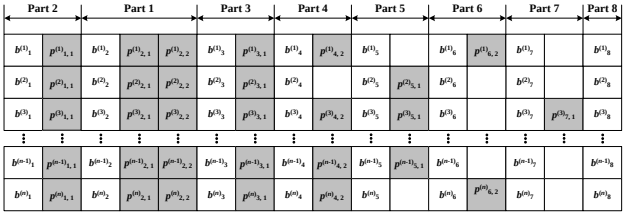


Figure 5: The result of the non-uniform puncturing of UEP with 8-level protection

Consequently, according to Equation (16), more important the information bit is, more parity bits are assigned for error protection. Statistically, each information bit belonging to level 1 and level 2 is assigned with 2 and (n – m_1)/n parity bits for error protection, respectively; each information bit belonging to level j is assigned with (n – m_j)/n parity bits (j = 3, 4, 5, 6, 7), and no parity bits are assigned to the information bits belonging to level 8. Here,

for simplicity, we make the summation of m_j (j = 1, 3, 4, 5, 6, 7) be equal to the value m in the 3-level scheme, see Equation (17). Thus, the coding rate of the proposed 8-level protection scheme is also $8n/(16n - m)$, which is equal to that of 3-level protection scheme.

$$m_1 + \sum_{j=3}^{7} m_j \equiv m. \tag{17}$$

3.3 Analysis of 3-Level and 8-Level UEP Schemes

The two Turbo-based schemes proposed above both utilize the non-uniform puncturing method to achieve the UEP capability and provide the hierarchical protection to the information bits of the speech signal. Compared with the EEP scheme described in Figure 3, the UEP schemes shown in Figures 4-5 make full use of the characteristics of speech signal, i.e., the sign bit, 3 bits in paragraph code, and 4 bits in segment code have different importance degrees, to achieve better performance.

The 3-level UEP scheme divides the importance degree into 3 parts, which makes the encoding and decoding procedures easier to implement compared with the 8-level UEP scheme. In other words, the 3-level UEP scheme can achieve a compromise of simple encoding/decoding structure and good protection capability considering the speech signal characteristics, which is more suitable for real-time applications. The 8-level UEP scheme divides the importance degree into 8 parts, and its encoding and decoding procedures are more complicated compared with the 3-level UEP scheme. But, the 8-level UEP scheme take full advantage of the hierarchical importance of the speech signal and can achieve better protection capability than the EEP scheme and the proposed 3-level UEP scheme, which is more suitable for the communication system requiring higher reliability.

4 Experimental Results and Comparisons

Experiments were conducted on a large number of the digital speech signals to evaluate the performances of our unequal protection schemes. All experiments were implemented on a computer with 2.40 GHz Intel Core 2 Quad Q6600 processor, 3.00 GB memory, and Windows 7 operating system. Due to the extensive data of sampling points, the whole speech signal was divided into several segments with the equal length, and the error protection scheme was carried on each segment independently. Average segment signal-to-noise ratio (ASSNR) was utilized to evaluate the quality of the speech signal. The average value of the segment signal-to-noise ratio, i.e., ASSNR, for all segments of the speech signal can be calculated according to Equation (18).

$$\text{ASSNR} = \frac{1}{K}\sum_{k=1}^{K} 10 \times \log_{10}\left\{\frac{\sum_{i=1}^{n} X_k^2(i)}{\sum_{i=1}^{n}[X_k(i) - X_k'(i)]^2}\right\}, \tag{18}$$

where K is total number of the divided segments for the whole speech signal, n is the number of sampling points in each speech segment, $X_k(i)$ and $X'_k(i)$ are the i^{th} sampling point values of the k^{th} segment for the original input speech signal on the sender side and the decoded signal on the receiver side, respectively. Obviously, the greater the value of ASSNR is, the better the quality of the received speech signal is. Experimental configurations are listed in Table 2.

We first compared the coding rate performances between the traditional Turbo-based EEP scheme and our proposed UEP schemes. As stated above, in the traditional Turbo-based EEP scheme, after the uniform puncturing, each information bit has one parity bit, thus, the coding rate is fixed to 1/2. For our proposed 3-level and 8-level UEP schemes, the coding rates both are $8n/(16n - m)$, which is related to the parameter m ($0 \le m < 6n$) in the non-uniform puncturing process. The value m denotes the number of bits $\{b^{(i)}_1, b^{(i)}_3, b^{(i)}_4, b^{(i)}_5, b^{(i)}_6, b^{(i)}_7\}$ assigned with no parity bits in each segment of the speech signal (i = 1, 2, …, n). Figure 6 shows the results of the coding rates for the EEP scheme and the proposed UEP scheme. It can be observed from Figure 6 that the coding rate of the proposed UEP scheme increases with m and is always not smaller than that of the EEP scheme, which demonstrates that the proposed scheme has better performance of the encoding efficiency than the EEP scheme. Note that, with the increase of m, the error protection capability of our scheme for the speech signal could decrease gradually. Thus, in the following, the performances of error protection were also compared.

Table 2: Experimental configurations

Parameters	***Values***
Data transmission channel	AWGN channel
Channel SNRs	E_b/N_0 = 0.6dB, 0.8dB, 1.0dB, 1.2dB
Interleaver	Pseudo-random interleaver
Number of sampling points in each segment	n = 64
Decoding algorithm	Log-MAP

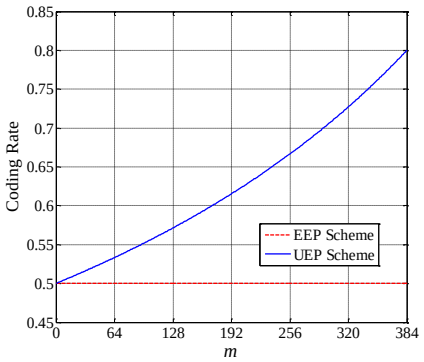


Figure 6: Comparisons of the coding rate between the traditional Turbo-based EEP scheme and our proposed UEP scheme

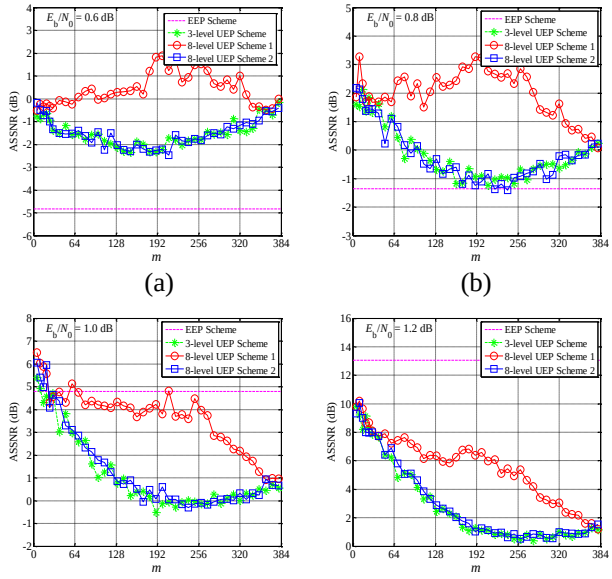


Figure 7: Comparison results of error protection performances under different channel SNRs for speech signal 1. (a) E_b/N_0 = 0.6 dB, (b) E_b/N_0 = 0.8 dB, (c) E_b/N_0 = 1.0 dB, (d) E_b/N_0 = 1.2 dB.

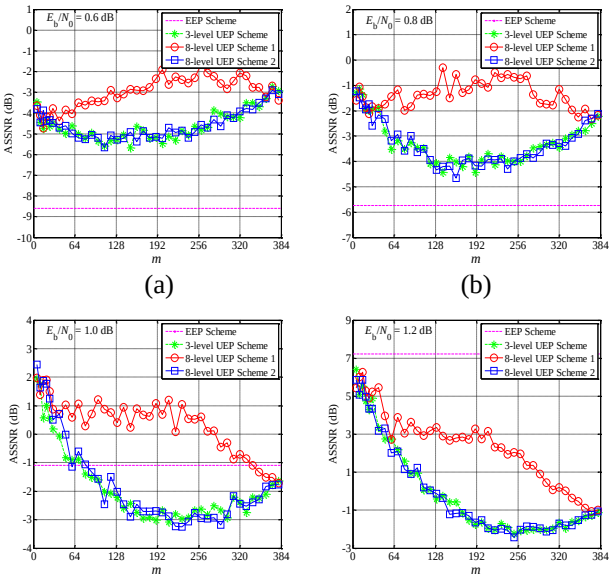


Figure 8: Comparison results of error protection performances under different channel SNRs for speech signal 2. (a) E_b/N_0 = 0.6 dB, (b) E_b/N_0 = 0.8 dB, (c) E_b/N_0 = 1.0 dB, (d) E_b/N_0 = 1.2 dB.

Figures 7-9 show the comparison results of error protection performances among traditional Turbo-based EEP scheme, proposed 3-level UEP scheme, and proposed 8-level UEP scheme. Figures 7, 8, and 9 correspond to the results of three typical speech signals, i.e., man.wav (male voice), woman.wav (female voice), and music.wav (female song), and each signal was tested under four different channel SNRs E_b/N_0, i.e., 0.6 dB, 0.8 dB, 1.0 dB, and 1.2 dB, respectively. The three digital speech signals all have

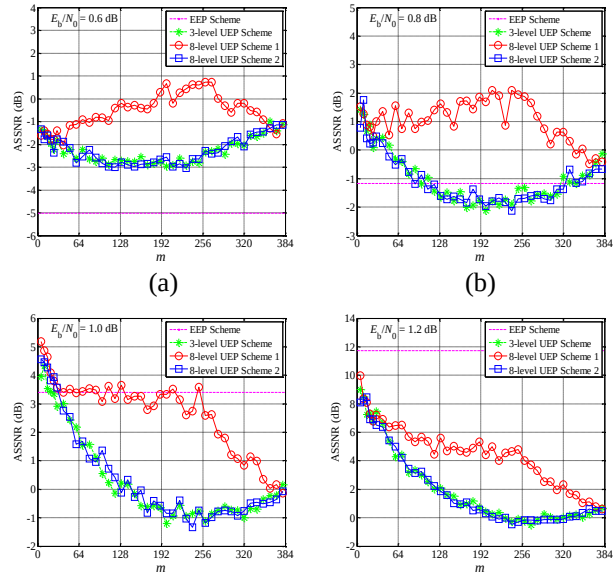


Figure 9: Comparison results of error protection performances under different channel SNRs for speech signal 3. (a) E_b/N_0 = 0.6 dB, (b) E_b/N_0 = 0.8 dB, (c) E_b/N_0 = 1.0 dB, (d) E_b/N_0 = 1.2 dB.

the durations of 8 seconds, and the used sampling frequency was 8 KHz, which means there are 64,000 sampling points in each signal. Because n was set to 64 in the experiments, each signal was divided into 1,000 segments, i.e., K =1000. Note that, for a given value of m in the proposed 8-level UEP scheme, there are possibly a large number of solutions for m_j (j = 1, 3, 4, 5, 6, 7) to meet the relationships in Equations (16-17). In Figures 7-9, the curves of 8-level UEP scheme 1 correspond to a randomly chosen group of m_1, m_3, m_4, m_5, m_6, m_7 that are satisfied with Equations (16-17), and the curves of 8-level UEP scheme 2 correspond to a specific group of m_1, m_3, m_4, m_5, m_6, m_7 that have the equal value, i.e., m/6. Thus, for a statistical point of view, 8-level UEP scheme 2 is equivalent to the 3-level UEP scheme.

Because hierarchical importance degrees of information bits are considered during the puncturing process of parity bits, some conclusions can be acquired from the results of Figures 6-9. (1) For each speech signal, when the channel SNR, i.e., E_b/N_0, increases, the ASSNAR value always becomes greater. It means that ASSNR value is directly proportional to E_b/N_0. (2) When m = 0, i.e., no parity bits are punctured from each information bit of $\{b^{(i)}_1, b^{(i)}_3, b^{(i)}_4, b^{(i)}_5, b^{(i)}_6, b^{(i)}_7\}$, the coding rate is 1/2 and the ASSNR value is the peak value of each curve. When m = 384, i.e., all parity bits are punctured from all information bits, the coding rate is the maximum value and the ASSNR value is the valley value of each curve. No matter m equals 0 or 384, the curves of the 3-level UEP scheme and the 8-level UEP scheme intersect at a point for the reason that their parity bits are at the same state, i.e., the second information bit with two parity bits and the eighth information bit with no parity bits. E_b/N_0 and ASSNR value have no linear relationship with the change of m due to the random

puncturing for the parity bits. Our two proposed UEP schemes not only have better error protection performance than the traditional Turbo codes of EEP, but also have greater coding rate, which means the higher transmission efficiency of our schemes. (3) For each given value of m, the 8-level UEP scheme 1 always performs better than the 8-level UEP scheme 2 due to the different distributions of m for the two schemes. When m is divided evenly into 6 parts according to 8-level UEP scheme 2, the parity bits of information bits $\{b^{(i)}_1, b^{(i)}_3, b^{(i)}_4, b^{(i)}_5, b^{(i)}_6, b^{(i)}_7\}$ are punctured equally. However, when m is divided into 6 parts according to the puncturing method of the 8-level UEP scheme 1, the parity bits are mainly punctured from the latter part of information bits $\{b^{(i)}_1, b^{(i)}_3, b^{(i)}_4, b^{(i)}_5, b^{(i)}_6, b^{(i)}_7\}$ and the parity bits of the former part of information bits are retained, which leads to better quality of the decoded speech signal. (4) Under the lower channel SNRs, the two proposed 8-level and 3-level UEP schemes generally have better performances of error protection than the traditional Turbo-based EEP scheme with respect to ASSNR. Due to the strategy of more hierarchical protection, 8-level UEP scheme is superior to 3-level UEP scheme. However, when the channel condition and SNRs become better, the superiority of the proposed UEP schemes is not significant compared with the EEP scheme, even though their coding rates are always greater than that of the EEP scheme, which demonstrates the proposed 8-level and 3-level UEP schemes are more suitable to be applied in the poor transmission condition.

5 Conclusions

Two novel unequal protection schemes for digital speech transmission are proposed in this paper. By calculating the changing value for the amplitude of each sampling point, the hierarchical importance analysis for each information bit in the 8-bit PCM code is first conducted. Then, according to the acquired regularity of hierarchical importance, two Turbo-based UEP schemes with 3-level and 8-level protection capability are designed for the reliable speech transmission through the non-uniform puncturing mechanism. Because more important information bits are adaptively assigned with more parity bits in the two proposed scheme, the performances of error protection for the speech signal are generally better than that of the traditional Turbo-based EEP scheme, especially in the poor channel condition with lower SNR. Additionally, the coding rate of our UEP schemes is always greater than that of the EEP scheme. Future investigations include how to obtain the optimal assignment of parity bits with higher efficiency in non-uniform puncturing process.

Acknowledgments

This work was supported by the Natural Science Foundation of China (61103181, 61303203), the Natural Science Foundation of Shanghai, China (13ZR1428400), and the Innovation Program of Shanghai Municipal Education Commission (14YZ087).

References

[1] K. M. Alajel, X. Wei and Y. F. Wang, "Unequal error protection scheme based hierarchical 16-QAM for 3-D video transmission," *IEEE Transactions on Consumer Electronics*, vol. IT-58, no. 3, pp. 731-738, 2012.

[2] C. Berrou, A. Glavieux and P. Thitimajshima, "Near shannon limit error correcting coding and decoding: turbo-codes. 1," in *Proceedings of IEEE International Conference on Communication*, pp. 1064-1070, 1993.

[3] I. Boyarinov and G. Katsman, "Linear unequal error protection codes," *IEEE Transactions on Information Theory*, vol. IT-27, no. 3, pp. 168-175, 1981.

[4] C. C. Kilgus and W. C. Gore, "Cyclic codes with unequal error protection," *IEEE Transactions on Information Theory*, vol. IT-17, no. 3, pp. 214-215, 1971.

[5] B. Masnick and J. Wolf, "On linear unequal error protection codes," *IEEE Transactions on Information Theory*, vol. IT-3, no. 10, pp. 600-607, 1967.

[6] A. Morcos and T. Elshabrawy, "Four-level UEP of H.264 scalable video coding using discrete wavelet transform," in *Proceedings of 2011 IEEE 22nd International Symposium on Personal, Indoor and Mobile Radio Communication*, pp. 1778-1782, 2011.

[7] Y. C. Sum and W. J. Tsai, "Analysis of unequal error protection for LDPCA codes," *Electronics Letters*, vol. 49, no. 2, pp. 102-104, 2013.

[8] N. Thomos, V. Boulgouris, and G. Strintzis, "Wireless image transmission using turbo codes and optimal unequal error protection," *IEEE Transactions on Image Processing*, vol. IT-14, no. 11, pp. 1890-1901, 2005.

[9] C. H. Wang, M. C. Chiu, and C. C. Chao, "On unequal error protection of convolutional codes from an algebraic perspective," *IEEE Transactions on Information Theory*, vol. IT-56, no.1, pp. 296-315, 2010.

[10] S. J. Xiang and J. W. Huang, "Audio watermarking to D/A and A/D conversions," *International Journal of Network Secruity*, vol. 3, no. 3, pp. 230-238, 2006.

[11] C. C. Yang, K. H. Chu, and Y. W. Yang, "3G and WLAN interworking security: current status and key issues," *International Journal of Network Secruity*, vol. 2, no. 1, pp: 1-13, 2006.

[12] K. C. Yang and J. S. Wang, "Unequal error protection for streaming media based on rateless codes," *IEEE Transactions on Computers*, vol. 61, no. 5, pp. 666-675, 2012.

[13] T. C. Yeh, J. R. Peng, S. S. Wang, and J. P. Hsu, "Securing bluetooth communications," *International Journal of Network Secruity*, vol. 14, no. 4, pp. 229-235, 2012.

[14] S. J. Zhang, F. Shao, and Y. Yu, "Unequal error protection of MELP compressed speech based on

plotkin type LDPC code," in *Proceeding of 2009 International Conference on Communication and Mobile Computing*, vol. 1, pp. 166-169, 2009.

[15] W. D. Zhang, S. Xia, and M. Torki, et al., "Unequal error protection of JPEG2000 image using short block length turbo codes," *IEEE Communications Letters*, vol.15, no. 6, pp. 659-661, 2011.

Boqing Xu received the B.S. degree in Communication Engineering from Dalian Maritime University in 1982 and the M.S. degree in Industrial Automation from Shandong University in 1987. In 2003, he received the Ph.D. degree Patten Recognition and Artificial Intelligence from Tongji University, Shanghai, China. Currently, he has been with the faculty of the School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, where he is currently an Associate Professor. His research interests include signal processing and optimization theory.

Qun Xiao received the B.S. degree in Science and Technology of Electronic Information from Hubei University of Art and Science, Hubei, China, in 2011. She is currently pursuing the M.S. degree in Signal and Information Processing from University of Shanghai for Science and Technology, Shanghai, China. Her research interests include signal processing and data coding.

Zhenxing Qian received the B.S. and Ph.D. degrees from the University of Science and Technology of China (USTC), Hefei, China, in 2003 and 2007, respectively. Since 2009, he has been with the faculty of the School of Communication and Information Engineering, Shanghai University, where he is currently an Associate Professor. His research interests include signal processing, data hiding, and digital forensics.

Chuan Qin received the B.S. and M.E. degrees in Electronic Engineering from the Hefei University of Technology, Anhui, China, in 2002 and 2005, respectively, and the Ph.D. degree in signal and information processing from Shanghai University, Shanghai, China, in 2008. Since 2008, he has been with the faculty of the School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, where he is currently a Lecturer. He also has been with Feng Chia University at Taiwan as a Postdoctoral Researcher from July 2010 to June 2012. His research interests include image processing and multimedia security.

Mitigating Key Escrow in Attribute-based Encryption

Yongtao Wang, Xiaonan Liu, Lulu Liang, Weiduan Feng, and Guang Yang
(Corresponding author: Yongtao Wang)

China Information Technology Security Evaluation Center, Beijing, P. R. China
(E-mail: wyt.itsec@gmail.com)
(Received Mar. 22, 2013; revised and accepted July 16, 2013)

Abstract

The notion of accountable authority introduced by Goyal (Crypto 2007) in identity-based encryption (IBE) setting is a novel approach to mitigate the (inherent) key escrow problem in identity based cryptosystems. As far as we know, the (inherent) key escrow problem also exists in attribute based encryption (ABE), for example ciphertext policy ABE (CP-ABE). In this paper, the concept of accountable authority is generalized to ABE setting. We first formalize the definitions and security models for accountable authority attribute-based encryption (A-ABE), and then present two concrete constructions. One is designed for the threshold ABE with large universe attributes, and the other is built for ciphertext policy ABE. In our scheme, a user will be identified by a pair (id, ω), where id denotes the identity of a user and ω denotes a attribute set associated to the user. In addition, both constructions are shown to be secure in the standard model under some reasonable assumptions.

Keywords: Accountable authority, attribute-based encryption, key escrow, standard model, traceability

1 Introduction

The concept of attribute-based encryption first introduced by Sahai and Waters [20] in 2005 provides one-to-many communication and is a new means for encrypted access control. In an ABE scheme, an access structure is integrated with the identity-based encryption. The original system of Sahai and Waters is a Threshold ABE system, in which both user's private key and ciphertext are associated with a set of attributes, respectively. A user can decrypt a ciphertext when at least d (threshold parameter) attributes overlap between the attribute set associated to the ciphertext and the attribute set associated to the user's private key. At present, there are many extensions for supporting more complex access structure, for example, the key policy ABE (KP-ABE) in [8, 17] and the ciphertext policy ABE (CP-ABE) in [2, 14]. We refer the reader to [4, 10, 15, 22] for some related results about ABE.

The motivation to consider accountable authority attribute-based encryption system is as follows. ABE can be viewed as a generalization of identity-based encryption, and it inherits the key escrow problem from IBE [3, 5, 21, 25]. In an ABE system, all users' private keys are issued by an unconditionally trusted authority. Such an authority possesses the master secret key of the system, and can decrypt all ciphertexts encrypted to any user. Moreover, the authority can redistribute users' private keys for malicious use. Thus, it has great significance that reducing the trust in the authority in an ABE system.

Goyal [6] first introduced the notion of accountable authority identity based encryption (A-IBE) for mitigating the key escrow problem in IBE. In an A-IBE scheme, if the authority redistributes some user's private key for malicious use, it will run the risk of being caught and sued by the user. The above goal can be achieved by the following approach: (1) For every identity id, there will be an exponential number of possible keys. (2) To generate a user's private key, an interactive key generation protocol will be implemented between the authority and the user. This protocol will ensure that the family, that the generated key belongs to, is concealed to the authority. (3) With this single key, it is intractable for the user to find any other keys from a different family. Thus, two keys from distinct families for an identity give evidence of the authority's misbehavior. At present, there are several constructions for A-IBE [1, 6, 7, 12, 13, 19]. In ABE setting, we notice that Li et al. [11] introduced a new type of ABE, which achieves the accountability of the authority. However, their scheme assumes that each user has a higher level secret before requesting an attribute private key. This work is orthogonal to ours.

In this paper, we formalize the definitions and security notions for accountable authority ABE and present two constructions. One is based on the large universe construction for ABE in [20], and the other is built on the ciphertext policy ABE scheme in [14]. We refer the reader

to [23, 24] for some other constructions. Our approach to achieve the notion of accountable authority ABE is inspired by the A-IBE scheme proposed by Libert et al. [12, 13]. In our constructions, we introduce identity *id* to label a user's private key, and a user will be identified by a pair (id, ω), where ω is a set of attributes. Furthermore, we modify the scheme in [12], and achieve that the ability of decryption of a user is independent of his identity. After that, we non-trivially integrate the modify scheme with an ABE scheme. Thus, the notion of A-ABE is achieved. We describe our two constructions in the white-box model [6]. However, notice that the weak black-box tracing algorithm described in [12] can be trivially extended to our schemes. In addition, our constructions are shown to be secure in the standard model under some reasonable assumptions.

The rest of the paper is organized as follows. In Section 2 we recall some preliminaries. In Section 3, we give the construction for accountable authority threshold ABE with large universe attributes and its security proofs. We describe the construction for accountable authority ciphertext policy ABE and give its security proofs in Section 4. Finally, we conclude in Section 5.

2 Preliminaries

2.1 Bilinear Maps and Complexity Assumptions

We now review the notion of bilinear maps. Let $\mathbb{G}_1$, $\mathbb{G}_2$ be two multiplicative cyclic groups of prime order p, and g be a generator of $\mathbb{G}_1$. Let e denote a bilinear map, $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, which has the following properties [3]:

- Bilinearity: For all $u, v \in \mathbb{G}_1$ and $a, b \in \mathbb{Z}_p$, it satisfies $e(u^a, v^b) = e(u, v)^{ab}$.
- Non-degeneracy: $e(g, g) \neq 1_{\mathbb{G}_2}$.
- Computability: There exists an efficient algorithm to compute $e(u, v)$, for all $u, v \in \mathbb{G}_1$.

We require the following two assumptions holds which have been used before in [9, 12].

Definition 1. (Modified Diffie-Hellman Assumption, MDH). *Given a tuple (g, h, g^x), where g is a generator of $\mathbb{G}_1$, and $x \in \mathbb{Z}_p$, $h \in \mathbb{G}_1$ are random, there is no polynomial-time algorithm to output $h^{1/x}$.*

Definition 2. (Modified Bilinear Decision Diffie-Hellman Assumption, MBDDH). *This assumption states that the two distributions $(A = g^a, B = g^b, C = g^c, C' = g^{c^2}, D = e(g, g)^{abc})$ and $(A = g^a, B = g^b, C = g^c, C' = g^{c^2}, D = e(g, g)^z)$ are indistinguishable for any polynomial-time adversary $\mathcal{B}$, where $a, b, c, z \in \mathbb{Z}_p$ are random. Let κ be the security parameter. The advantage function $\mathrm{Adv}_{\mathcal{B}}^{mbddh}(\kappa)$ of $\mathcal{B}$ is defined as*

$$\big|\Pr\big[\mathcal{B}(g^a, g^b, g^c, g^{c^2}, e(g, g)^{abc}) = 1\big] - \Pr\big[\mathcal{B}(g^a, g^b, g^c, g^{c^2}, e(g, g)^z) = 1\big]\big|.$$

We say that the MBDDH assumption holds if $\mathrm{Adv}_{\mathcal{B}}^{mbddh}(\kappa)$ is negligible for all polynomial-time adversaries.

Note that the MDH assumption is equivalent to the Diffie-Hellman assumption [12], and the MBDDH assumption is equivalent to the Bilinear Decision Diffie-Hellman assumption (BDDH) [9].

2.2 Syntax

We now describe the syntax of an A-ABE scheme. In our setting, a user will be identified by a pair (id, ω). It is allowable for different users with the same set of attributes. However, we require that a user should be assigned only one set of attributes. Formally, an accountable authority attribute-based encryption scheme consists of five polynomial-time algorithms described as follows:

- **Setup:** This algorithm takes as input a security parameter κ, and outputs a master public key mpk and a master secret key msk.
- **KeyGen:** This is an interactive protocol implemented between a user U and the authority. The public input to the authority and U consists of the mpk and (id, ω) (of U). The private input to the authority is the msk. In addition, a sequence of random coin tosses may be used by the authority and U as private inputs. At the end of the protocol, U can extract a private key $d_{id,\omega}$.
- **Encryption:** Takes as input the mpk, a set of attributes ω' (in CP-ABE, ω' is replaced by an access structure W) and a message M, this algorithm outputs a ciphertext E.
- **Decryption:** Takes as input a user secret key $d_{id,\omega}$ and a ciphertext E encrypted under ω' (or W), this algorithm outputs a plaintext message M if $|\omega \cap \omega'| \geq d$ (in CP-ABE, ω should satisfy the access structure W), where d is a threshold parameter.
- **Trace:** This algorithm takes a well-formed decryption key $d_{id,\omega}$ as input, and outputs the decryption key family number n_F.

Note that the above algorithms are described in the white-box traceability model. In this model, the Trace algorithm can only deal with a well-formed key. However, the Trace algorithm needs to trace a decryption box in the black-box traceability model [7].

2.3 Security Models

In this section, we describe the security models of our A-ABE scheme in the white-box setting. The reader is referred to [6, 7, 12] for further extensions in the black-box model.

The IND-SS-CPA game. We simply extend the selective model of [20] to our setting. Let $\mathcal{A}$ be an adversary.

- **Init.** $\mathcal{A}$ declares a set of attributes ω^* (in CP-ABE, $\mathcal{A}$ declares an access structure W^*).
- **Setup.** The challenger runs the Setup algorithm of A-ABE and gives the public parameters to $\mathcal{A}$.
- **Phase 1.** $\mathcal{A}$ runs the key generation protocol with the challenger for many pairs (id_j, ω_j), where $|\omega_j \cap \omega^*| < d$ (in CP-ABE, this condition should state that ω_j does not satisfy W^*) for all j. There is no limitation on id_j.
- **Challenge.** $\mathcal{A}$ submits two equal length messages M_0, M_1. The challenger flips a random coin, ν, and encrypts M_ν with ω^* (replaced by the access structure W^* in CP-ABE). The ciphertext is passed to $\mathcal{A}$.
- **Phase 2.** Phase 1 is repeated.
- **Guess.** $\mathcal{A}$ outputs a guess ν' of ν.

In the above game, the advantage of the adversary $\mathcal{A}$ is defined as $|\Pr[\nu' = \nu] - \frac{1}{2}|$.

The FindKey game. This game follows from [6] except slight modification for our setting. Let $\mathcal{A}$ be a malicious authority.

- **Setup.** $\mathcal{A}$ generates and gives the mpk with a pair (id, ω) to the challenger. The challenger runs a sanity check on mpk and aborts if the check fails.
- **Key Generation.** The challenger and $\mathcal{A}$ run the key generation protocol to generate a decryption key for (id, ω). The challenger gets the key $d_{id,\omega}$ as private output and runs a key sanity check on it. It aborts if the check fails.
- **Find Key.** $\mathcal{A}$ outputs a decryption key $d'_{id,\omega}$. The challenger runs a key sanity check on it. It aborts if the check fails.

Let K_1 denote the event that $\mathrm{Trace}(d'_{id,\omega}) = \mathrm{Trace}(d_{id,\omega})$. Define $\mathcal{A}$' advantage as $\Pr[K_1]$. The above game emulates the attack that a malicious authority try to produce a private key belonging to the same family as the user's key generated in the key generation protocol.

The ComputeNewKey game. This game is defined along the line of [6]. Here, we describe it in the selective model. Let $\mathcal{A}$ be an adversary.

- **Init.** $\mathcal{A}$ declares an identity id^*.
- **Setup.** The challenger runs the Setup algorithm of A-ABE and gives the public parameters to $\mathcal{A}$.
- **Key Generation.** $\mathcal{A}$ runs the KeyGen with the challenger for many pairs (id_j, ω_j), where id_j must be distinct. There is no limitation on ω_j.
- **New Key Computation.** $\mathcal{A}$ outputs two decryption keys $d_{id^*,\omega}$ and $d'_{id^*,\omega}$. The challenger runs a key sanity check on them. It aborts if any check fails.

Let K_2 denote the event that $\mathrm{Trace}(d'_{id^*,\omega}) \neq \mathrm{Trace}(d_{id^*,\omega})$. In this game, define $\mathcal{A}$' advantage as $\Pr[K_2]$. Intuitively, this game emulates the attack that a user try to compute a new key belonging to a different family from his key generated in the key generation protocol.

Definition 3. *An A-ABE scheme is IND-SS-CPA secure if all polynomial time adversaries have at most a negligible advantage in the above three games.*

3 Accountable Authority Threshold ABE with Large Universe Attributes

We now describe our first construction, which mainly borrows ideas from the A-IBE scheme [12] and is based on the large universe construction of the attribute-based encryption scheme proposed by Sahai and Waters [20].

3.1 Description

In this construction, we assume n be the maximum size attribute set for a user, d be the threshold value and N be the set of $\{1, 2, \ldots, n+1\}$. For simplicity, let ω be a set of n elements of $\mathbb{Z}_p^*$. In addition, we can apply a collision-resistant hash function $h : \{0,1\}^* \to \mathbb{Z}_p^*$, which allows arbitrary strings as attributes. Define the Lagrange coefficient $\Delta_{k,S}$ for $k \in \mathbb{Z}_p$ and a set, S, of elements in $\mathbb{Z}_p$: $\Delta_{k,S}(x) = \prod_{j \in S, j \neq k} \frac{x-j}{k-j}$. Our construction follows:

- **Setup:** First, generate a set of pairing groups at the security level κ. Next, choose randomly $x, y, y_1 \in \mathbb{Z}_p^*$, $h, Z, g_2, t_1, \ldots, t_{n+1} \in \mathbb{G}_1$, and set $X = g^x, Y_1 = g_2^{y_1}, g_1 = g^y$. Now, define a function T as in [20]: $T(x) = g_2^{x^n} \prod_{i=1}^{n+1} t_i^{\Delta_{i,N}(x)}$. Finally, set the master public key mpk as

$$\{X, h, Z, t_1, \ldots, t_{n+1}, K = e(g_1, g_2), K_1 = e(g, Y_1)\},$$

  and the master private key msk as $\{x, y, y_1\}$.
- **KeyGen:** To generate a private key for a user U with (id, ω). The following protocol will be executed between U and the authority.
  - U chooses $s_0, \theta \in \mathbb{Z}_p^*$ at random, and provides a commitment $R = h^{s_0} \cdot X^\theta$ with an interactive witness indistinguishable proof of knowledge of the (s_0, θ) to the authority. In addition, U retains (s_0, θ).
  - The authority verifies the proof of knowledge, outputs $\perp$ if fails. Otherwise, it chooses randomly $s_1, r' \in \mathbb{Z}_p^*$ and a $d-1$ degree polynomial $q(x)$ with $q(0) = y - y_1$. The authority returns $d'_{id,\omega} = (d'_1, d'_2, d'_3, d'_4)$ as

$$((g_2^{y_1} R h^{s_1})^{\frac{1}{x}} \cdot (g^{id} Z)^{r'}, X^{r'}, s_1, \{D_i = g_2^{q(i)} T(i)^{r_i}, \quad F_i = g^{r_i}\}_{i \in \omega}),$$

where r_i are chosen randomly from $\mathbb{Z}_p^*$.

– U chooses $r'' \in \mathbb{Z}_p^*$ at random and computes $d_{id,\omega} = (d_1, d_2, d_3, d_4)$ as $(d'_1/g^\theta \cdot (g^{id}Z)^{r''}, d'_2 \cdot X^{r''}, d'_3 + s_0, d'_4)$, which should equal

$$((g_2^{y_1}h^s)^{\frac{1}{x}} \cdot (g^{id}Z)^r, X^r, s, \{D_i = g_2^{q(i)}T(i)^{r_i}, \quad F_i = g^{r_i}\}_{i\in\omega}),$$

where $r = r' + r''$ and $s = s_0 + s_1$. Now U checks $d_{id,\omega}$ as follows. First, the consistence of every element of d_4 should be checked. Choose an arbitrary d-element subset, S, of ω and compute $R_i = e(D_i, g)/e(F_i, T(i))$ for $i \in S$. Then compute $R_0 = \prod_{i\in S}(R_i^{\Delta_{i,S}(0)})$. Let Γ be an arbitrary subset of S such that $|\Gamma| = d-1$. Define $S' = \Gamma \cup \{0\}$. U checks the following relation for each $j \in \omega - S$:

$$\prod_{i\in S'} \left(R_i^{\Delta_{i,S'}(j)}\right) = \frac{e(D_j, g)}{e(F_j, T(j))}.$$

Second, U checks

$$\frac{e(d_1, X)}{e(g, h)^{d_3} \cdot e(g^{id}Z, d_2)} = K_1,$$

and $R_0 \cdot K_1 = K$. U outputs $\perp$ if any check fails. Otherwise, U sets his private key as $d_{id,\omega}$ and the key family number as $n_F = d_3 = s$.

- **Encryption:** The sender chooses $t \in \mathbb{Z}_p^*$ at random to encrypt a message $M \in \mathbb{G}_2$ under a set of attributes ω'. Compute $E = (\omega', E_1, E_2, E_3, E_4, E_5)$ as

$$(\omega', g^t, Z^t, X^t, M \cdot e(g_1, g_2)^t, \{T(i)^t\}_{i\in\omega'}).$$

- **Decryption:** Let E be a valid encryption of M under ω'. E can be decrypted by a user with the private key $d_{id,\omega}$, where $|\omega \cap \omega'| \geq d$. First compute $E'_1 = E_1^{id} \cdot E_2 = (g^{id} \cdot Z)^t$ and $E'_5 = \prod_{i\in S}(\frac{e(D_i,E_1)}{e(F_i,T(i)^t)})^{\Delta_{i,S}(0)}$, where S be an arbitrary d-element subset of $\omega \cap \omega'$. Next decrypt E as:

$$M = E_4 \cdot \frac{e(E_1, h)^{d_3} \cdot e(E'_1, d_2)}{e(d_1, E_3) \cdot E'_5},$$

- **Trace:** Takes as input a well-formed decryption key $d_{id,\omega} = (d_1, d_2, d_3, d_4)$, this algorithm outputs the decryption key family number $n_F = d_3$.

3.2 Analysis of the Construction

If the cryptosystem is operated as specified, we have $E'_5 = e(g^t, g_2)^{y-y_1}$ and

$$\begin{aligned} & E_4 \cdot \frac{e(E_1, h)^{d_3} \cdot e(E'_1, d_2)}{e(d_1, E_3) \cdot E'_5} \\ = & E_4 \cdot \frac{e(g^t, h)^s \cdot e((g^{id}Z)^t, X^r)}{e((g_2^{y_1}h^s)^{\frac{1}{x}} \cdot (g^{id}Z)^r, X^t) \cdot e(g^t, g_2)^{y-y_1}} \\ = & E_4 \cdot \frac{1}{e(g^{y_1}, g_2^t) \cdot e(g^{y-y_1}, g_2^t)} \\ = & M. \end{aligned}$$

The above construction is based on the large universe construction in [20]. However, we notice that one can use our approach to construct an A-ABE based on the large universe construction of KP-ABE [8]. Now we present the security proofs for our construction.

Theorem 1. *The above construction is IND-SS-CPA secure under the MBDDH assumption.*

Proof. Let $\mathcal{A}$ be an adversary against our scheme with advantage ϵ. We build a simulator $\mathcal{B}$ that can solve a MBDDH instance with advantage $\frac{\epsilon}{2}$. First, let the challenger set the groups $\mathbb{G}_1$ and $\mathbb{G}_2$ with an efficient bilinear map e. Second, the challenger flips a fair binary coin μ outside of $\mathcal{B}$'s view. If $\mu = 0$, the challenger sets $(A, B, C, C', D) = (g^a, g^b, g^c, g^{c^2}, e(g, g)^{abc})$, otherwise it sets $(A, B, C, C', D) = (g^a, g^b, g^c, g^{c^2}, e(g, g)^z)$ for random a, b, c, $z \in \mathbb{Z}_p^*$. The simulator proceeds as follows:

- **Init.** $\mathcal{B}$ receives the target set of attributes ω^* from $\mathcal{A}$.

- **Setup.** $\mathcal{B}$ chooses $\alpha, \beta, \gamma, y_1 \in \mathbb{Z}_p^*$ and sets $h = A^\alpha, X = C^\beta, Z = X^\gamma, K = e(A, B)$ and $K_1 = e(g, B^{y_1})$ (we have implicitly set $g_1 = A, g_2 = B$). $\mathcal{B}$ chooses a random n degree polynomial $f(x)$ and computes an n degree polynomial $u(x)$ such that $u(x) = -x^n$ for all $x \in \omega^*$ and $u(x) \neq -x^n$ for $x \notin \omega^*$. For $i \in \{1, \ldots, n+1\}$, $\mathcal{B}$ sets $t_i = g_2^{u(i)}g^{f(i)}$. Now $\mathcal{B}$ gives the public parameters to $\mathcal{A}$.

- **Phase 1.** Suppose $\mathcal{A}$ requests a private key (id, ω). We assume that id is non zero. The simulator will receive an element $R = h^{s_0} \cdot X^\theta$ with a WI proof of knowledge of (s_0, θ) from $\mathcal{A}$. If the proof succeeds to be verified, $\mathcal{B}$ prepares the private key as follows. Firstly, it chooses randomly $s_1 \in \mathbb{Z}_p^*$ and defines $W = Y_1 \cdot R \cdot h^{s_1}$, $d'_3 = s_1$. Then, d'_1 and d'_2 are generated as:

$$(d'_1, d'_2) = ((g^{id} \cdot Z)^{r'} \cdot W^{-\frac{\gamma}{id}}, X^{r'} \cdot W^{-\frac{1}{id}}),$$

where r' is chosen randomly from $\mathbb{Z}_p^*$. If we let $\tilde{r}' = r' - \frac{\log_g(W)}{(c\beta)\cdot id}$, d'_1 and d'_2 have the correct distributions. We have

$$\begin{aligned} d'_1 &= W^{1/(c\beta)} \cdot (g^{id} \cdot Z)^{\tilde{r}'} \\ &= W^{1/(c\beta)} \cdot (g^{id} \cdot X^\gamma)^{r'} \cdot (g^{id} \cdot X^\gamma)^{-\frac{w}{c\beta\cdot id}} \\ &= (g^{id} \cdot Z)^{r'} \cdot W^{-\frac{\gamma}{id}}, \end{aligned}$$

and $d'_2 = X^{\tilde{r}'} = X^{r'} \cdot (g^{c\beta})^{-\frac{w}{c\beta\cdot id}} = X^{r'} \cdot W^{-\frac{1}{id}}$, where $w = \log_g(W)$. To generate d'_4, $\mathcal{B}$ proceeds as follows. First, define three sets $\Gamma = \omega^* \cap \omega$, Γ' such that $\Gamma \subseteq \Gamma' \subseteq \omega$ and $|\Gamma'| = d - 1$, and $S = \Gamma' \cup \{0\}$. For $i \in \Gamma'$, Define $D_i = g_2^{\lambda_i}T(i)^{r_i}, F_i = g^{r_i}$, where r_i, λ_i are chosen randomly in $\mathbb{Z}_p^*$. For $i \in \omega - \Gamma'$, $\mathcal{B}$ chooses $r'_i \in \mathbb{Z}_p^*$ and defines D_i as

$$\Big(\prod_{j\in\Gamma'} g_2^{\lambda_j \Delta_{j,S}(i)}\Big)\big((g_1 g^{-y_1})^{\frac{-f(i)}{i^n+u(i)}}(g_2^{i^n+u(i)}g^{f(i)})^{r'_i}\big)^{\Delta_{0,S}(i)},$$

and $F_i = ((g_1 g^{-y_1})^{\frac{-1}{i^n+u(i)}} g^{r'_i})^{\Delta_{0,S}(i)}$. Let $r_i = (r'_i - \frac{a-y_1}{i^n+u(i)})\Delta_{0,S}(i)$, the above values have the correct distributions. D_i is equal to

$$\begin{aligned}
&\big(\prod_{j\in\Gamma'} g_2^{\lambda_j \Delta_{j,S}(i)}\big)\big((g_1 g^{-y_1})^{\frac{-f(i)}{i^n+u(i)}}(g_2^{i^n+u(i)} g^{f(i)})^{r'_i}\big)^{\Delta_{0,S}(i)} \\
&= \big(\prod_{j\in\Gamma'} g_2^{\lambda_j \Delta_{j,S}(i)}\big)\big(g^{\frac{-(a-y_1)f(i)}{i^n+u(i)}}(g_2^{i^n+u(i)} g^{f(i)})^{r'_i}\big)^{\Delta_{0,S}(i)} \\
&= \big(\prod_{j\in\Gamma'} g_2^{\lambda_j \Delta_{j,S}(i)}\big) g_2^{(a-y_1)\Delta_{0,S}(i)}\big((g_2^{i^n+u(i)} g^{f(i)})^{r_i}\big)^{\Delta_{0,S}(i)} \\
&= g_2^{q(i)} T(i)^{r_i}
\end{aligned}$$

and

$$\begin{aligned}
F_i &= ((g_1 g^{-y_1})^{\frac{-1}{i^n+u(i)}} g^{r'_i})^{\Delta_{0,S}(i)} \\
&= (g^{\frac{-(a-y_1)}{i^n+u(i)}} g^{r'_i})^{\Delta_{0,S}(i)} = g^{r_i}.
\end{aligned}$$

Finally, $d'_{id,\omega}$ is returned to $\mathcal{A}$.

- **Challenge.** $\mathcal{A}$ will submit two challenge messages M_1 and M_0 to the simulator. The simulator chooses randomly $\rho \in \mathbb{Z}_p^*$ and flips a fair binary coin, ν. It returns the challenge ciphertext of an encryption of M_ν as:

  $$E^* = (\omega^*, C^\rho, C'^{\beta\gamma\rho}, C'^{\beta\rho}, M_\nu D^\rho, \{C^{\rho f(i)}\}_{i\in\omega^*}).$$

  Let $t = c\rho$. If $D = e(g,g)^{abc}$, the above ciphertext is a valid encryption of M_ν. Otherwise, if D is random, E_4^* gives no information about M_ν.

- **Phase 2.** The simulator proceeds as it did in Phase 1.

- **Guess.** $\mathcal{A}$ will submit a guess ν' of ν. If $\nu = \nu'$ the simulator will output $\mu' = 0$. Otherwise it will output $\mu' = 1$.

The advantage of the simulator in solving MBDDH instance is $\frac{\epsilon}{2}$. □

Theorem 2. *The construction is secure in the FindKey game in the information theoretic sense.*

The above theorem directly follows from [12], due to the uses of the perfect hiding property of Pedersen's commitment [18] and the perfect witness indistinguishability of the protocol [16].

Theorem 3. *The construction is secure in the Compute-NewKey game under the MDH assumption.*

Proof. Let $\mathcal{A}$ be an adversary against the Compute-NewKey game. We build a simulator $\mathcal{B}$ which can find $h^{1/x}$ given $(g, h, X = g^x)$. $\mathcal{B}$ proceeds as follows:

- **Init.** $\mathcal{B}$ receives the target identity id^* from $\mathcal{A}$.

- **Setup.** To prepare the public parameters. First, $\mathcal{B}$ takes X, h from the MDH instance. Second, it chooses $\alpha, \beta, \gamma \in \mathbb{Z}_p^*$, $t_1, \ldots, t_{n+1} \in \mathbb{G}_1$ and sets $K = e(g^\alpha, g^\beta), Z = g^{-id^*} X^\gamma$. $\mathcal{B}$ chooses ρ, s'_1 and defines $Y_1 = X^\rho h^{-s'_1}$ and computes K_1. Finally, $\mathcal{B}$ gives the public parameters to $\mathcal{A}$.

- **Key Generation.** Suppose $\mathcal{A}$ requests a private key (id, ω). The simulator will receive an element $R = h^{s_0} \cdot X^\theta$ with a WI proof of knowledge of (s_0, θ) from $\mathcal{A}$. If the proof succeeds to be verified, $\mathcal{B}$ prepares the private key as follows:

  – For $id \neq id^*$, $\mathcal{B}$ picks $s_1, r' \in \mathbb{Z}_p^*$ at random and defines $W = Y_1 R h^{s_1}$, $d'_3 = s_1$. Then, d'_1, d'_2 can be generated as

  $$(d'_1, d'_2) = ((g^{id} Z)^{r'} W^{-\frac{\gamma}{id-id^*}}, X^{r'} W^{-\frac{1}{id-id^*}}).$$

  If we let $\tilde{r}' = r' - \frac{\log_g(W)}{x\cdot(id-id^*)}$, the above components have the correct distribution. Additionally, d'_4 can be generated as follows. By our setting of Y_1, we have $y_1 = \frac{x\rho - s'_1 \log_g h}{\beta}$. It first chooses an arbitrary subset Γ of ω such that $|\Gamma| = d-1$. For $i \in \Gamma$, it chooses randomly $\lambda_i, r_i \in \mathbb{Z}_p^*$ and sets $D_i = g_2^{\lambda_i} T(i)^{r_i}$, $F_i = g^{r_i}$. We implicitly select a $d-1$ degree polynomial $q(x)$ with $q(i) = \lambda_i$ and $q(0) = \alpha - \frac{x\rho - s'_1 \log_g h}{\beta}$. For $i \in \omega - \Gamma$, it chooses $r_i \in \mathbb{Z}_p^*$ and sets

  $$D_i = \big(\prod_{j\in\Gamma} g_2^{\lambda_j \Delta_{j,S}(i)}\big)\big(g_2^\alpha X^{-\rho} h^{s'_1}\big)^{\Delta_{0,S}(i)} T(i)^{r_i},$$

  and $F_i = g^{r_i}$. Notice that the above values have correct distributions.

  – For $id = id^*$, $\mathcal{B}$ uses the knowledge extractor to find (s_0, θ) of R by rewinding $\mathcal{A}$. It sets $s_1 = s'_1 - s_0$. Now it chooses $r \in \mathbb{Z}_p^*$ and computes

  $$(d'_1, d'_2, d'_3) = (g^{\rho+\theta} \cdot (g^{id^*} \cdot Z)^r, X^r, s_1).$$

  For d'_1, we have $(Y_1 R h^{s_1})^{1/x} \cdot (g^{id^*} \cdot Z)^r = g^{\rho+\theta} \cdot (g^{id^*} \cdot Z)^r$. The above values have correct distributions. To prepare d'_4, $\mathcal{B}$ does as the above description for the case of $id \neq id^*$.

  Finally, $d'_{id,\omega}$ is returned to $\mathcal{A}$.

- **New Key Computation.** At this point, $\mathcal{A}$ outputs two well-formed private keys for id^*, i.e., $d^{(1)}_{id^*,\omega} = (d_1^{(1)}, d_2^{(1)}, d_3^{(1)}, d_4^{(1)})$ and $d^{(2)}_{id^*,\omega} = (d_1^{(2)}, d_2^{(2)}, d_3^{(2)}, d_4^{(2)})$, such that $s = d_3^{(1)} \neq d_3^{(2)} = s'$. Then, we have $d_1^{(1)} = (Y_1 h^s)^{1/x} \cdot X^{\alpha r'}, d_2^{(1)} = X^r$ and $d_1^{(2)} = (Y_1 h^{s'})^{1/x} \cdot X^{\alpha r'}, d_2^{(2)} = X^{r'}$, where $r, r' \in \mathbb{Z}_p^*$ are unknown to $\mathcal{B}$. Now, the simulator can compute $h^{1/x} = \big(\frac{d_1^{(1)}/(d_2^{(1)})^\alpha}{d_1^{(2)}/(d_2^{(2)})^\alpha}\big)^{\frac{1}{s-s'}}$.

This completes the proof. □

4 Accountable Authority Ciphertext Policy ABE

This construction is built on the ciphertext policy ABE scheme in [14]. We assume n be the maximum size attribute set for a user and N be the set of $\{1, 2, \ldots, n\}$. We refer to attributes i and their negations $\neg i$ as literals. The ciphertext policy achieved is AND gate access structure $W = \bigwedge_{i \in I} \underline{i}$, where $I \in N$ and every i is a literal, i.e., i or $\neg i$.

4.1 Description

- **Setup:** First, generate a set of pairing groups at the security level κ. Next, choose randomly $x, y, y_1, t_1, \ldots, t_{3n} \in \mathbb{Z}_p^*$, a generator g of $\mathbb{G}_1$ and $h, Z \in \mathbb{G}_1$. Set $X = g^x, Y_1 = g^{y_1}, K = e(g,g)^y, K_1 = e(g, Y_1)$ and $T_i = g^{t_i}$ for $i \in \{1, \ldots, 3N\}$. Finally, set the master private key msk and the master public key mpk as:
$$msk = \{x, y, y_1, t_1, \ldots, t_{3n}\},$$
$$mpk = \{X, h, Z, K, K_1, T_1, \ldots, T_{3n}\}.$$

- **KeyGen:** To generate a private key for a user U with (id, ω). The following protocol will be executed between U and the authority.
  - U chooses $s_0, \theta \in \mathbb{Z}_p^*$ at random, and provides a commitment $R = h^{s_0} \cdot X^{\theta}$ with an interactive witness indistinguishable proof of knowledge of the (s_0, θ) to the authority. In addition, U retains (s_0, θ).
  - The authority verifies the proof of knowledge, outputs $\perp$ if fails. Otherwise, it selects $r_1, \ldots, r_n \in \mathbb{Z}_p^*$ such that $\sum_{i=1}^{n} r_i = y - y_1$. The authority first generates d_4'. For each $i \in N$, set $D_i = g^{\frac{r_i}{t_i}}$ if $i \in \omega$; otherwise, let it be $g^{\frac{r_i}{t_{n+i}}}$. In addition, set $F_i = g^{\frac{r_i}{t_{2n+i}}}$ for all $i \in N$. Now it chooses randomly $s_1, r' \in \mathbb{Z}_p^*$ and returns $d'_{id,\omega} = (d_1', d_2', d_3', d_4')$ as
$$((g^{y_1} R h^{s_1})^{\frac{1}{x}} \cdot (g^{id} Z)^{r'}, X^{r'}, s_1, \{D_i, F_i\}_{i \in N}).$$
  - U chooses $r'' \in \mathbb{Z}_p^*$ at random and computes $d_{id,\omega} = (d_1, d_2, d_3, d_4)$ as $(d_1'/g^{\theta} \cdot (g^{id} Z)^{r''}, d_2' \cdot X^{r''}, d_3' + s_0, d_4')$, which should equal
$$((g^{y_1} h^{s})^{\frac{1}{x}} \cdot (g^{id} Z)^{r}, X^{r}, s, \{D_i, F_i\}_{i \in N}),$$
where $r = r' + r''$ and $s = s_0 + s_1$. Now U checks $d_{id,\omega}$ as follows. First, the consistence of every element of d_4 should be checked. For each $i \in N$, compute $R_i = e(D_i, T_i)$ if $i \in \omega$, otherwise, compute $R_i = e(D_i, T_{n+i})$. Set $R_0 = \prod_{i \in N} R_i$. In addition, compute $R_i' = e(F_i, T_{2n+i})$ for $i \in N$ and check $R_i = R_i'$ for $i \in N$. Next, check
$$\frac{e(d_1, X)}{e(g,h)^{d_3} \cdot e(g^{id} Z, d_2)} = K_1,$$
and $R_0 \cdot K_1 = K$. U outputs $\perp$ if any check fails. Otherwise, U sets his private key as $d_{id,\omega}$ and the key family number as $n_F = d_3 = s$.

- **Encryption:** The sender chooses $t \in \mathbb{Z}_p^*$ at random to encrypt a message $M \in \mathbb{G}_2$ under $W = \bigwedge_{i \in I} \underline{i}$. For each $i \in I$, let E_i be T_i^t if $\underline{i} = i$, or be T_{n+i}^t if $\underline{i} = \neg i$. For each $i \in N \setminus I$, let E_i be T_{2n+i}^t. Compute $C = (W, C_1, C_2, C_3, C_4, C_5)$ as
$$(W, g^t, Z^t, X^t, M \cdot K^t, \{E_i\}_{i \in N}).$$

- **Decryption:** Let C be a valid encryption of M under $W = \bigwedge_{i \in I} \underline{i}$. C can be decrypted by a user with the private key $d_{id,\omega}$, where ω satisfies W. First compute $C_1' = C_1^{id} \cdot C_2 = (g^{id} \cdot Z)^t$. Then compute
$$C_5' = \prod_{\underline{i} = i \wedge i \in \omega} e(D_i, E_i) \prod_{\underline{i} = \neg i \wedge i \notin \omega} e(D_i, E_i) \prod_{i \notin I} e(F_i, E_i).$$
Next decrypt C as:
$$M = C_4 \cdot \frac{e(C_1, h)^{d_3} \cdot e(C_1', d_2)}{e(d_1, C_3) \cdot C_5'},$$

- **Trace:** Takes as input a well-formed decryption key $d_{id,\omega} = (d_1, d_2, d_3, d_4)$, this algorithm outputs the decryption key family number $n_F = d_3$.

4.2 Analysis of the Construction

If the cryptosystem is operated as specified, we have $C_5' = e(g^t, g)^{y - y_1}$ and
$$\begin{aligned} & C_4 \cdot \frac{e(C_1, h)^{d_3} \cdot e(C_1', d_2)}{e(d_1, C_3) \cdot C_5'} \\ = & C_4 \cdot \frac{e(g^t, h)^s \cdot e((g^{id} Z)^t, X^r)}{e((g^{y_1} h^s)^{\frac{1}{x}} \cdot (g^{id} Z)^r, X^t) \cdot e(g^t, g)^{y - y_1}} \\ = & C_4 \cdot \frac{1}{e(g^{y_1}, g^t) \cdot e(g^{y - y_1}, g^t)} \\ = & M. \end{aligned}$$

Now we present the security proofs for our second construction.

Theorem 4. *The above construction is IND-SS-CPA secure under the MBDDH assumption.*

Proof. Let $\mathcal{A}$ be an adversary against our scheme with advantage ϵ. We build a simulator $\mathcal{B}$ that can solve a MBDDH instance with advantage $\frac{\epsilon}{2}$. First, let the challenger set the groups $\mathbb{G}_1$ and $\mathbb{G}_2$ with an efficient bilinear map e. Second, the challenger flips a fair binary coin μ outside of $\mathcal{B}$'s view. If $\mu = 0$, the challenger sets $(A, B, C, C', D) = (g^a, g^b, g^c, g^{c^2}, e(g,g)^{abc})$; otherwise it sets $(A, B, C, C', D) = (g^a, g^b, g^c, g^{c^2}, e(g,g)^z)$ for random a, b, c, $z \in \mathbb{Z}_p^*$. The simulator proceeds as follows:

- **Init.** $\mathcal{B}$ receives the target structure $W^* = \bigwedge_{i \in I} \underline{i}$ from $\mathcal{A}$.

- **Setup.** $\mathcal{B}$ chooses $\alpha, \beta, \gamma, \delta \in \mathbb{Z}_p^*$ and sets $K = e(A,B), K_1 = e(g, B^\delta), h = A^\alpha, X = C^\beta, Z = X^\gamma$. For each $i \in N$, $\mathcal{B}$ selects $\alpha_i, \beta_i, \gamma_i \in \mathbb{Z}_p^*$. For $i \in I$, set $T_i = g^{\alpha_i}, T_{n+i} = B^{\beta_i}$ and $T_{2n+i} = B^{\gamma_i}$ if $\underline{i} = i$; otherwise, set $T_i = B^{\alpha_i}, T_{n+i} = g^{\beta_i}$ and $T_{2n+i} = B^{\gamma_i}$. For $i \notin I$, set $T_i = B^{\alpha_i}, T_{n+i} = B^{\beta_i}$ and $T_{2n+i} = g^{\gamma_i}$. Now $\mathcal{B}$ gives the public parameters to $\mathcal{A}$.

- **Phase 1.** Suppose $\mathcal{A}$ requests a private key (id, ω), where id is non zero and ω does not satisfy W^*. The simulator will receive an element $R = h^{s_0} \cdot X^\theta$ with a WI proof of knowledge of (s_0, θ) from $\mathcal{A}$. If the proof succeeds to be verified, $\mathcal{B}$ prepares the private key as follows. Firstly, it chooses randomly $s_1 \in \mathbb{Z}_p^*$, and defines $W = B^\delta \cdot R \cdot h^{s_1}$ and $d_3' = s_1$. Then, d_1' and d_2' are generated as:

$$(d_1', d_2') = ((g^{id} \cdot Z)^{r'} \cdot W^{-\frac{\gamma}{id}}, X^{r'} \cdot W^{-\frac{1}{id}}),$$

  where r' is chosen randomly from $\mathbb{Z}_p^*$. If we let $\tilde{r}' = r' - \frac{\log_g(W)}{(c\beta)\cdot id}$, d_1' and d_2' have the correct distributions. To generate d_4', $\mathcal{B}$ proceeds as follows. There exist $j \in I$ such that: either $j \in \omega$ and $\underline{j} = \neg j$, or $j \notin S$ and $\underline{j} = j$, due to ω does not satisfy W^*. For simplicity, assume $\mathcal{B}$ chooses such j: $j \notin S$ and $\underline{j} = j$. For each $i \in N, i \neq j$, $\mathcal{B}$ selects randomly $r_i' \in \mathbb{Z}_p^*$ and sets $r_i = r_i' b$. It sets $r_j = ab - b\delta - \sum_{i \in N \wedge i \neq j} r_i$. Then D_j and F_j can be computed as:

$$D_j = g^{\frac{r_j}{b\beta_j}} = A^{\frac{1}{\beta_j}} g^{\frac{-\delta - \sum_{i \in N \wedge i \neq j} r_i'}{\beta_j}},$$
$$F_j = g^{\frac{r_j}{b\gamma_j}} = A^{\frac{1}{\gamma_j}} g^{\frac{-\delta - \sum_{i \in N \wedge i \neq j} r_i'}{\gamma_j}}.$$

  For $i \neq j$, we have follows. When $i \in \omega$, set $D_i = B^{\frac{r_i'}{\alpha_i}}$ if $i \in I \wedge \underline{i} = i$ or set $D_i = g^{\frac{r_i'}{\alpha_i}}$ if $(i \in I \wedge \underline{i} = \neg i) \vee i \notin I$. When $i \notin \omega$, set $D_i = g^{\frac{r_i'}{\beta_i}}$ if $(i \in I \wedge \underline{i} = i) \vee i \notin I$ or set $D_i = B^{\frac{r_i'}{\beta_i}}$ if $i \in I \wedge \underline{i} = \neg i$. For F_i, we set $F_i = g^{\frac{r_i'}{\gamma_i}}$ if $i \in I$; otherwise, set $F_i = B^{\frac{r_i'}{\gamma_i}}$. It is easy to see the above values have correct distributions. Finally, $d'_{id,\omega}$ is returned to $\mathcal{A}$.

- **Challenge.** $\mathcal{A}$ will submit two challenge messages M_1 and M_0 to the simulator. The simulator chooses randomly $\rho \in \mathbb{Z}_p^*$ and flips a fair binary coin, ν. It returns the challenge ciphertext of an encryption of M_ν as:

$$C^* = (W^*, C^\rho, C'^{\beta\gamma\rho}, C'^{\beta\rho}, M_\nu D^\rho,$$
$$\{C^{\alpha_i} | i \in I \wedge \underline{i} = i\}, \{C^{\beta_i} | i \in I \wedge \underline{i} = \neg i\}, \{C^{\gamma_i} | i \notin I\}).$$

  Let $t = c\rho$. If $D = e(g,g)^{abc}$, the above ciphertext is a valid encryption of M_ν. Otherwise, if D is random, the challenge ciphertext gives no information about M_ν.

- **Phase 2.** The simulator proceeds as it did in Phase 1.

- **Guess.** $\mathcal{A}$ will submit a guess ν' of ν. If $\nu = \nu'$ the simulator will output $\mu' = 0$. Otherwise it will output $\mu' = 1$.

The advantage of the simulator in solving MBDDH instance is $\frac{\epsilon}{2}$. □

Theorem 5. *The construction is secure in the FindKey game in the information theoretic sense.*

This theorem directly follows from [12], due to the uses of the perfect hiding property of Pedersen's commitment [18] and the perfect witness indistinguishability of the protocol [16].

Theorem 6. *The construction is secure in the Compute-NewKey game under the MDH assumption.*

Proof. Let $\mathcal{A}$ be an adversary against the Compute-NewKey game. We build a simulator $\mathcal{B}$ which can find $h^{1/x}$ given $(g, h, X = g^x)$. $\mathcal{B}$ proceeds as follows:

- **Init.** $\mathcal{B}$ receives the target identity id^* from $\mathcal{A}$.

- **Setup.** To prepare the public parameters. First, $\mathcal{B}$ takes X, h from the MDH instance. Second, it chooses $\alpha, \gamma, t_1, \ldots, t_{3n} \in \mathbb{Z}_p^*$, and sets $K = e(g,g)^\alpha, Z = g^{-id^*} X^\gamma$ and $T(i) = g^{t_i}$ for $i \in \{1, \ldots, 3n\}$. $\mathcal{B}$ chooses ρ, s_1' and defines $Y_1 = X^\rho h^{-s_1'}$ and computes K_1. Finally, $\mathcal{B}$ gives the public parameters to $\mathcal{A}$.

- **Key Generation.** Suppose $\mathcal{A}$ requests a private key (id, ω). The simulator will receive an element $R = h^{s_0} \cdot X^\theta$ with a WI proof of knowledge of (s_0, θ) from $\mathcal{A}$. If the proof succeeds to be verified, $\mathcal{B}$ prepares the private key as follows:

  – For $id \neq id^*$, $\mathcal{B}$ picks $s_1, r' \in \mathbb{Z}_p^*$ at random and defines $W = Y_1 R h^{s_1}$, $d_3' = s_1$. Then, d_1', d_2' can be generated as $(d_1', d_2') = ((g^{id} Z)^{r'} W^{-\frac{\gamma}{id - id^*}}, X^{r'} W^{-\frac{1}{id - id^*}})$. If we let $\tilde{r}' = r' - \frac{\log_g(W)}{x \cdot (id - id^*)}$, the above components have the correct distribution. Additionally, d_4' can be generated as follows. It chooses randomly $j \in \omega$, $r_i \in \mathbb{Z}_p^*$ for $i \in N \wedge i \neq j$. Set $r_j = \alpha - x\rho + s_1' \log_g h - \sum_{i \in N \wedge i \neq j} r_i$. Then D_j and F_j can be computed as:

$$D_j = g^{\frac{\alpha - \sum_{i \in N \wedge i \neq j} r_i}{t_j}} X^{\frac{-\rho}{t_j}} h^{\frac{s_1'}{t_j}},$$
$$F_j = g^{\frac{\alpha - \sum_{i \in N \wedge i \neq j} r_i}{t_{2n+j}}} X^{\frac{-\rho}{t_{2n+j}}} h^{\frac{s_1'}{t_{2n+j}}}.$$

    For $i \neq j \wedge i \in N$, D_i and F_i can be computed as the description of the scheme. Notice that the above values have correct distributions.

  – For $id = id^*$, $\mathcal{B}$ uses the knowledge extractor to find (s_0, θ) of R by rewinding $\mathcal{A}$. It sets $s_1 = s_1' - s_0$. Now it chooses $r \in \mathbb{Z}_p^*$ and computes

$$(d_1', d_2', d_3') = (g^{\rho + \theta} \cdot (g^{id^*} \cdot Z)^r, X^r, s_1).$$

For d'_1, we have $(Y_1 R h^{s_1})^{1/x} \cdot (g^{id^*} Z)^r = g^{\rho+\theta} \cdot (g^{id^*} Z)^r$. Thus, the above values have correct distributions. To prepare d'_4, $\mathcal{B}$ does as the above description for the case of $id \neq id^*$.

Finally, $d'_{id,\omega}$ is returned to $\mathcal{A}$.

- **New Key Computation.** At this point, $\mathcal{A}$ outputs two well-formed private keys for id^*, i.e., $d^{(1)}_{id^*,\omega} = (d^{(1)}_1, d^{(1)}_2, d^{(1)}_3, d^{(1)}_4)$ and $d^{(2)}_{id^*,\omega} = (d^{(2)}_1, d^{(2)}_2, d^{(2)}_3, d^{(2)}_4)$, such that $s = d^{(1)}_3 \neq d^{(2)}_3 = s'$. Then, we have $d^{(1)}_1 = (Y_1 h^s)^{1/x} \cdot X^{\alpha r}, d^{(1)}_2 = X^r$ and $d^{(2)}_1 = (Y_1 h^{s'})^{1/x} \cdot X^{\alpha r'}, d^{(2)}_2 = X^{r'}$, where $r, r' \in \mathbb{Z}^*_p$ are unknown to $\mathcal{B}$. Now, the simulator can compute $h^{1/x} = \left(\frac{d^{(1)}_1/(d^{(1)}_2)^\alpha}{d^{(2)}_1/(d^{(2)}_2)^\alpha}\right)^{\frac{1}{s-s'}}$.

This completes the proof. □

5 Conclusions

To mitigate the key escrow problem existed in threshold attribute based encryption and ciphertext policy attribute based encryption, we introduce the notion of accountable authority attribute based encryption and present related constructions. In addition, we proof the security of our constructions in the standard model under some reasonable assumptions.

Acknowledgments

This study was supported by the National Natural Science Foundation of China (No. 61202493). The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] M. H. Au, Q. Huang, J. K. Liu, W. Susilo, D. S. Wong, and G. Yang, "Traceable and retrievable identity-based encryption," in *Applied Cryptography and Network Security*, pp. 94–110, 2008.

[2] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *IEEE Symposium on Security and Privacy*, pp. 321–334, 2007.

[3] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology - Crypto '01*, pp. 213–229, 2001.

[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] C. Gentry, "Practical identity-based encryption without random oracles," in *Advances in Cryptology - Eurocrypt '06*, pp. 445–464, 2006.

[6] V. Goyal, "Reducing trust in the pkg in identity based cryptosystems," in *Advances in Cryptology - Crypto '07*, pp. 430–447, 2007.

[7] V. Goyal, S. Lu, A. Sahai, and B. Waters, "Black-box accountable authority identity-based encryption," in *Proceedings of the 15th ACM Conference on Computer and Communications Security*, pp. 427–436, 2008.

[8] 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.

[9] E. Kiltz and Y. Vahlis, "Cca2 secure ibe: standard model efficiency through authenticated symmetric encryption," in *Topics in Cryptology - CT-RSA '08*, pp. 221–238, 2008.

[10] C. C. Lee, P. S. Chung, and M. S. Hwang, "A survey on attribute-based encryption schemes of access control in cloud environments," *International Journal of Network Security*, vol. 15, no. 4, pp. 231–240, 2013.

[11] J. Li, K. Ren, and K. Kim. "A2be: Accountable attribute-based encryption for abuse free access control,". Cryptology ePrint Archive, http://eprint.iacr.org/2009/118, 2009.

[12] B. Libert and D. Vergnaud, "Towards black-box accountable authority ibe with short ciphertexts and private keys," in *Public Key Cryptography - PKC '09*, pp. 235–255, 2009.

[13] B. Libert and D. Vergnaud, "Towards practical black-box accountable authority ibe: Weak black-box traceability with short ciphertexts and private keys," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 7189–7204, 2011.

[14] C. Ling and N. Calvin, "Provably secure ciphertext policy abe," in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, pp. 456–465, 2007.

[15] D. Nali, C. M. Adams, and A. Miri, "Using threshold attribute-based encryption for practical biometric-based access control.," *International Journal of Network Security*, vol. 1, no. 3, pp. 173–182, 2005.

[16] T. Okamoto, "Provably secure and practical identification schemes and corresponding signature schemes," in *Advances in Cryptology - Crypto '92*, pp. 31–53, 1993.

[17] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, pp. 195–203, 2007.

[18] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Advances in Cryptology - Crypto '91*, pp. 129–140, 1992.

[19] A. Sahai and H. Seyalioglu, "Fully secure accountable-authority identity-based encryption," in *Public Key Cryptography - PKC '11*, pp. 296–316, 2011.

[20] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology - Eurocrypt '05*, pp. 457–473, 2005.
[21] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in cryptology - Crypto '84*, pp. 47–53, 1985.
[22] Q. Tang and D. Ji, "Verifiable attribute based encryption.," *International Journal of Network Security*, vol. 10, no. 2, pp. 114–120, 2010.
[23] Y. Wang, K. Chen, and Y. Long, "Towards accountable authority attribute-based encryption," *High Technology Letters*, vol. 19, no. 1, pp. 82–87, 2013.
[24] Y. Wang, K. Chen, Y. Long, and Z. Liu, "Accountable authority key policy attribute-based encryption," *Science China Information Sciences*, vol. 55, no. 7, pp. 1631–1638, 2012.
[25] B. Waters, "Efficient identity-based encryption without random oracles," in *Advances in Cryptology - Eurocrypt '05*, pp. 114–127, 2005.

Yongtao Wang was born in 1980. He received his Ph.D. degree in Computer Science and Engineering from Shanghai Jiao Tong University, Shanghai, China, in 2011. He is currently a Research Assistant at China Information Technology Security Evaluation Center, Beijing, China. His research interests include information security and modern cryptography, etc.

Xiaonan Liu was born in Changchun city of Jilin province in June 1982.Graduated from College of Computer Science and Technology of Jilin University in June 2010 and received a doctors degree in the same year. The main research field is Computer Network, Wireless Communication Network and Information Security. She works in China Information Technology Security Evaluation Center, her position is Assistant Researcher. Dr. Liu published academic papers more than 10 articles, is the member of China Computer Federation and ACM. Articles have been published in publications such as Lecture Notes in Computer Science and Journal of Computational Information Systems.

Lulu Liang reveived the B.S and Ph.D. degree from Beijing Jiaotong University, China in 2007, and 2012 respectively. Since 2012, he has been with China Information Technology Security Evaluation Center as a researcher. His current research interests include wireless sensor networks, risk assessment, web security.

Weiduan Feng was born in 1982. He received his Ph.D. degree in Department of Mathematics from Shanghai Jiao Tong University, Shanghai, China, in 2010. He is currently an associate researcher at China Information Technology Security Evaluation Center, Beijing, China. His research interests include information security and modern cryptography, etc.

Guang Yang was born in 1980. She received her Ph.D. degree in Computer Application from Harbin Engineering University, Harbin, China, in 2009. She is currently an associate professor at China Information Technology Security Evaluation Center, Beijing, China. Her research interests include information security and wireless network security, etc.

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.femto.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].

2.5 Author benefits

No page charge is made.

Subscription Information

Individual subscriptions to IJNS are available at the annual rate of US$ 200.00 or NT 6,000 (Taiwan). The rate is US$600.00 or NT 19,800 (Taiwan) for institutional subscriptions. Price includes surface postage, packing and handling charges worldwide. Please make your payment payable to "Femto Technique Co., LTD." For detailed information, please refer to http://ijns.femto.com.tw or Email to ijns.publishing@gmail.com.