Security Analysis and Improvement of an Access Control Protocol for WBANs

Parvin Rastegari[1], Mojtaba Khalili[2], and Ali Sakhaei[3]
(Corresponding author: Parvin Rastegari)
Electrical and Computer Engineering Group, Golpayegan College of Engineering, Isfahan University of Technology[1]
Golpayegan, 87717-67498, Iran
Email: p.rastegari@iut.ac.ir
Department of Electrical Engineering, K. N. Toosi University of Technology[2]
Tehran, 1631714191, Iran
Department of Statistics, Payame Noor University (PNU)[3]
P.O.Box 19395-4697, Tehran, Iran
(Received Sept. 13, 2022; Revised and Accepted Jan. 28, 2023; First Online Feb. 17, 2023)[*]

Abstract

Since the emergence of wireless body area networks (WBANs) as a new technology in telemedicine, the challenges of secure communications in these networks have been noticed extensively; recently, Gao *et al.* have designed an efficient access control protocol for WBANs and claimed that their proposal could authenticate the physician to the patient and satisfy the confidentiality of the request message sent from the physician to the patient concurrently in a certificateless setting. Moreover, at the end of the protocol, the physician and the patient establish a session key for their following secure communications. They first designed a certificateless signcryption (CL-SC) scheme and then implied it to propose their access control protocol. In this paper, we design a key replacement attack against Gao *et al.*'s CL-SC scheme, in which the adversary can obtain the confidential request message sent from the physician to the patient. Moreover, based on our designed attack, the adversary can obtain the session key established by the physician for the following communications to the patient. Afterward, we fix the scheme to be secure against our proposed attacks.

Keywords: Access Control Protocol; Certificateless signcryption; ROM; Signcryption; WBANs

1 Introduction

New technologies for telemedicine have been extensively spread all over the world. The wireless body area network (WBAN) technology which was first proposed in 1996 [21], plays an important role in this field. In a WBAN, the human's vital data from body and environment parameters are collected via a wireless network including some low-power small sensors and actuators. The sensors might be wearable (such as neck, wrist, eye, arm, foot and body wears sensors) or implantable (such as cerebral pressure sensors, blood analyzer chips, heart sensors and so on). Due to the extensive applications of WBANs in various fields (e. g. medical, military, lifestyle, entertainment and so on), the IEEE 802.15.6 standard was presented to provide short-range reliable seamless communications with low-power consumption [13]. It is important to note that the efficiency in the sense of storage, computation and communication costs gets a lot of attention in WBANs because of the source-constrained low-power sensors and the bandwidth-limited communications.

The security aspects of WBANs have been in much attention in recent years. There are a lot of studies in this field and readers can refer to [7, 13] for a comprehensive review. The security requirements of WBANs depend on the applications in which they are used. As mentioned, one of the main applications of these networks is in telemedicine which helps us to replace the face-to-face interaction between the patient and the physician by monitoring patients? health-related parameters remotely, processing and sending them to medical databases. So, the corresponding medical advice can be transferred to the patients according to the received vital data. This remote interaction, can reduce both the medical costs and the risk of infection in infectious disease such as COVID-19 [9]. It is clear that the authentication of the patient and the medical team as well as the confidentiality of the transferred messages, to preserve the privacy of the patients, are very important in telemedicine applications.

A digital signature scheme is a well-known primitive which can be used to satisfy the authentication, the non-repudiation and the integrity of the messages in security protocols. Moreover, an encryption scheme satisfies the confidentiality of the messages in these protocols. In 1997,

[*]This article is an extended version of an ISCISC'21 paper [17]

Zheng proposed the concept of a signcryption scheme which provides the goals of the signature and encryption schemes concurrently in a way much more efficient than encrypting and signing messages separately [20]. A signcryption scheme is a useful primitive for designing access control protocols which manage the security and privacy of the networks by allowing only authorized users to access the network. There are a lot of studies on designing efficient access control protocols based on signcryption schemes in the literature [1, 4, 6, 8, 10–12], which many of them are proposed in the certificateless setting [6,8,10,11]. Certificateless public key cryptography was proposed by Al-Riyami and Paterson in 2003 to eliminate the problem of the management of huge number of certificates in conventional public key infrastructure as well as the key escrow problem in ID-Based public key cryptography [2]. In 2008, the idea of certificateless signcryption (CL-SC) was proposed by Barbosa and Farshim [3]. Since the introduction of CL-SC scheme in 2008, some works have been done to propose CL-SC schemes with provable security in the standard model (i. e. without the assumption of random oracles) [5,15,18,19]. However these schemes are not suitable for designing access control protocols for source-constrained low-power applications such as WBANs because of their heavy computation costs. Furthermore, as some of these schemes are attacked in the literature (such as the proposed attacks in [14,16]), one can see that if the games for the security proofs of schemes are not designed correctly, the security of them are not reliable at all even in the standard model. Based on these descriptions, almost all proposed CL-SC schemes for source-constrained, low-power and bandwidth-limited applications are content with the security proofs in the random oracle model (ROM) [6, 8, 10, 11].

Recently, Gao *et al.* have proposed an efficient CL-SC scheme and designed an access control for WBANs based on their proposal [6]. They proved the confidentiality (IND-CCA2) and unforgeability (EUF-CMA) of their proposal against both the key replacement attacker (which is denoted as $\mathcal{A}_I$ in the literature) and the malicious KGC attacker (which is denoted as $\mathcal{A}_{II}$ in the literature) in the random oracle model (ROM). In this paper:

- We design an attack which shows that the confidentiality of Gao *et al.*'s CL-SC scheme is vulnerable against the key replacement attack, in contrast to their claim. In the designed attack, a key replacement attacker $\mathcal{A}_I$ can obtain the signcrypted messages by replacing the public key of the receiver.
- According to our attack, $\mathcal{A}_I$ can also obtain the session key which is established by the physician for the next communications to the patient in Gao *et al.*'s access control protocol.
- We fix the Gao *et al.*'s scheme to be robust against the proposed attacks.

The remained of the paper is organized as follows. In Section 2, some required preliminaries are provided. In Section 3, an overview of Gao *et al.*'s CL-SC scheme and access control protocol is described. In Section 4, we propose our attacks against the Gao *et al.*'s proposals. In Section 5, we fix Gao *et al.*'s proposals to be robust against our designed attacks. In Section 6, a comparison between Gao *et al.*'s proposals and our improvements is provided. Finally, the paper is concluded in Section 7.

2 Preliminaries

2.1 Related Complexity Assumptions

Definition 1. *Suppose that G is a group of a prime order q and P is a generator of G. The Discrete Logarithm (DL) Problem is that on inputs $P, aP \in G$ (for unknown $a \in \mathbb{Z}_q^*$), compute $a \in \mathbb{Z}_q^*$.*

Definition 2. *The Decisional Diffie-Hellman (DDH) Problem is that on inputs $P, aP, bP, X \in G$ (for unknown $a, b \in \mathbb{Z}_q^*$), decide whether $X = abP$ (and returns $\gamma = 1$) or not (and returns $\gamma = 0$).*

2.2 CL-SC Scheme

2.2.1 Syntax

A key generation center (KGC), a sender (A) and a receiver (B) are three entities in a CL-SC scheme for an access control in a WBAN, which has five algorithms as follows [6]:

Setup. The KGC takes a security parameter k as input and outputs a master key α which is kept secret and the public parameters *params* which are published.

Partial Key Generation (ParKeyGen). When a user U with the identity ID_U registers to KGC, the KGC calculates a corresponding partial key $ParK_U$ and sends it to U.

Key Generatin (KeyGen). When the user U receives $ParK_U$ from KGC, he/she selects a secret value x_U randomly and calculates his/her public/private key pair (PuK_U, PrK_U) by the use of $ParK_U$ and x_U.

Signcryption. Suppose that the sender A wants to create a signcryption δ on a message m for the receiver B. A uses his/her private key PrK_A and the B's public key PuK_B to create such signcryption.

UnSigncryption. Upon receiving δ from A, B uses his/her private key PrK_B and the A's public key PuK_A to verify δ and obtain m.

2.2.2 Security Requirements

In a certificateless setting, there are two types of adversaries [2]:

- The type I adversary $\mathcal{A}_I$ who can replace public keys of the users, but does not have access to the master key which is called as the key replacement attacker. In adversarial models in the literature, $\mathcal{A}_I$ is assumed to have access to the Public-Key, Partial-Key, Replace-Public-Key, Private-Key, Signcrypt, Unsigncrypt and Hash oracles.

- The type II adversary $\mathcal{A}_{II}$ who has access to the master key, but is not able to replace public keys which is called as the malicious KGC attacker. In adversarial models in the literature, $\mathcal{A}_{II}$ is assumed to have access to the Public-Key, Private-Key, Signcrypt, Unsigncrypt and Hash oracles.

A CL-SC scheme must satisfy two basic security requirements, i. e. the confidentiality (in the sense of IND-CCA2) and the unforgeability (in the sense of EUF-CMA) against both $\mathcal{A}_I$ and $\mathcal{A}_{II}$. These security requirements are defined by four games described in [15].

2.3 Network Model of an Access Control for WBANs

According to the IEEE 802.15.6 standard, WBANs are deployed in a star topology in which a node located on the center of the body (e. g. the waist) plays the role of a controller [13] which can communicate to all sensor nodes directly. Sensor nodes which are located in, on or around the body, gather the vital information of the patient (Bob) and sends them to the central controller regularly. The controller sends the aggregated information to the receiver e. g. the physician (Dr. Alice) via the internet. Then the receiver (Dr. Alice) analyses the received information and sends the corresponding message e. g. the medical advice to the patient (Bob).

It is obvious that without considering the security aspects in this topology, the privacy of the patient (Bob) is not preserved at all, since everybody can access to his vital information and the corresponding medical advice from the insecure internet platform. Access control protocols provide solutions to overcome this problem by permitting to only authorized entities to have access to the private information. In [6], Gao *et al.* have proposed a CL-SC scheme and implied their proposal to design an access control protocol for WBANs. In their model, a service provider (SP) is responsible for deploying WBANs and registering all users (including the patients and the physicians) to the network. In fact, the SP plays the role of the KGC in the CL-SC scheme who generates the partial keys of the users as explained in Section 2.2.1. Figure 1 shows the star topology and the interactions between the SP and the users in Gao *et al.*'s network model.

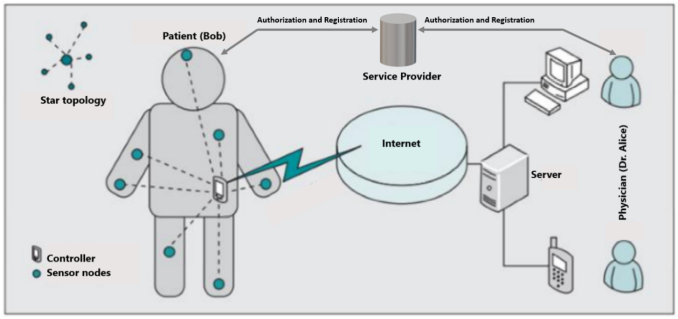

Figure 1: The star topology and the interactions between the SP and the users in Gao *et al.*'s model

3 Gao *et al.*'s Proposals

In [6], Gao *et al.* proposed a CL-SC scheme without bilinear pairing and proved the security of their proposal in the random oracle model (ROM). Afterwards, they designed an access control protocol for WBANs based on their CL-SC scheme. In this section, an overview of their CL-SC scheme and access control protocol is provided.

3.1 Gao *et al.*'s CL-SC Scheme

The algorithms of Gao *et al.*'s CL-SC scheme are as follows [6]:

Setup. On input a security parameter k, the SP selects a cyclic group G of a large prime order q, a generator P of G and three collision-resistant hash functions $H_1 : \{0,1\}^* \times G \longrightarrow \mathbb{Z}_q^*$, $H_2 : \{0,1\}^* \longrightarrow \mathbb{Z}_q^*$ and $H_3 : \mathbb{Z}_q^* \longrightarrow \{0,1\}^{l_0+|\mathbb{Z}_q^*|}$, where l_0 is the bit length of the message and $|\mathbb{Z}_q^*|$ is the bit length of an element in $\mathbb{Z}_q^*$. Afterwards, the SP picks a random $\alpha \in_R \mathbb{Z}_q^*$ as the system's master key and calculates the corresponding public key $P_{pub} = \alpha P$. At last, the SP publishes public parameters $params = \{G, q, P, P_{pub}, H_1, H_2, H_3\}$ and keeps α secret.

ParKeyGen. In this algorithm, an entity U sends his/her identity ID_U to the SP. The SP chooses a random value $r_U \in_R \mathbb{Z}_q^*$ and calculates $R_U = r_U P$ and $d_U = r_U + \alpha H_1(ID_U, R_U)$ and sends $ParK_U = (R_U, d_U)$ to U via a secure channel. The user U can verify the correctness of the received partial keys by checking whether the equation $R_U + H_1(ID_U, R_U)P_{pub} = d_U P$ holds or not.

KeyGen. The entity U picks a random $x_U \in_R \mathbb{Z}_q^*$, computes $X_U = x_U P$ and sets $PrK_U = (d_U, x_U)$ as his/her private key and $PuK_U = (R_U, X_U)$ as his/her public key.

Signcryption. Suppose that an entity A wants to create a signcryption δ on a message m for an entity B. A executes the following steps:

1) Picks a random value $\beta \in_R \mathbb{Z}_q^*$ and computes $T = \beta P$.

2) Sets $h_B = H_1(ID_B, R_B)$.
3) Calculates $V = \beta(X_B + R_B + h_B P_{pub})$.
4) Sets $h = H_2(m||T||ID_A||ID_B||X_A||X_B)$.
5) Calculates $S = (x_A + \beta)/(h + d_A + x_A)$.
6) Calculates $C = H_3(V) \oplus (m||S)$.
7) Returns $\delta = (S, C, T)$ and sends it to B.

UnSigncryption. Upon receiving a signcryption $\delta = (S, C, T)$ from A, B executes the following steps to verify δ and obtain m:

1) Calculates $V = (x_B + d_B)T$.
2) Calculates $m||S = H_3(V) \oplus C$ and consequently recovers m as the first l_0 bits of $m||S$.
3) Sets $h = H_2(m||T||ID_A||ID_B||X_A||X_B)$.
4) Sets $h_A = H_1(ID_A, R_A)$.
5) Verifies the signcryption by checking the following equality:

$$S(X_A + R_A + h_A P_{pub} + hP) = X_A + T.$$

If the above equality holds, B accepts m as a signcryption from A, otherwise B rejects it and returns $\perp$.

3.2 Gao *et al.*'s Access Control Protocol

Gao *et al.*'s proposed access control protocol is summarized in Figure 2. Their proposal has four phases as follows:

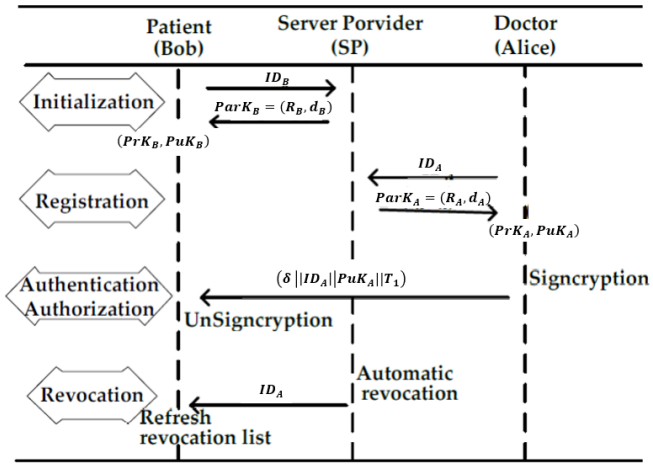

Figure 2: Gao *et al.*'s certificateless access control protocol

The Initialization Phase. In this phase, the SP who is the KGC introduced in Section 2.2.1, runs the Setup algorithm of the CL-SC scheme explained in Section 3.1, to generate *params* and α. The SP publishes *params* and keeps α secret. After deploying WBANs, when a user such as Bob requests SP for his partial key by sending his identity ID_B to the SP, it generates $ParK_B = (R_B, d_B)$ as explained in the ParKeyGen algorithm in Section 3.1 and sends it to Bob via a secure channel. Then Bob can produce his private and public keys (PrK_B, PuK_B) as explained in the KeyGen algorithm in Section 3.1.

The Registration Phase. In this phase, the receivers including the physician team such as Dr. Alice are registered by the SP. When Dr. Alice submits her identity ID_A to the SP, it checks whether the identity is valid or not. If not, the SP rejects the request. Otherwise, the SP sets an expiration date (ED) for Dr. Alice, generates $ParK_A = (R_A, d_A)$ as explained in the ParKeyGen algorithm in Section 3.1 and sends it to Dr. Alice via a secure channel. Then Dr. Alice can produce her private and public keys (PrK_A, PuK_A) as explained in the KeyGen algorithm in Section 3.1.

The Authentication Phase. When Dr. Alice wants to access the collected data of WBANs (e. g. the vital data of patient Bob), she first creates a signcryption $\delta = (S, C, T)$ on a request message m concatenated with a current timestamp T_1 (to prevent the replay attack), i. e. $m||T_1$. Then Dr. Alice sends $(\delta||ID_A||PuK_A||T_1)$ to Bob. Upon receiving the access request from Dr. Alice, Bob first checks whether $T_2 - T_1 \leq \Delta T$ or not, where T_2 is the current timestamp. If not, Bob rejects and terminates the session as a replay attack may be occurred. Otherwise, Bob runs the UnSigncryption algorithm by using his private key PrK_B. If the output of the UnSigncryption algorithm is $\perp$, Bob stops and terminates the session. Otherwise, Bob obtains m, accepts Dr. Alice's request, and starts to communicate with her using the session key $H_3(V)$ which is established between Bob and Dr. Alice.

The Revocation Phase. Due to the expiration date (ED), the SP revokes Dr. Alice access privilege by revoking her partial private key $ParK_A$ and sends ID_A to Bob which automatically makes Dr. Alice illegal to Bob. So, Bob stops the communication with Dr. Alice and she cannot be authenticated to Bob again, as her partial key is revoked by the SP.

4 Cryptanalysis of Gao *et al.*'s Proposals

4.1 Cryptanalysis of Gao *et al.*'s CL-SC Scheme

Gao *et al.* have claimed that their proposed CL-SC scheme is confidential (IND-CCA2) and unforgeable (EUF-CMA) against type I and type II adversaries $\mathcal{A}_I$ and $\mathcal{A}_{II}$, in the random oracle model (ROM), based on

CDH and DL assumptions in G (See Definition 1 and Definition 2) [6]. However, in this section, we design a key replacement attack against the confidentiality of Gao *et al.*'s CL-SC scheme. In our proposed attack, a type I adversary $\mathcal{A}_I$ can replace the public key of the receiver B to obtain all signcrypted messages sent from A to B without the knowledge of the corresponding private key of B. To this goal, $\mathcal{A}_I$ picks two random values $r_B^*, x_B^* \in_R \mathbb{Z}_q^*$ and computes:

$$R_B^* = r_B^* P,$$
$$X_B^* = x_B^* P - H_1(ID_B, R_B^*) P_{pub}.$$

Then $\mathcal{A}_I$ replaces the real public key of B, i. e. $PuK_B = (R_B, X_B)$, with $PuK_B^* = (R_B^*, X_B^*)$. By this public key replacement, A will use (R_B^*, X_B^*) to create a signcryption δ^* on a message m for B. In order to produce δ^*, A runs the following steps:

1) Picks a random value $\beta \in_R \mathbb{Z}_q^*$ and computes $T = \beta P$.
2) Sets $h_B^* = H_1(ID_B, R_B^*)$.
3) Calculates $V^* = \beta(X_B^* + R_B^* + h_B^* P_{pub})$.
4) Sets $h^* = H_2(m||T||ID_A||ID_B||X_A||X_B^*)$.
5) Calculates $S^* = (x_A + \beta)/(h^* + d_A + x_A)$.
6) Calculates $C^* = H_3(V^*) \oplus (m||S^*)$.
7) Returns $\delta^* = (S^*, C^*, T)$ and sends it to B.

By obtaining $\delta^* = (S^*, C^*, T)$ from the channel, $\mathcal{A}_I$ can easily calculate:

$$V^* = (x_B^* + r_B^*)T, \tag{1}$$

obtain:

$$m||S^* = H_3(V^*) \oplus C^*,$$

and recover m as the first l_0 bits of $m||S^*$. It is straightforward to check the correctness of Equation (1) as we have:

$$\begin{aligned} V^* &= \beta(X_B^* + R_B^* + h_B^* P_{pub}) \\ &= \beta(x_B^* P - H_1(ID_B, R_B^*) P_{pub} + r_B^* P + H_1(ID_B, R_B^*) P_{pub}) \\ &= \beta(x_B^* P + r_B^* P) = (x_B^* + r_B^*)\beta P = (x_B^* + r_B^*)T. \end{aligned}$$

As a result, $\mathcal{A}_I$ can deceive A to use $PuK_B^* = (R_B^*, X_B^*)$ instead of $PuK_B = (R_B, X_B)$ for generating a signcryption for B, and consequently obtain m and break the confidentiality of the scheme. So, the Gao *et al.*'s CL-SC scheme is not confidential against $\mathcal{A}_I$ in contrast to their claim.

4.2 Cryptanalysis of Gao *et al.*'s Access Control Protocol

Gao *et al.* have claimed that their protocol provides the confidentiality for future communications between Dr. Alice and Bob, i. e. no one can obtain the shared key between them. However, we will show that their claim isn't provided. As explained in the authentication phase of Gao *et al.*'s access control protocol in Section 3.2, upon receiving δ from Dr. Alice, Bob checks it and if it is valid, he obtains m. Then both Bob and Dr. Alice set the session key $H_3(V)$ for their future communications. Now, suppose that a type I adversary $\mathcal{A}_I$ has replaced the real public key of Bob $PuK_B = (R_B, X_B)$ with $PuK_B^* = (R_B^*, X_B^*)$ as explained in Section 4.1. So, Dr. Alice sets $H_3(V^*)$ as the session key for communicating with Bob, where:

$$V^* = \beta(X_B^* + R_B^* + h_B^* P_{pub}).$$

It is obvious that $\mathcal{A}_I$ can obtain the session key $H_3(V^*)$ by computing V^* as follows:

$$V^* = (x_B^* + r_B^*)T.$$

As a result, $\mathcal{A}_I$ can obtain the session key, communicate to Dr. Alice instead of Bob and access to all messages sent from Dr. Alice to Bob during the session. So, the confidentiality and the privacy of Bob will not be preserved at all.

5 Improvement of Gao *et al.*'s Proposals

In this section, we improve Gao *et al.*'s CL-SC scheme [6] to be robust against our proposed attack in Section 4.1. Then we provide the security proof of our improvement. Finally, we fix Gao *et al.*'s access control protocol based on our improved CL-SC scheme.

5.1 The Improved CL-SC Scheme

The algorithms of the improved CL-SC scheme are as follows:

Setup. It is similar to the Setup algorithm of Gao *et al.*'s CL-SC scheme, explained in Section 3.1.

ParKeyGen. In this algorithm, an entity U picks a random $x_U \in_R \mathbb{Z}_q^*$, computes $X_U = x_U P$ and sends X_U and ID_U to the SP. The SP chooses a random value $r_U \in_R \mathbb{Z}_q^*$, calculates $R_U = r_U P$ and $d_U = r_U + \alpha H_1(ID_U, R_U, X_U)$ and sends $ParK_U = (R_U, d_U)$ to U via a secure channel. The user U can verify the correctness of the received partial keys by checking whether the equation $R_U + H_1(ID_U, R_U, X_U)P_{pub} = d_U P$ holds or not.

KeyGen. The entity U sets $PrK_U = (d_U, x_U)$ as his/her private key and $PuK_U = (R_U, X_U)$ as his/her public key.

Signcryption. Suppose that an entity A wants to create a signcryption δ on a message m for an entity B. A executes the following steps:

1) Picks a random value $\beta \in_R \mathbb{Z}_q^*$ and computes $T = \beta P$.
2) Sets $h_B = H_1(ID_B, R_B, X_B)$.
3) Calculates $V = \beta(X_B + R_B + h_B P_{pub})$.
4) Sets $h = H_2(m||T||ID_A||ID_B||X_A||X_B)$.
5) Calculates

$$S = \frac{x_A + \beta}{h + d_A + x_A} = (x_A + \beta)(h + d_A + x_A)^{-1} \bmod q,$$

6) Calculates $C = H_3(V) \oplus (m||S)$.
7) Returns $\delta = (S, C, T)$ and sends it to B.

UnSigncryption. Upon receiving a signcryption $\delta = (S, C, T)$ from A, B executes the following steps to verify δ and obtain m:

1) Calculates $V = (x_B + d_B)T$.
2) Calculates $m||S = H_3(V) \oplus C$ and consequently recovers m as the first l_0 bits of $m||S$.
3) Sets $h = H_2(m||T||ID_A||ID_B||X_A||X_B)$.
4) Sets $h_A = H_1(ID_A, R_A, X_A)$.
5) Verifies the signcryption by checking the following equality:

$$S(X_A + R_A + h_A P_{pub} + hP) = X_A + T.$$

If the above equality holds, B accepts m as a signcryption from A, otherwise B rejects it and returns $\perp$.

Remark 5.1. *Note that in the improved scheme, in the ParKeyGen algorithm, d_U is computed as $d_U = r_U + \alpha H_1(ID_U, R_U, X_U)$ instead of $d_U = r_U + \alpha H_1(ID_U, R_U)$. Consequently, h_B and h_A are computed as $h_B = H_1(ID_B, R_B, X_B)$ and $h_A = H_1(ID_A, R_A, X_A)$ in the Signcryption and UnSigncryption algorithms. As a result, $\mathcal{A}_I$ cannot replace $PuK_B = (R_B, X_B)$ such as our proposed attack in Section 4.1.*

5.2 Analysis of the Improved CL-SC Scheme

5.2.1 Correctness

The correctness of the fixed scheme can be checked easily, as follows:

$$\begin{aligned} &R_U + H_1(ID_U, R_U, X_U)P_{pub} \\ &= r_U P + H_1(ID_U, R_U, X_U)\alpha P \\ &= (r_U + \alpha H_1(ID_U, R_U, X_U))P \\ &= d_U P, \end{aligned}$$

which shows the correctness of the partial key,

$$\begin{aligned} V &= (x_B + d_B)T \\ &= (x_B + r_B + \alpha H_1(ID_B, R_B, X_B))\beta P \\ &= \beta(x_B P + r_B P + H_1(ID_B, R_B, X_B)\alpha P) \\ &= \beta(X_B + R_B + h_B P_{pub}), \end{aligned}$$

which shows the correctness of the computed V in both sides, and:

$$\begin{aligned} &S(X_A + R_A + h_A P_{pub} + hP) \\ &= \frac{x_A + \beta}{h + d_A + x_A}(x_A P + r_A P + H_1(ID_A, R_A, X_A)\alpha P + hP) \\ &= \frac{x_A + \beta}{h + d_A + x_A}(x_A + r_A + H_1(ID_A, R_A, X_A)\alpha + h)P \\ &= \frac{x_A + \beta}{h + d_A + x_A}(x_A + d_A + h)P \\ &= (x_A + \beta)P = x_A P + \beta P = X_A + T, \end{aligned}$$

which shows the correctness of the verification part of the UnSigncryption algorithm.

5.2.2 Confidentiality

It can be shown that the improved CL-SC scheme is confidential (IND-CCA2) against type I and type II adversaries $\mathcal{A}_I$ and $\mathcal{A}_{II}$, in the random oracle model (ROM), based on the DDH assumption. The confidentiality against $\mathcal{A}_I$ and $\mathcal{A}_{II}$ are respectively defined according to Game I and Game II in [15], except that as our proof is provided in ROM, the adversary has access to Hash oracles, too.

Lemma 1. *If there is an adversary $\mathcal{A}_I$ who can win Game I in [15], with a non-negligible advantage ε, one can construct an algorithm $\mathcal{C}$, which can solve an instance of the DDH problem with an advantage at least $\frac{\varepsilon}{(n_q+1)^2}$, where n_q is the number of queries from Partial-Private-Key, Private-Key and Signcrypt oracles.*

Proof. Suppose that the algorithm $\mathcal{C}$ gets an instance $P, aP, bP, X \in G$, of a DDH problem and wants to decide whether $X = abP$ or not. First, $\mathcal{C}$ creates a list $\mathcal{L} = \{ID_U, h_{1,U}, h_{2,A,B,m,T}, T, V, h_{3,T}, d_U, x_U, r_U, X_U, R_U, c_U, ParK_U, PuK_U, PrK_U)\}$ which is initially empty. Then $\mathcal{C}$ plays Game I in [15] with $\mathcal{A}_I$ as follows:

Initialization: Given a security parameter k, $\mathcal{C}$ sets $P_{pub} = aP$. Then it produces other system parameters such that explained in the Setup algorithm of the improved scheme and sends $params = \{G, q, P, P_{pub}, H_1, H_2, H_3\}$ to $\mathcal{A}_I$. Note that as $P_{pub} = aP$, $\mathcal{C}$ does not know the corresponding master secret key $\alpha = a$.

Phase 1 Queries: $\mathcal{A}_I$ sends polynomially bounded number of queries to the Hash, Public-Key, Partial-Private-Key, Replace-Public-Key, Private-Key, Signcrypt and Unsigncrypt oracles and $\mathcal{C}$ responds to these queries as follows:

- H_1 queries: Receiving a $H_1(ID_U, R_U, X_U)$ query from $\mathcal{A}_I$, $\mathcal{C}$ first checks whether $h_{1,U}$ exists in $\mathcal{L}$ or not. If so, $\mathcal{C}$ picks it and sends it to $\mathcal{A}_I$. Otherwise, $\mathcal{C}$ randomly picks $c_U \in_R \{0,1\}$ such that $\Pr[c_U = 1] = \frac{1}{n_q+1}$ [6]. Then $\mathcal{C}$ acts as follows:
  - If $c_U = 0$, $\mathcal{C}$ randomly selects $h_{1,U} \in_R \mathbb{Z}_q^*$, sends it to $\mathcal{A}_I$ and inserts $c_U = 0$ and $h_{1,U}$ in $\mathcal{L}$.
  - If $c_U = 1$, $\mathcal{C}$ sets $h_{1,U} = K$ (a constant value), sends it to $\mathcal{A}_I$ and inserts $c_U = 1$ in $\mathcal{L}$.
- H_2 queries: Receiving a $H_2(m||T||ID_A||ID_B||X_A||X_B)$ query from $\mathcal{A}_I$, $\mathcal{C}$ first checks whether $h_{2,A,B,m,T}$ exists in $\mathcal{L}$ or not. If so, $\mathcal{C}$ picks and sends it to $\mathcal{A}_I$. Otherwise, $\mathcal{C}$ randomly selects $h_{2,A,B,m,T} \in_R \mathbb{Z}_q^*$, sends it to $\mathcal{A}_I$ and inserts it in $\mathcal{L}$.
- H_3 queries: Receiving a $(H_3(V), T)$ query from $\mathcal{A}_I$, $\mathcal{C}$ first checks whether $h_{3,T}$ exists in $\mathcal{L}$ or not. If so, $\mathcal{C}$ picks and sends it to $\mathcal{A}_I$. Otherwise, $\mathcal{C}$ randomly selects $h_{3,T} \in_R \{0,1\}^{l_0+|\mathbb{Z}_q^*|}$, sends it to $\mathcal{A}_I$ and inserts $T, V, h_{3,T}$ in $\mathcal{L}$.
- Public-Key queries: Receiving a PuK_U query from $\mathcal{A}_I$, $\mathcal{C}$ first checks whether PuK_U exists in $\mathcal{L}$ or not. If so, $\mathcal{C}$ picks and sends it to $\mathcal{A}_I$. Otherwise, $\mathcal{C}$ checks c_U in $\mathcal{L}$ and acts as follows:
  - If $c_U = 0$, $\mathcal{C}$ picks random values $x_U, r_U, z \in_R \mathbb{Z}_q^*$, computes $R_U = r_U P$, $X_U = x_U P$, $d_U = r_U + zH_1(ID_U, R_U, XU)$, sends $Puk_U = (R_U, X_U)$ to $\mathcal{A}_I$. Then $\mathcal{C}$ inserts $d_U, x_U, X_U, R_U, ParK_U = (R_U, d_U), PuK_U = (R_U, X_U), PrK_U = (d_U, x_U)$ in $\mathcal{L}$.
  - If $c_U = 1$, $\mathcal{C}$ randomly selects $x_U, r_U \in_R \mathbb{Z}_q^*$, computes $R_U = r_U P$ and $X_U = x_U P$, sets $PuK_U = (R_U, X_U)$, sends PuK_U to $\mathcal{A}_I$ and inserts $x_U, r_U, X_U, R_U, PuK_U = (R_U, X_U)$ in $\mathcal{L}$.
- Partial-Private-Key queries: Receiving a $ParK_U$ query from $\mathcal{A}_I$, $\mathcal{C}$ first checks whether $ParK_U$ exists in $\mathcal{L}$ or not. If so, $\mathcal{C}$ picks and sends it to $\mathcal{A}_I$. Otherwise, $\mathcal{C}$ checks c_U in $\mathcal{L}$ and acts as follows:
  - If $c_U = 0$, $\mathcal{C}$ runs a Public-Key query as explained. Then $\mathcal{C}$ returns $ParK_U$ to $\mathcal{A}_I$.
  - If $c_U = 1$, $\mathcal{C}$ aborts the simulation.
- Private-Key queries: Receiving a PrK_U query from $\mathcal{A}_I$, $\mathcal{C}$ first checks whether PrK_U exists in $\mathcal{L}$ or not. If so, $\mathcal{C}$ picks and sends it to $\mathcal{A}_I$. Otherwise, $\mathcal{C}$ checks c_U in $\mathcal{L}$ and acts as follows:
  - If $c_U = 0$, $\mathcal{C}$ runs a Public-Key query as explained. Then $\mathcal{C}$ returns PrK_U to $\mathcal{A}_I$.
  - If $c_U = 1$, $\mathcal{C}$ aborts the simulation.
- Replace-Public-Key queries: When $\mathcal{A}_I$ wants to replace a public key $PuK_U = (R_U, X_U)$ with a new public key $PuK'_U = (R'_U, X'_U)$, $\mathcal{C}$ applies this query and replaces PuK_U with PuK'_U in $\mathcal{L}$.
- Signcrypt queries: When $\mathcal{A}_I$ sends a signcrypt query on (ID_A, ID_B, m) to the Signcrypt oracle, $\mathcal{C}$ checks c_A and acts as follows:
  - If $c_A = 0$, $\mathcal{C}$ picks PrK_A from $\mathcal{L}$. Note that if PrK_A does not exist in $\mathcal{L}$, $\mathcal{C}$ can obtain it by a Private-Key query as explained before. Then $\mathcal{C}$ runs the Signcryption algorithm of the improved scheme to produce the signcryption δ on m from A to B and sends it to $\mathcal{A}_I$.
  - If $c_A = 1$, $\mathcal{C}$ aborts the simulation.
- Unsigncrypt queries: When $\mathcal{A}_I$ sends an Unsigncrypt query on $(ID_A, ID_B, \delta = (S, C, T))$ to the Unigncrypt oracle, $\mathcal{C}$ checks c_B and acts as follows:
  - If $c_B = 0$, $\mathcal{C}$ picks PrK_B from $\mathcal{L}$. Note that if PrK_B does not exist in $\mathcal{L}$, $\mathcal{C}$ can obtain it by a Private-Key query as explained before. Then $\mathcal{C}$ runs the UnSigncryption algorithm of the improved scheme to obtain m and sends it to $\mathcal{A}_I$.
  - If $c_B = 1$, $\mathcal{C}$ checks all the values of $h_{3,T}$ stored in $\mathcal{L}$ one by one to compute $m||S = H_3(V) \oplus C$ and obtain m. Then $\mathcal{C}$ picks the corresponding $h_{1,A}$ and $h_{2,A,B,m,T}$ (For each T) from $\mathcal{L}$ and verifies whether the equation $S(X_A + R_A + h_{1,A}P_{pub} + h_{2,A,B,m,T}P) = X_A + T$ holds or not. If there exist a $h_{3,T}$, for which this equation holds, $\mathcal{C}$ returns the corresponding m to $\mathcal{A}_I$. Otherwise, $\mathcal{C}$ returns $\perp$ to $\mathcal{A}_I$.

Challenge: In this step, $\mathcal{A}_I$ sends two equal lengths messages m_0 and m_1 and two identities ID_{A^*} and ID_{B^*} to $\mathcal{C}$. $\mathcal{C}$ first checks c_{B^*} in $\mathcal{L}$ and acts as follows:

- If $c_{B^*} = 0$, $\mathcal{C}$ aborts the simulation.
- If $c_{B^*} = 1$, $\mathcal{C}$ sets $T^* = bP$. Then $\mathcal{C}$ obtains $(T^*, V^*, H_3(V^*))$ from $\mathcal{L}$, chooses random values $S^* \in_R \mathbb{Z}_q^*$ and $\gamma^* \in_R \{0,1\}$, sets $C^* = H_3(V^*) \oplus (m_{\gamma^*}||S^*)$ and sends $\delta^* = (S^*, C^*, T^*)$ to $\mathcal{A}_I$.

Phase 2 Queries: $\mathcal{A}_I$ can again send polynomially bounded number of queries similar to that explained in Phase 1 Queries and $\mathcal{C}$ responds to these queries such explained.

Guess: In this step, $\mathcal{A}_I$ returns a guess $\gamma' \in \{0,1\}$ of γ^*.

At the end of the game, $\mathcal{C}$ acts as follows:

- If the simulation is aborted in any steps, $\mathcal{C}$ randomly selects $\gamma \in_R \{0,1\}$ as its guess of the answer to the DDH problem.

- Otherwise, if $\gamma' = \gamma^*$, $\mathcal{C}$ retrieves x_{B^*} and r_{B^*} from $\mathcal{L}$. Note that as the simulation is not aborted in the Challenge step, we have $c_{B^*} = 1$, so $\mathcal{C}$ can retrieve x_{B^*} and r_{B^*}. Furthermore, we have $h_{1,B^*} = K$, as $c_{B^*} = 1$. Then $\mathcal{C}$ obtains $(T^*, V^*, H_3(V^*))$ from $\mathcal{L}$ and checks whether the equation:

$$\frac{V^* - (x_{B^*} + r_{B^*})T^*}{K} = X, \tag{2}$$

holds or not. If so, $\mathcal{C}$ returns $\gamma = 1$, otherwise it returns $\gamma = 0$, as its answer to the DDH problem.

Note that as $c_{B^*} = 1$, $\mathcal{C}$ does not know $d_{B^*} = r_{B^*} + \alpha H_1(ID_{B^*}, R_{B^*}, X_{B^*})$, as $P_{pub} = aP$ and $\alpha = a$ is unknown to $\mathcal{C}$. Moreover, remember that $\mathcal{C}$ sets $T^* = bP$ in the Challenge step which indicates that $\beta = b$ which is also unknown to $\mathcal{C}$. In this case, if δ^* is actually a valid signcryption on m_{γ^*}, we have:

$$\begin{aligned}
&\frac{V^* - (x_{B^*} + r_{B^*})T^*}{K} \\
&= \frac{\beta(X_{B^*} + R_{B^*} + h_{1,B^*}P_{pub}) - (x_{B^*} + r_{B^*})bP}{K} \\
&= \frac{b(X_{B^*} + R_{B^*} + KaP) - b(X_{B^*} + R_{B^*})}{K} \\
&= abP,
\end{aligned}$$

So, if Equation (2) holds, it is implied that $X = abP$, then $\mathcal{C}$ returns $\gamma = 1$. Otherwise, it returns $\gamma = 0$ as its answer to the DDH problem.

Probability Analysis: Suppose that $\Pr[\mathcal{C} \text{ wins}]$ is the success probability of $\mathcal{C}$ to solve the DDH problem and $\Pr[\mathcal{A}_I \text{ wins}]$ is the success probability of $\mathcal{A}_I$ in the above game. Note that if the simulation is aborted in any steps, $\mathcal{C}$ randomly selects its guess $\gamma \in_R \{0,1\}$ as its answer to the DDH problrm, so $\Pr[\mathcal{C} \text{ wins}] = \frac{1}{2}$. If the advantage of $\mathcal{A}_I$ in winning the game is ε, i. e. $\Pr[\mathcal{A}_I \text{ wins}] \geq \frac{1}{2} + \varepsilon$, we have:

$$\begin{aligned}
\Pr[\mathcal{C} \text{ wins}] &= \Pr[\mathcal{C} \text{ wins}|\text{abort}]\Pr[\text{abort}] \\
&\quad + \Pr[\mathcal{C} \text{ wins}|\overline{\text{abort}}]\Pr[\overline{\text{abort}}] \\
&= \frac{1}{2}\Pr[\text{abort}] + \Pr[\mathcal{A}_I \text{ wins}]\Pr[\overline{\text{abort}}] \\
&\geq \frac{1}{2}(1 - \Pr[\overline{\text{abort}}]) + (\frac{1}{2} + \varepsilon)\Pr[\overline{\text{abort}}] \\
&= \frac{1}{2} + \varepsilon\Pr[\overline{\text{abort}}]
\end{aligned}$$

On the other hand, $\mathcal{C}$ will not abort if all the following independent events happen:

- E_1**:** $c_U = 0$ in all Partial-Private-Key and Private-Key queries.

- E_2**:** $c_A = 0$ in all Signcrypt queries.

- E_3**:** $c_{B^*} = 1$ in the Challenge step.

Defining E_i as the event of $c_U = 1$ in the i'th query and noting $\Pr[c_U = 1] = \frac{1}{n_q+1}$, we have:

$$\Pr[E_i] = \Pr[c_U = 1] = \frac{1}{n_q + 1}.$$

So we have:

$$\Pr[E_3] = \Pr[E_i] = \frac{1}{n_q + 1},$$

and:

$$\begin{aligned}
\Pr[E_1 \bigcap E_2] &= \Pr[\bigcap_{i=1}^{n_q} \bar{E}_i] = 1 - \Pr[\bigcup_{i=1}^{n_q} E_i] \\
&\geq 1 - \sum_{i=1}^{n_q} \Pr[E_i] = 1 - \frac{n_q}{n_q + 1}.
\end{aligned}$$

Therefore:

$$\begin{aligned}
\Pr[\overline{\text{abort}}] &\geq \Pr[E_1 \bigcap E_2 \bigcap E_3] = \Pr[E_1 \bigcap E_2].\Pr[E_3] \\
&\geq (1 - \frac{n_q}{n_q + 1})(\frac{1}{n_q + 1}) = \frac{1}{(n_q + 1)^2}
\end{aligned}$$

Finally we have:

$$\Pr[\mathcal{C} \text{ wins}] \geq \frac{1}{2} + \frac{\varepsilon}{(n_q + 1)^2}$$

In summary, if $\mathcal{A}_I$ wins the game with a non-negligible advantage ε (i. e. guesses γ' correctly with probability at least $\frac{1}{2} + \varepsilon$ for a non-negligible value of ε), then $\mathcal{C}$ can solve an instance of the DDH problem with a non-negligible advantage ε' (i. e. guess γ correctly with probability at least $\frac{1}{2} + \varepsilon'$), where $\varepsilon' \geq \frac{\varepsilon}{(n_q+1)^2}$ which is a contradiction with the DDH assumption in complexity theory. □

Lemma 2. *If there is an adversary $\mathcal{A}_{II}$ who can win Game II in [15], with a non-negligible advantage ε, one can construct an algorithm $\mathcal{C}$, which can solve an instance of the DDH problem with an advantage at least $\frac{\varepsilon}{(n_q+1)^2}$, where n_q is the number of queries from Private-Key and Signcrypt oracles.*

Proof. Suppose that the algorithm $\mathcal{C}$ gets an instance $P, aP, bP, X \in G$, of a DDH problem and wants to decide whether $X = abP$ or not. First, $\mathcal{C}$ creates a list $\mathcal{L} = \{ID_U, h_{1,U}, h_{2,A,B,m,T}, T, V, h_{3,T}, x_U, X_U, c_U, PuK_U, PrK_U)\}$ which is initially empty. Then $\mathcal{C}$ plays Game II in [15] with $\mathcal{A}_{II}$ as follows:

Initialization: Given a security parameter k, $\mathcal{C}$ generates system parameters such that explained in the Setup algorithm of the improved scheme and sends $params = \{G, q, P, P_{pub}, H_1, H_2, H_3\}$ to $\mathcal{A}_{II}$. Note that $\mathcal{C}$ knows the master secret key α, here.

Phase 1 Queries: $\mathcal{A}_{II}$ sends polynomially bounded number of queries to the Hash, Public-Key, Private-Key, Signcrypt and Unsigncrypt oracles and $\mathcal{C}$ responds to these queries as follows:

- H_1, H_2 and H_3 queries: $\mathcal{C}$ responds to these queries similar to that explained in the proof of Lemma 1.
- Public-Key queries: Receiving a PuK_U query from $\mathcal{A}_{II}$, $\mathcal{C}$ first checks whether PuK_U exists in $\mathcal{L}$ or not. If so, $\mathcal{C}$ picks and sends it to $\mathcal{A}_{II}$. Otherwise, $\mathcal{C}$ checks c_U in $\mathcal{L}$ and acts as follows:
  - If $c_U = 0$, $\mathcal{C}$ picks random values $x_U, r_U \in_R \mathbb{Z}_q^*$, computes $R_U = r_U P$, $X_U = x_U P$, $d_U = r_U + \alpha H_1(ID_U, R_U, XU)$, sends $Puk_U = (R_U, X_U)$ to $\mathcal{A}_{II}$. Then $\mathcal{C}$ inserts $PuK_U = (R_U, X_U), PrK_U = (d_U, x_U)$ in $\mathcal{L}$.
  - If $c_U = 1$, $\mathcal{C}$ sets $R_U = aP$. then it randomly selects $x_U \in_R \mathbb{Z}_q^*$, computes $X_U = x_U P$, sets $PuK_U = (R_U, X_U)$, sends PuK_U to $\mathcal{A}_{II}$ and inserts $x_U, X_U, PuK_U = (R_U, X_U)$ in $\mathcal{L}$.
- Private-Key, Signcrypt and Unsigncrypt queries: $\mathcal{C}$ responds to these queries similar to that explained in the proof of Lemma 1.

Challenge: This step is also similar to that in the proof of Lemma 1.

Phase 2 Queries: This step is also similar to that in the proof of Lemma 1.

Guess: In this step, $\mathcal{A}_I$ returns a guess $\gamma' \in \{0,1\}$ of γ^*.

At the end of the game, $\mathcal{C}$ acts as follows:

- If the simulation is aborted in any steps, $\mathcal{C}$ randomly selects $\gamma \in_R \{0,1\}$ as its guess of the answer to the DDH problem.
- Otherwise, if $\gamma' = \gamma^*$, $\mathcal{C}$ retrieves x_{B^*} from $\mathcal{L}$. Note that as the simulation is not aborted in the Challenge step, we have $c_{B^*} = 1$ and so $h_{1,B^*} = K$. Then $\mathcal{C}$ obtains $(T^*, V^*, H_3(V^*))$ from $\mathcal{L}$ and checks whether the equation:

$$V^* - (x_{B^*} + K\alpha)T^* = X, \tag{3}$$

holds or not. If so, $\mathcal{C}$ returns $\gamma = 1$, otherwise it returns $\gamma = 0$, as its answer to the DDH problem.

Note that $\mathcal{C}$ sets $T^* = bP$ in the Challenge step. So, $\beta = b$ which is unknown to $\mathcal{C}$. Moreover, as $c_{B^*} = 1$, we have $h_{1,B^*} = K$ and $R_{B^*} = aP$. In this case, if δ^* is actually a valid signcryption on m_{γ^*}, we have:

$$\begin{aligned} &V^* - (x_{B^*} + K\alpha)T^* \\ &= \beta(X_{B^*} + R_{B^*} + h_{1,B^*}P_{pub}) - (x_{B^*} + K\alpha)bP \\ &= b(X_{B^*} + aP + K\alpha P) - b(X_{B^*} + K\alpha P) \\ &= abP, \end{aligned}$$

So, if Equation (3) holds, it is implied that $X = abP$, then $\mathcal{C}$ returns $\gamma = 1$. Otherwise, it returns $\gamma = 0$ as its answer to the DDH problem.

Probability Analysis: It is similar to that explained in the proof of Lemma 1, except that the number of Partial-Private-Key and Replace-Public-Key queries are 0 here. □

Theorem 1. *The improved CL-SC scheme is confidential (IND-CCA2) against $\mathcal{A}_I$ and $\mathcal{A}_{II}$ based on the DDH assumption.*

Proof. the proof is directly implied from Lemma 1 and Lemma 2. □

5.2.3 Unforgeability

It can be shown that the improved CL-SC scheme is unforgeable (EUF-CMA) against type I and type II adversaries $\mathcal{A}_I$ and $\mathcal{A}_{II}$, in the random oracle model (ROM), based on the DL assumption. The unforgeability against $\mathcal{A}_I$ and $\mathcal{A}_{II}$ are respectively defined according to Game III and Game IV in [15], except that as our proof is provided in ROM, the adversary has access to Hash oracles, too.

Lemma 3. *If there is an adversary $\mathcal{A}_I$ who can win Game III in [15], with a non-negligible advantage ε, one can construct an algorithm $\mathcal{C}$, which can solve an instance of the DL problem with an advantage at least $\frac{\varepsilon p_{frk}}{(n_q+1)^2}$, where n_q is the number of queries from Partial-Private-Key, Private-Key and Signcrypt oracles and p_{frk} is the success probability of the adversary in Forking Lemma [6].*

Proof. Suppose that the algorithm $\mathcal{C}$ gets an instance $P, aP \in G$, of a DL problem and wants to obtain $a \in \mathbb{Z}_q^*$. First, $\mathcal{C}$ creates a list $\mathcal{L}$ such that explained in the proof of Lemma 1, which is initially empty. Then $\mathcal{C}$ plays Game III in [15] with $\mathcal{A}_I$ as follows:

Initialization: This step is similar to that in the proof of Lemma 1.

Queries: This step is similar to the Phase 1 Queries step in the proof of Lemma 1

Output: After a polynomially bounded number of queries, $\mathcal{A}_I$ outputs a valid signcryption $\delta^* = (S^*, C^*, T^*)$ on a message m^* from A^* to B^*.

At the end of the game, $\mathcal{C}$ acts as follows:

- If the simulation is aborted in any steps or $c_{A^*} = 0$, $\mathcal{C}$ aborts.
- Otherwise, $\mathcal{C}$ obtains m^* such that explained in the Unsigncrypt queries in the proof of Lemma 1. If δ^* is a valid signcryption on m^*, according to the Froking Lemma [6], $\mathcal{C}$ can get two valid signcryptions from A^* to B^* on m^* with the same random value β and different values of the random oracle h_{2,A^*,B^*,m^*,T^*}. So, $\mathcal{C}$ gets these two valid signcryptions with the same $T^* = \beta P$ and different values of $h = h_{2,A^*,B^*,m^*,T^*}$

and $h' = h'_{2,A^*,B^*,m^*,T^*}$. Denote these two valid signcryptions by $\delta_1 = (S_1, C_1, T^*)$ and $\delta_2 = (S_2, C_2, T^*)$. According to the step 5 of the signcryption algorithm, we have:

$$S_1(h + d_{A^*} + x_{A^*}) = x_{A^*} + \beta \bmod q,$$
$$S_2(h' + d_{A^*} + x_{A^*}) = x_{A^*} + \beta \bmod q.$$

So, we have:

$$S_1(h + d_{A^*} + x_{A^*}) = S_2(h' + d_{A^*} + x_{A^*}) \bmod q.$$

Note that as $c_{A^*} = 1$, $h_{1,A^*} = K$ and $d_{A^*} = r_{A^*} + \alpha h_{1,A^*} = r_{A^*} + aK$. Moreover, $P_{pub} = aP$ and the master secret key $\alpha = a$ is unknown to $\mathcal{C}$. So, we have:

$$S_1(h + r_{A^*} + aK + x_{A^*}) = S_2(h' + r_{A^*} + aK + x_{A^*}) \bmod q.$$

In the above equation all values except a is known to $\mathcal{C}$. So $\mathcal{C}$ can obtain a as its answer to the DL problem.

Probability Analysis: Suppose that Pr[$\mathcal{C}$ wins] is the success probability of $\mathcal{C}$ to solve the DL problem and Pr[$\mathcal{A}_I$ wins] is the success probability of $\mathcal{A}$ in the above game. If the advantage of $\mathcal{A}_I$ in winning the game is ε, i. e. Pr[$\mathcal{A}_I$ wins] $\geq \varepsilon$, we have:

$$\begin{aligned}\Pr[\mathcal{C}\text{ wins}] &= \Pr[\overline{\text{abort}} \bigcap \mathcal{A}_I \text{wins}] \\ &= \Pr[\overline{\text{abort}}].\Pr[\mathcal{A}_I \text{wins}] \\ &\geq \varepsilon.\Pr[\overline{\text{abort}}]\end{aligned}$$

On the other hand, $\mathcal{C}$ will not abort if all the following independent events happen:

- E_1**:** $c_U = 0$ in all Partial-Private-Key and Private-Key queries.
- E_2**:** $c_A = 0$ in all Signcrypt queries.
- E_3**:** $c_{A^*} = 1$.
- E_4**:** $\mathcal{C}$ can get two valid signcryptions with the same random tape and deifferent values of random oracles in Forking Lemma.

Similar to the explanations in the probability analysis of the proof of Lemma 1, we have:

$$\Pr[\overline{\text{abort}}] \geq \Pr[E_1 \bigcap E_2 \bigcap E_3 \bigcap E_4] \geq \frac{p_{frk}}{(n_q+1)^2},$$

So:

$$\Pr[\mathcal{C}\text{ wins}] \geq \frac{\varepsilon p_{frk}}{(n_q+1)^2}$$

In summary, if $\mathcal{A}_I$ wins the game with a non-negligible advantage ε (i. e. forges a valid signcryption with probability at least ε for a non-negligible value of ε), then $\mathcal{C}$ can solve an instance of the DL problem with a non-negligible advantage ε' (i. e. obtains a with probability at least ε'), where $\varepsilon' \geq \frac{\varepsilon p_{frk}}{(n_q+1)^2}$ which is a contradiction with the DL assumption in complexity theory. □

Lemma 4. *If there is an adversary $\mathcal{A}_{II}$ who can win Game IV in [15], with a non-negligible advantage ε, one can construct an algorithm $\mathcal{C}$, which can solve an instance of the DL problem with an advantage at least $\frac{\varepsilon p_{frk}}{(n_q+1)^2}$, where n_q is the number of queries from Private-Key and Signcrypt oracles and p_{frk} is the success probability of the adversary in Forking Lemma [6].*

Proof. Suppose that the algorithm $\mathcal{C}$ gets an instance $P, aP \in G$, of a DL problem and wants to obtain a.. First, $\mathcal{C}$ creates a list $\mathcal{L}$ such that explained in the proof of Lemma 2, which is initially empty. Then $\mathcal{C}$ plays Game IV in [15] with $\mathcal{A}_{II}$ as follows:

Initialization: This step is similar to that in the proof of Lemma 2.

Queries: This step is similar to the Phase 1 Queries step in the proof of Lemma 2.

Output: After a polynomially bounded number of queries, $\mathcal{A}_{II}$ outputs a valid signcryption $\delta^* = (S^*, C^*, T^*)$ on a message m^* from A^* to B^*.

At the end of the game, $\mathcal{C}$ acts as follows:

- If the simulation is aborted in any steps or $c_{A^*} = 0$, $\mathcal{C}$ aborts.
- Otherwise, $\mathcal{C}$ obtains m^* such that explained in the Unsigncrypt queries in the proof of Lemma 2. If δ^* is a valid signcryption on m^*, according to the Forking Lemma [6], $\mathcal{C}$ can get two valid signcryptions from A^* to B^* on m^* with the same random value β and different values of the random oracle h_{2,A^*,B^*,m^*,T^*}. So, $\mathcal{C}$ gets these two valid signcryptions with the same $T^* = \beta P$ and different values of $h = h_{2,A^*,B^*,m^*,T^*}$ and $h' = h'_{2,A^*,B^*,m^*,T^*}$. Denote these two valid signcryptions by $\delta_1 = (S_1, C_1, T^*)$ and $\delta_2 = (S_2, C_2, T^*)$. According to the step 5 of the signcryption algorithm, we have:

$$S_1(h + d_{A^*} + x_{A^*}) = x_{A^*} + \beta \bmod q,$$
$$S_2(h' + d_{A^*} + x_{A^*}) = x_{A^*} + \beta \bmod q.$$

So, we have:

$$S_1(h + d_{A^*} + x_{A^*}) = S_2(h' + d_{A^*} + x_{A^*}) \bmod q.$$

Note that as $c_{A^*} = 1$, $h_{1,A^*} = K$ and $d_{A^*} = r_{A^*} + \alpha h_{1,A^*} = r_{A^*} + \alpha K$. Moreover, the master secret key α is known to $\mathcal{C}$, but as $R_{A^*} = aP$, $r_{A^*} = a$ is unknown to $\mathcal{C}$. So, we have:

$$S_1(h + a + \alpha K + x_{A^*}) = S_2(h' + a + \alpha K + x_{A^*}) \bmod q.$$

In the above equation all values except a is known to $\mathcal{C}$. So $\mathcal{C}$ can obtain a as its answer to the DL problem.

Table 1: Comparison of the Gao *et al.*'s scheme and our improvement

Scheme	Conf. Against $\mathcal{A}_I$	Conf. Against $\mathcal{A}_{II}$	Unf. Against $\mathcal{A}_I$	Unf. Against $\mathcal{A}_{II}$	Secrecy of the Shared Key
[6]	×	✓	✓	✓	×
Ours	✓	✓	✓	✓	✓

Probability Analysis: It is similar to that explained in the proof of Lemma 3, except that the number of Partial-Private-Key and Replace-Public-Key queries are 0 here. □

Theorem 2. *The improved CL-SC scheme is unforgeable (EUF-CMA) against $\mathcal{A}_I$ and $\mathcal{A}_{II}$ based on the DL assumption.*

Proof. the proof is directly implied from Lemma 3 and Lemma 4. □

5.3 The Improved Access Control Protocol

If our improved CL-SC scheme is used in Gao *et al.*'s access control protocol which is explained in Section 3.2, it will be robust against our attack in Section 4.2, as in the fixed scheme, $\mathcal{A}_I$ can not replace PuK_B to obtain the session key $H_3(V)$, according to Remark 5.1. Figure 3 shows the access control protocol, based on the improved CL-SC scheme. It should be noted that in the improved protocol, Dr. Alice and Bob must send X_A and X_B (in addition to ID_A and ID_B) to the SP to get their partial keys $ParK_A$ and $ParK_B$.

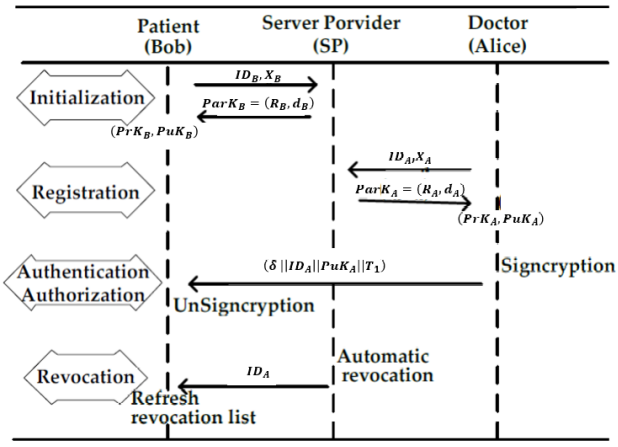

Figure 3: The improved access control protocol

6 Comparison

Table 1 provides a security comparison between the Gao *et al.*'s proposals and our improvements. As shown in Table 1, Gao *et al.*'s CL-SC scheme is not confidential against a key replacement attacker $\mathcal{A}_I$ and consequently the shared key will reveal in their proposed access control protocol and the secrecy of the shared key will not be guaranteed in their protocol. In our improvement, we fixed their CL-SC scheme to be confidential against $\mathcal{A}_I$ and consequently the secrecy of the shared key will be guaranteed in the access control protocol based on the improved CL-SC scheme. It is so important to note that this enhancement will not force any more computational and communications costs on Gao *et al.*'s proposals, as we have just replaced $H_1(ID_U, R_U)$ in Gao *et al.*'s proposal with $H_1(ID_U, R_U, X_U)$ to protect the improved scheme against the proposed attacks, which does not force any additional computational and communications costs.

7 Conclusion

In this work, we cryptanalyzed a recently proposed access control protocol for WBANs proposed by Gao *et al.* They first proposed a certificateless signcryption (CL-SC) scheme in the random oracle model (ROM) and claimed that their scheme is confidential (IND-CCA2) and unforgeable (EUF-CMA) against type I and type II adversaries, in the certificateless setting. Consequently, they designed an access control protocol for WBANs in which the physician (Dr. Alice) sends a signcrypted request message to the patient (Bob) and if she is authenticated to Bob, they establish a session key for their next communications. However, we showed that, in contrast to their claim, Gao *et al.*'s CL-SC scheme is not confidential against the type I adversary (a key replacement attacker) and consequently, this adversary can obtain the session key which is established by the physician for the next communications to the patient. Moreover, we fixed Gao *et al.*'s CL-SC scheme to be robust against our proposed attack. It is notable that the access control protocol based on our improved CL-SC scheme will not be vulnerable against the designed attack, too.

References

[1] E. Ahene, Z. Qin, A. K. Adusei, and F. Li, "Efficient signcryption with proxy re-encryption and its application in smart grid," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 9722–9737, 2019.

[2] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *International Confer-*

ence on the Theory and Application of Cryptology and Information Security, pp. 452–473, 2003.

[3] M. Barbosa and P. Farshim, "Certificateless signcryption," in *Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security*, pp. 369–372, 2008.

[4] S. Belguith, N. Kaaniche, M. Hammoudeh, and T. Dargahi, "Proud: Verifiable privacy-preserving outsourced attribute based signcryption supporting access policy update for cloud assisted IoT applications," *Future Generation Computer Systems*, vol. 111, pp. 899–918, 2020.

[5] Z. Caixue, "Certificateless signcryption scheme without random oracles," *Chinese Journal of Electronics*, vol. 27, no. 5, pp. 1002–1008, 2018.

[6] G. Gao, X. Peng, and L. Jin, "Efficient access control scheme with certificateless signcryption for wireless body area networks." *International Journal Network Security*, vol. 21, no. 3, pp. 428–437, 2019.

[7] M. S. Hajar, M. O. Al-Kadri, and H. K. Kalutarage, "A survey on wireless body area networks: architecture, security challenges and research opportunities," *Computers & Security*, p. 102211, 2021.

[8] P. Kasyoka, M. Kimwele, and S. M. Angolo, "Towards an efficient certificateless access control scheme for wireless body area networks," *Wireless Personal Communications*, vol. 115, no. 2, pp. 1257–1275, 2020.

[9] M. Kumar and S. Chand, "Medhypchain: A patient-centered interoperability hyperledger-based medical healthcare system: Regulation in covid-19 pandemic," *Journal of Network and Computer Applications*, vol. 179, p. 102975, 2021.

[10] X. Liu, Z. Wang, Y. Ye, and F. Li, "An efficient and practical certificateless signcryption scheme for wireless body area networks," *Computer Communications*, vol. 162, pp. 169–178, 2020.

[11] S. Mandal, B. Bera, A. K. Sutrala, A. K. Das, K.-K. R. Choo, and Y. Park, "Certificateless-signcryption-based three-factor user access control scheme for iot environment," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3184–3197, 2020.

[12] V. S. Naresh, S. Reddi, S. Kumari, V. D. Allavarpu, S. Kumar, and M.-H. Yang, "Practical identity based online/off-line signcryption scheme for secure communication in internet of things," *IEEE Access*, vol. 9, pp. 21 267–21 278, 2021.

[13] B. Narwal and A. K. Mohapatra, "A survey on security and authentication in wireless body area networks," *Journal of Systems Architecture*, vol. 113, p. 101883, 2021.

[14] P. Rastegari, "On the security of some recently proposed certificateless signcryption schemes," in *17th International ISC Conference on Information Security and Cryptology (ISCISC'20)*, IEEE, pp. 95–100, 2020.

[15] P. Rastegari and M. Berenjkoub, "An efficient certificateless signcryption scheme in the standard model," *ISeCure*, vol. 9, no. 1, 2017.

[16] P. Rastegari and M. Dakhilalian, "Cryptanalysis of a certificateless signcryption scheme," in *16th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC'19)*, IEEE, pp. 67–71, 2019.

[17] P. Rastegari and M. Khalili, "Cryptanalysis and improvement of an access control protocol for wireless body area networks," in *18th International ISC Conference on Information Security and Cryptology (ISCISC'21)*, 2021.

[18] P. Rastegari, W. Susilo, and M. Dakhlalian, "Efficient certificateless signcryption in the standard model: Revisiting luo and wan's scheme from wireless personal communications (2018)," *The Computer Journal*, vol. 62, no. 8, pp. 1178–1193, 2019.

[19] S. Shan, "An efficient certificateless signcryption scheme without random oracles," *International Journal of Electronics and Information Engineering*, vol. 11, no. 1, pp. 9–15, 2019.

[20] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) << cost (signature)+ cost (encryption)," in *Annual international cryptology conference*, Springer, pp. 165–179, 1997.

[21] T. G. Zimmerman, "Personal area networks: Near-field intrabody communication," *IBM Systems Journal*, vol. 35, no. 3.4, pp. 609–617, 1996.

Biography

Parvin Rastegari received the B.Sc., M.Sc. and Ph.D. degrees in electrical engineering from Isfahan University of Technology, Isfahan, Iran, in 2008, 2011 and 2019, respectively. Since 2020, she has been with the Electrical and Computer Engineering Group, Golpayegan College of Engineering, Isfahan University of Technology, Golpayegan, Iran, as an assistant professor. Her current research interests include cryptographic primitives and protocols.

Mojtaba Khalili received a Ph.D. degree in electrical engineering from the department of electrical and computer engineering, Isfahan University of Technology in 2019. He is currently an assistant professor at the K.N Toosi University. His research interests are cryptographic primitives and protocols.

Ali Sakhaei received the B.S and M.S degrees from Shahid Beheshti University, Tehran, Iran in 2004 and 2006 respectively, and the Ph.D. degree from Payame Noor University, Tehran, Iran in 2018. He is currently an Assistant Professor with the statistics Department, Basic Sciences College, Payame Noor University, Tehran, Iran. His current research interests include stochastic process, Actuarial mathematics and Non-life insurance.