The ISC Int'l Journal of Information Security
ISeCure

November 2023, Volume 15, Number 3 (pp. 1–8)
http://www.isecure-journal.org

Security Analysis and Improvement of an Access Control Scheme for Wireless Body Area Networks **

Parichehr Dadkhah [1,*], Mohammad Dakhilalian [1], and Parvin Rastegari [2]

[1] *Department of Electrical and Computer Engineering, Isfahan University of Technology, Isfahan, Iran*
[2] *Electrical and Computer Engineering Group, Golpayegan College of Engineering, Isfahan University of Technology, Golpayegan, Iran*

ARTICLE INFO.

Article history:
Received: —
Revised: —
Accepted: —
Published Online: —

Keywords:
Access Control, ROM, Signcryption, WBANs

Type: Research Article

doi: ---

dor: ---

ABSTRACT

Wireless Body Area Networks (WBANs) have attracted a lot of attention in recent researches as they play a vital role in diagnosing, controlling and treating diseases. These networks can improve the quality of medical services by following the health status of people and providing online medical advice for them, momentarily. Despite the numerous advantages of these networks, they may cause irrecoverable problems for patients, if security considerations are not properly met. So, it is very important to find solutions for satisfying security requirements in these networks. A signcryption scheme can be considered as one of the most important cryptographic tools for providing the security requirements in WBANs. Recently, Kasyoka *et al.* proposed a signcryption scheme based on which they designed an access control protocol for WBANs. They proved the security of their proposals in the random oracle model (ROM). In this paper, we concentrate on Kasyoka *et al.*'s proposals and show that their proposed signcryption scheme and consequently their proposed access control protocol for WBANs are vulnerable against various attacks, in contrast to their claims. Afterward, we fix the scheme to be secure against our proposed attacks.

1 Introduction

Electronic health (e-health) or remote medical electronic care has received a lot of attention in recent years due to the expansion of the Internet, smartphones and health applications. One of the emerging aspects of e-health is Wireless Body Area Networks (WBANs) in which the patients' health status, including blood pressure, heart rate, etc., can be collected through sensors connected to their body. These sensors can be invasive or non-invasive. Invasive sensors are inserted into the human body, while non-invasive ones are attached on the human skin. In a WBAN, the patients' vital information is collected by the sensors and sent to an authorized entity such as a doctor or a nurse. The smart device transmits the information to the health server through the Internet, and the doctor can send the necessary prescription by observing the patients' conditions and medical records. Figure 1 shows the structure of a WBAN [1].

Online tracking of people, even while moving, allows hospital personnel to provide better services. As mentioned, this can be achieved by connecting different sensors to the patients' bodies and sending the

* Corresponding author.
**This article is an extended/revised version of an ISCISC'23 paper.
Email addresses: p.dadkhah@ec.iut.ac.ir, mdalian@iut.ac.ir, p.rastegari@iut.ac.ir
ISSN: 2008-2045

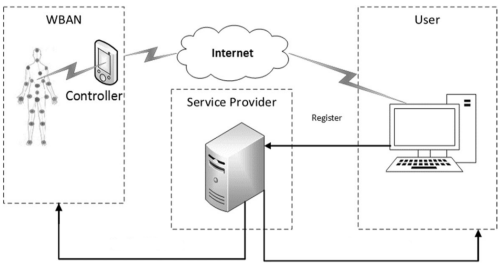

Figure 1. The structure of a WBAN

corresponding signals to the hospital personnel. So, they can detect abnormal signals in the shortest possible time and send the information to the specialist, if necessary. The specialist doctor can then send the necessary proceedings to the patient via SMS, video or voice. It is obvious that this technology has numerous benefits such as rapid diagnosis and treatment of the disease, the comfort of the patient due to no need to visit, the doctor's more focus on diagnosing the disease and prescribing appropriate recommendations, making hospitals quieter and so on [1]. Although this technology has many advantages, it is vital to note that if the system does not work properly or an error occurs in sending or receiving data, human lives may be at risk. Therefore, security considerations must be taken into account, in this scenario. Without security considerations in WBANs, a malicious entity can enter the network, perform malicious operations, steal critical information and cause irreparable damage to the system. Furthermore, it is obvious that the authentication of hospital employees is necessary to protect the patients from risks such as wrong medication, dosage or time of administration. Therefore, the security of these networks is a challenging issue.

Security protocols are the main tool for satisfying the security requirements in WBANs. The designers of these protocols usually face to the limitations of computation power, communications bandwidth and storage space. Moreover, due to the mobility of the patients, protocols with mobility capability must be considered. A signcryption scheme is one the most important cryptographic tools for designing security protocols in WBANs which meet all the mentioned limitations. So far, many efforts have been made to design security protocols for WBANs using signcryption schemes [2–8].

Signcryption schemes are designed based on Public Key Cryptography (PKC). In traditional PKC, the user's public key is validated by the signature of a trusted Certificate Authority (CA) on the public key. This process requires spending a lot of time and high computational, communications and storage costs by the CA. To solve this problem, the concept of identity based PKC (ID-PKC) was proposed [9]. In ID-PKC, the public key is obtained directly from the user's ID and the private key is generated by a trusted authority called a Key Generation Center (KGC). However, the major problem of ID-PKC is the key escrow problem, as the KGC knows all users' private keys. To solve this problem, Al-Riyami and Paterson presented the idea of certificateless PKC (CL-PKC), in 2003 [10]. This idea was born from various researches on providing PKC-based schemes that do not require the use of certificates and do not have the key escrow problem of ID-PKC, simultaneously. The proposed solution of Al-Riyami and Paterson, the CL-PKC, has both of these features [10]. The CL-PKC can be modeled as a PKC between traditional PKI and ID-PKC.

1.1 Related Works

In 2003, Al-Riyami and Paterson [10] proposed the concept of CL-PKC. In the same year, Huang *et al.* [11] showed that Al-Riyami and Paterson's proposal has a security gap and is vulnerable to the public key replacement attack. They fixed the existing security gap in their new proposed scheme. In 2004, Yum *et al.* [12] presented a method based on certificateless signatures, which has the same level of security as traditional public key algorithms. Unlike the previous methods, it is not based on pairing. In 2007, Choi *et al.* [13] presented a new approach involving the combination of short signatures using bilinear maps. In their proposed CLS scheme, a complete private key of a user is a single group element and the process of signature verification requires only one pairing operation. Moreover, the proposed signature has a flexible structure and hence can be used as a certificateless signature scheme with additional features such as certificateless ring and blind signature schemes. In the same year, Huang *et al.* [14] investigated certificateless security models. They also presented two new proposals that are secure in the random oracle model (ROM). In their paper, for the first time, three new types of an adversary were introduced according to the attack power including normal, strong and super adversaries. In 2008, Dent [15] reviewed all certificateless signatures up to that year from the security point of view. In 2011, Huang *et al.* [16] have examined the security of the schemes presented until that year with the same definition of three types of adversaries as presented in [14] combined with traditional adversaries. In 2019, Zhang *et al.* [17] presented a certificateless signature scheme, which only requires a public channel for the signing process. They claimed that their proposed signature is resistant against both public key replacement attacks and malicious-but-passive third parties in the standard model. However, Yang *et al.* [18] showed that the proposed signature [17] is vulnerable to the key replacement attacks. In

2020, Du *et al.* [19] proposed a certificateless signature based on elliptic curve that is resistant against the adaptive chosen message attack. In the same year, Thumbur *et al.* [20] presented the first certificateless signature without pairing, which is highly optimized in terms of computing power and storage space. Recently, Kasyoka *et al.* [1] have presented an efficient certificateless signcryption (CLSC) scheme based on which they designed an access control protocol for WBANs. They proved the confidentiality (IND-CCA2) and the unforgeability (EUF-CMA) of their proposal against both types of adversaries A_I and A_{II} in the random oracle model (ROM). It is notable that A_I is actually an adversary that performs a public key replacement attack, while A_{II} is a malicious KGC that forms an attack with the master secret key in his/her hand.

1.2 Contributions

In this paper, we concentrate on Kasyoka *et al.*'s proposal [1] and show its vulnerabilities in different aspects in the certificateless setting. In more detail, we show that their scheme has the following drawbacks:

- Every user can extract the KGC's master secret key from his/her partial private key, which breaks the security of their scheme, as every entity can then impersonate another entity by replacing his/her public key corresponding to a new secret value and obtain the corresponding full private key by the new replaced secret value and the revealed master secret key.
- After receiving the sender's signcryption on a message m, the receiver can forge another signcryption on a new message m^* on behalf of the sender to a new receiver.
- Contrary to the authors' claim, their scheme is not certificateless at all, since the partial private key of the sender is not required to produce a valid signcryption. Furthermore, the partial private key of the receiver is not required in the unsigncryption algorithm.
- Because of the previous drawback, their scheme is vulnerable against the public key replacement attack.

Consequently, we improve Kasyoka *et al.*'s proposal to solve its vulnerabilities.

1.3 Paper Organization

The continuation of this paper is compiled as follows. In section 2, the system model and the security requirements of a certificateless signcryption scheme are described. In section 3, an overview of Kasyoka *et al.*'s CLSC scheme and access control protocol is described. In section 4, we show the security flaws in Kasyoka *et al.*'s proposals and describe our designed attacks in details. In section 5, we provide an improvement of Kasyoka *et al.*'s proposal to fix its flaws. Finally, a conclusion is provided in section 6.

2 Certificateless Signcryption Scheme

A certificateless signcryption scheme (CLSC) is a type of signcryption in which the user's full private key is generated by the cooperation of the key generation center (KGC) and the user. In this process, the KGC generates a partial private key and sends it to the user through a secure channel. Then the user produces a full private key by selecting a secret value and concatenating it with the partial private key.

2.1 System Model

The entities involved in a CLSC scheme, are a KGC, a sender S and a receiver R. A CLSC scheme can be defined by the following six algorithms:

(1) Setup: This algorithm is performed by the KGC on a security parameter ν as input, to output a master secret key msk and public parameters $params$. The KGC keeps msk secret and publishes $params$.
(2) PuK-Set: This algorithm is operated by the i-th user with the identity ID_i on $params$ and a random secret value chosen by the user x_i as input, to output the user's public key PK_i.
(3) PPrK-Extract: This algorithm is executed by the KGC on ID_i, PK_i, msk and $params$ as input, to output the i-th user's partial private key d_i. Then the KGC delivers d_i to the user through a secure channel.
(4) PrK-Set: This algorithm is performed by the i-th user on $params$, x_i and d_i as input, to output the full private key of the user SK_i.
(5) SC: This algorithm is performed by a sender S on a message m, ID_S, SK_S, ID_R and PK_R as input, to output a signcryption σ on m for a receiver R.
(6) USC: This algorithm is operated by the receiver R on σ, ID_S, PK_S, ID_R and SK_R as input, to output m if the received signcryption is valid and $\perp$, otherwise.

2.2 Security Requirements

The connection established in a WBAN between the controller and the user must at least guarantee five security features, including confidentiality, authentication, integrity, non-repudiation and anonymity [1]. A CLSC scheme can well meet the first four requirements while the last one, i. e. the anonymity, can be achieved by using pseudo-IDs instead of real IDs. In

a certificateless setting in PKC, two types of adversaries are considered [1, 8]:

- The type I adversary A_I who doesn't have access to the master secret key and only has the ability to replace the public keys of the users. A_I is known as a public key replacement attacker.
- The type II adversary A_{II} who has access to the master secret key but doesn't have the ability to replace the public keys of the users. A_{II} is known as a malicious KGC attacker.

3 Kasyoka *et al.*'s CLSC Scheme

Kasyoka *et al.*'s proposed CLSC scheme is made up of the following steps [1]:

(1) Setup: On input a security parameter ν, the KGC selects a cyclic group G of a prime order q, a generator of G denoted by P and three secure hash functions $H_1, H_2, H_3 : \{0,1\}^* \rightarrow Z_q^*$. Then the KGC chooses a random value $s \in_R Z_q^*$ as the master secret key and sets the corresponding general public key as $P_{pub} = sP$. KGC keeps s secret and publishes the tuple $params = (G, P, q, P_{pub}, H_1, H_2, H_3)$.

(2) PuK-Set: The user i selects $x_i \in_R Z_q^*$ as a secret value and computes $PK_i = x_i P$. Then the user sends PK_i to the KGC.

(3) PPrK-Extract: The KGC firstly calculates d_i as $d_i = s.H_1(ID_i, PK_i, P_{pub}) \bmod q$. Then the KGC secretly sends d_i to the user i.

(4) PrK-Set: The user i sets $SK_i = (d_i, x_i, z_i)$, where $z_i = d_i^{-1} x_i^{-1} \bmod q$.

(5) SC: To create a signcryption σ on a message m for a receiver R, the sender S executes the following steps:
- Picks a random value $r \in_R Z_q^*$.
- Sets $W = rP$.
- Sets $\beta = rPK_R$.
- Sets $h_3 = H_3(W, \beta)$.
- Sets $c = h_3 \oplus m$.
- Sets $h = H_2(W, c, PK_S, PK_R, ID_S, ID_R)$.
- Computes $\gamma = h.d_S.r.z_S \bmod q$.

Finally, S outputs $\sigma = (\gamma, c, h)$ and sends it to R.

(6) USC: Upon receiving σ, the receiver R executes the following steps:
- Computes $Q = (\gamma.h^{-1} \bmod q)PK_S$.
- Sets $h' = H_2(Q, c, PK_S, PK_R, ID_S, ID_R)$.
- If $h \neq h'$, outputs $\perp$.
- If $h = h'$, computes $\beta = x_R Q$ and obtains $m = H_3(Q, \beta) \oplus c$.

Kasyoka *et al.* have claimed that their proposed CLSC scheme is confidential (IND-CCA2) and unforgeable (EUF-CMA) against both A_I and A_{II} under the Discrete Logarithm (DL) assumption in ROM [1].

Afterward, they proposed an access control scheme for WBANs based on their CLSC scheme, which directly inherits its security requirements from their CLSC scheme [1]. However, we will show in the next section that unfortunately Kasyoka *et al.*'s CLSC scheme (and consequently their proposed access control scheme for WBANs) is not secure, in contrast to their claims.

4 Security Flaws of Kasyoka *et al.*'s CLSC Scheme

Our investigations show that Kasyoka *et al.*'s CLSC scheme can be penetrated in many ways. In the following, we describe some of the security gaps in Kasyoka *et al.*'s scheme and explain our attacks against their proposal in details.

4.1 Extraction the Master Secret Key

As mentioned, in the PPrK-Extract algorithm of Kasyoka *et al.*'s CLSC scheme, the KGC computes $d_i = s.H_1(ID_i, PK_i, P_{pub}) \bmod q$ and sends it to the user i through a secure channel. It is clear that the user i can simply calculate $l_i = H_1(ID_i, PK_i, P_{pub})$ and obtains the master secret key s from Equation 1.

$$s = d_i.l_i^{-1} \bmod q. \tag{1}$$

It is obvious that the user i (as an insider adversary who can obtain s as mentioned) can then easily break the confidentiality and unforgeability of a CLSC scheme by the $msk = s$ in his/her hand.

4.2 Forging Signcryptions on Behalf of the Sender by the Receiver

We show that in Kasyoka *et al.*'s CLSC scheme, after receiving a signcryption σ of a sender S on a message m by a receiver R, R can then forge another signcryption σ^* on behalf of S on a new message m^* for another receiver R^*.

In more detail, suppose that R has received a valid signcryption $\sigma = (\gamma, c, h)$ on a message m from S. Then R can forge a signcryption $\sigma^* = (\gamma^*, c^*, h^*)$ on behalf of S on a message m^* for another receiver R^* by the following steps:

- Obtains $W = (\gamma.h^{-1} \bmod q)PK_S$.
- Obtains $\beta = x_R W$.
- Obtains $h_3 = H_3(W, \beta)$.
- Sets $c^* = h_3 \oplus m^*$.
- Sets $h^* = H_2(W, c^*, PK_S, PK_{R^*}, ID_S, ID_{R^*})$.
- Sets $\gamma^* = \gamma.h^{-1}.h^* \bmod q$.

Finally, R returns $\sigma^* = (\gamma^*, c^*, h^*)$ and sends it to R^* as a signcryption on a message m^* on behalf of S. It is easy to check that σ^* passes the verification phase of the USC algorithm executed by R^*, successfully.

In more detail, R^* calculates:

$$Q^* = (\gamma^*.h^{*^{-1}} \bmod q)PK_S, \quad (2)$$

and:

$$h^{*\prime} = H_2(Q^*, c^*, PK_S, PK_{R^*}, ID_S, ID_{R^*}), \quad (3)$$

and accepts the signcryption if $h^* = h^{*\prime}$. It is straightforward to show the correctness of Equation 2 and Equation 3, as:

$$\begin{aligned} Q^* &= (\gamma^*.h^{*^{-1}} \bmod q)PK_S \\ &= (\gamma.h^{-1}.h^*.h^{*^{-1}} \bmod q)PK_S \\ &= (\gamma.h^{-1} \bmod q)PK_S \\ &= W, \end{aligned}$$

and:

$$\begin{aligned} h^{*\prime} &= H_2(Q^*, c^*, PK_S, PK_{R^*}, ID_S, ID_{R^*}) \\ &= H_2(W, c^*, PK_S, PK_{R^*}, ID_S, ID_{R^*}) \\ &= h^*, \end{aligned}$$

which shows that σ^*, which is forged by R on behalf of S, passes the verification phase of the USC algorithm executed by R^*, successfully.

4.3 Certificateless Performance Analysis

It is well-known that, in certificateless setting in a signcryption scheme, a sender S must use both x_S and d_S to produce a signcryption on a message m for a receiver R. Similarly, R must use both x_R and d_R to obtain m. However, unfortunately, this necessity is not considered in Kasyoka *et al.*'s CLSC scheme neither at the sender's side nor at the receiver's side.

In more detail, at the sender's side, we have:.

$$\begin{aligned} \gamma &= h.d_S.r.z_S \bmod q \\ &= h.d_S.r.d_S^{-1}.x_S^{-1} \bmod q \\ &= h.r.x_S^{-1} \bmod q. \end{aligned} \quad (4)$$

According to Equation 4, γ and consequently σ can be calculated only by the use of x_S without the need of the knowledge of d_S.

Furthermore, it is clear that at the receiver's side, the receiver can calculate $\beta = x_R Q$ and obtain $m = H_3(Q, \beta) \oplus c$, by only x_R, without the necessity of the knowledge of d_R.

So, we can say that Kasyoka *et al.*'s signcryption scheme is not certificateless at all, in contrast to their main claim. This lack makes it easy to apply public key replacement attacks against both the unforgeability and the confidentiality of Kasyoka *et al.*'s scheme as will be described in two following sections.

4.4 Public Key Replacement Attack Against the Unforgeability

As mentioned earlier, in Kasyoka *et al.*'s signcryption scheme, the sender can calculate γ by the use of just x_S produced by him/herself and without the need of d_S generated by the KGC. Therefore, a type I adversary A_I can simply perform a public key replacement attack against the unforgeability of Kasyoka *et al.*'s scheme according to the following steps:

(1) A_I selects a random value $x_S^* \in_R Z_q^*$ and replaces the real public key of the sender PK_S with the new public key $PK_S^* = x_S^* P$.
(2) Then A_I executes the following steps to forge a signature σ on a message m on behalf of a sender S for a receiver R:
   - Picks a random value $r \in_R Z_q^*$.
   - Sets $W = rP$.
   - Sets $\beta = r.PK_R$.
   - Sets $h_3 = H_3(W, \beta)$.
   - Sets $c = h_3 \oplus m$.
   - Sets $h = H_2(W, c, PK_S, PK_R, ID_S, ID_R)$.
   - Computes $\gamma = h.r.{x_S^*}^{-1} \bmod q$.

Finally, S outputs $\sigma = (\gamma, c, h)$ and sends it to R. It is obvious that σ is a valid signcryption on behalf of S with the replaced public key PK_S^* in R's point of view.

4.5 Public Key Replacement Attack Against the Confidentiality

As mentioned earlier, in Kasyoka *et al.*'s signcryption scheme, the receiver can execute the USC algorithm and obtain m by the use of just x_R produced by him/herself and without the need of d_R generated by the KGC. Therefore, a type I adversary A_I can simply perform a public key replacement attack against the confidentiality of Kasyoka *et al.*'s scheme according to the following steps:

(1) A_I selects a random value $x_R^* \in_R Z_q^*$ and replaces the real public key of the receiver PK_R with the new public key $PK_R^* = x_R^* P$.
(2) Then every entity who wants to create a signcryption for R uses PK_R^* instead of PK_R. In this sense, the adversary A_I can capture $\sigma = (\gamma, c, h)$ from the public channel and executes the following steps to obtain m:
   - Computes $Q = (\gamma.h^{-1} \bmod q)PK_S$.
   - Sets $h' = H_2(Q, c, PK_S, PK_R^*, ID_S, ID_R)$.
   - If $h \neq h'$, outputs $\perp$.
   - If $h = h'$, computes $\beta = x_R^* Q$ and obtains $m = H_3(Q, \beta) \oplus c$.

So, the adversary A_I can deceive the sender to create a signcryption in which the message m (which must be confidential between the sender and the receiver)

can be revealed by A_I.

It is notable that as Kasyoka *et al.*'s scheme does not meet the basic security requirements of a signcryption scheme in the certificateless setting, their access control scheme for WBANs is not secure, either.

5 The Improved CLSC Scheme

In this section, we improve Kasyoka *et al.*'s signcryption scheme to fix its flaws described in section 4. The improved CLSC scheme is made up of the following steps:

(1) Setup: This step is similar to the Setup algorithm of Kasyoka *et al.*'s scheme described in section 4.

(2) PPrK-Extract: The user i selects $x_i \in_R Z_q^*$ as a secret value, computes $X_i = x_i P$ and sends X_i to the KGC. The KGC firstly selects $t_i \in_R Z_q^*$ and sets $T_i = t_i P$. Then the KGC calculates d_i as $d_i = s.H_1(ID_i, X_i, T_i, P_{pub}) + t_i \bmod q$ and sends (T_i, d_i) to the user i via a secure channel.

(3) PuK-Set: The user i sets $PK_i = (T_i, X_i)$.

(4) PrK-Set: The user i sets $SK_i = (d_i, x_i)$.

(5) SC: To create a signcryption σ on a message m for a receiver R, the sender S executes the following steps:

- Picks a random value $r \in_R Z_q^*$.
- Sets $W = r.(x_S + d_S)P$.
- Sets $\beta = r.(x_S + d_S)X_R$.
- Computes $h_R = H_1(ID_R, X_R, T_R, P_{pub})$ and sets $h_3 = H_3(W, \beta, d_S(T_R + h_R P_{pub}))$.
- Sets $c = h_3 \oplus m$.
- Sets $h = H_2(W, c, PK_S, PK_R, ID_S, ID_R)$.
- Computes $\gamma = h.r.(x_S + d_S) \bmod q$.

Finally, S outputs $\sigma = (\gamma, c, h)$ and sends it to R.

(6) USC: Upon receiving $\sigma = (\gamma, c, h)$, the receiver R executes the following steps:

- Computes $Q = \gamma.h^{-1}P$.
- Sets $h' = H_2(Q, c, PK_S, PK_R, ID_S, ID_R)$.
- If $h \neq h'$, outputs $\perp$.
- If $h = h'$, computes $\beta = x_R Q$, $h_S = H_1(ID_S, X_S, T_S, P_{pub})$ and obtains $m = H_3(Q, \beta, d_R(T_S + h_S.P_{pub})) \oplus c$.

The correctness of the improved scheme can be easily checked by Equation 5 and Equation 6, as:

$$\begin{aligned} h' &= H_2(Q, c, PK_S, PK_R, ID_S, ID_R) \\ &= H_2(\gamma.h^{-1}P, c, PK_S, PK_R, ID_S, ID_R) \\ &= H_2(h.r.(x_S + d_S).h^{-1}P, c, PK_S, PK_R, ID_S, ID_R) \\ &= H_2(r.(x_S + d_S)P, c, PK_S, PK_R, ID_S, ID_R) \\ &= H_2(W, c, PK_S, PK_R, ID_S, ID_R) \\ &= h, \end{aligned} \tag{5}$$

and:

$$\begin{aligned} & H_3(Q, \beta, d_R(T_S + h_S.P_{pub})) \oplus c \\ &= H_3(W, \beta, d_R(t_S P + h_S.s.P) \oplus c \\ &= H_3(W, \beta, d_R(t_S + h_S.s)P) \oplus c \\ &= H_3(W, \beta, d_R.d_S P) \oplus c \\ &= H_3(W, \beta, d_S.(t_R + h_R.s)P) \oplus c \\ &= H_3(W, \beta, d_S.(t_R P + h_R.sP)) \oplus c \\ &= H_3(W, \beta, d_S.(T_R + h_R P_{pub})) \oplus h_3 \oplus m \\ &= h_3 \oplus h_3 \oplus m = m. \end{aligned} \tag{6}$$

It is notable that all the flaws of Kasyoka *et al.*'s scheme described in section 4, are fixed in the improved version, as:

- In the PPrK-Extract algorithm of the improved version, the KGC computes d_i as $d_i = s.H_1(ID_i, X_i, T_i, P_{pub}) + t_i \bmod q$ instead of $d_i = s.H_1(ID_i, PK_i, P_{pub}) \bmod q$. By inserting t_i in the computation of d_i, the user i is prevented from extracting the master secret key, by the attack described in Section 4.1.
- In the SC algorithm, h_3 is computed as $h_3 = H_3(W, \beta, d_S(T_R + H_1.P_{pub}))$, instead of $h_3 = H_3(W, \beta)$. By considering $d_S(T_R + H_1.P_{pub})$ as one of the inputs of $H_3(.)$, after receiving a signcryption σ of a sender S on a message m by a receiver R, R no longer can forge another signcryption σ^* on behalf of S on a new message m^* for another receiver R^*, since R needs d_S or d_{R^*} to calculate $h_3 = H_3(W, \beta, d_S(T_{R^*} + h_{R^*}.P_{pub}))$ or $h_3 = H_3(W, \beta, d_{R^*}(T_S + h_S.P_{pub}))$, which are both secret to R. So, the improved scheme is robust against the attack described in Section 4.2.
- In the SC algorithm, S needs to know both x_S and d_S to create a valid signcryption. Similarly, in the USC algorithm, R needs to know both x_R and d_R to obtain m, successfully. So, in contrast to Kasyoka *et al.*'s scheme, the improved version meets the basic requirement of a certificateless setting in a signcryption scheme, described in Section 4.3, and hence it is no longer vulnerable against the attacks explained in Section 4.4 and Section 4.5.

6 Conclusion

In this work, we cryptanalyzed an access control scheme for WBANs, proposed by Kasyoka *et al.*, recently and showed that unfortunately their proposal is vulnerable against well-known attacks, in contrast to their claims. Kasyoka *et al.* proposed a CLSC scheme and claimed that their proposal is unforgeable (EUF-CMA) and confidential (IND-CCA2) in the random oracle model. Then, they designed an access control scheme, based on their CLSC scheme. However, we designed attacks which show that Kasyoka *et al.*'s CLSC scheme and consequently their access control protocol for WBANs are not secure at all. Afterward,

we improved their proposal to be robust against our designed attacks.

References

[1] Philemon Kasyoka, Michael Kimwele, and Shem Mbandu Angolo. Towards an efficient certificateless access control scheme for wireless body area networks. *Wireless Personal Communications*, 115:1257–1275, 2020.

[2] Insaf Ullah, Muhammad Asghar Khan, Ako Muhammad Abdullah, Fazal Noor, Nisreen Innab, and Chien-Ming Chen. Enabling secure communication in wireless body area networks with heterogeneous authentication scheme. *Sensors*, 23(3):1121, 2023.

[3] H Azath, J Gokulraj, J Surendiran, D Geetha, and TR Ganesh Babu. Security for health information by elliptical curve diffie-hellman and improve energy efficiency in wban. In *AIP Conference Proceedings*, volume 2523, page 020075. AIP Publishing LLC, 2023.

[4] Sunday Oyinlola Ogundoyin and Ismaila Adeniyi Kamil. Paash: A privacy-preserving authentication and fine-grained access control of outsourced data for secure smart health in smart cities. *Journal of Parallel and Distributed Computing*, 155:101–119, 2021.

[5] Abdullah M Almuhaideb. Re-auth: Lightweight re-authentication with practical key management for wireless body area networks. *Arabian Journal for Science and Engineering*, 46(9):8189–8202, 2021.

[6] Senthil Kumar Swami Durai, Balaganesh Duraisamy, and JT Thirukrishna. Certain investigation on healthcare monitoring for enhancing data transmission in wsn. *International journal of wireless information networks*, pages 1–8, 2021.

[7] G Shanmugavadivel, B Gomathy, and SM Ramesh. An enhanced data security and task flow scheduling in cloud-enabled wireless body area network. *Wireless personal communications*, 120:849–867, 2021.

[8] Parvin Rastegari and Mojtaba Khalili. Cryptanalysis and improvement of an access control protocol for wireless body area networks. In *2021 18th International ISC Conference on Information Security and Cryptology (ISCISC)*, pages 57–62. IEEE, 2021.

[9] Adi Shamir. Identity-based cryptosystems and signature schemes. In *Advances in Cryptology: Proceedings of CRYPTO 84 4*, pages 47–53. Springer, 1985.

[10] Sattam S Al-Riyami and Kenneth G Paterson. Certificateless public key cryptography. In *International conference on the theory and application of cryptology and information security*, pages 452–473. Springer, 2003.

[11] Xinyi Huang, Willy Susilo, Yi Mu, and Futai Zhang. On the security of certificateless signature schemes from asiacrypt 2003. In *International Conference on Cryptology and Network Security*, pages 13–25. Springer, 2005.

[12] Dae Hyun Yum and Pil Joong Lee. Generic construction of certificateless signature. In *Australasian Conference on Information Security and Privacy*, pages 200–211. Springer, 2004.

[13] Kyu Young Choi, Jong Hwan Park, Jung Yeon Hwang, and Dong Hoon Lee. Efficient certificateless signature schemes. In *International Conference on Applied Cryptography and Network Security*, pages 443–458. Springer, 2007.

[14] Xinyi Huang, Yi Mu, Willy Susilo, Duncan S Wong, and Wei Wu. Certificateless signature revisited. In *Australasian Conference on Information Security and Privacy*, pages 308–322. Springer, 2007.

[15] Alexander W Dent. A survey of certificateless encryption schemes and security models. *International Journal of Information Security*, 7(5):349–377, 2008.

[16] Xinyi Huang, Yi Mu, Willy Susilo, Duncan S Wong, and Wei Wu. Certificateless signatures: new schemes and security models. *The computer journal*, 55(4):457–474, 2012.

[17] Yinghui Zhang, Robert H Deng, Dong Zheng, Jin Li, Pengfei Wu, and Jin Cao. Efficient and robust certificateless signature for data crowdsensing in cloud-assisted industrial iot. *IEEE Transactions on Industrial Informatics*, 15(9):5099–5108, 2019.

[18] Wenjie Yang, Shangpeng Wang, Xinyi Huang, and Yi Mu. On the security of an efficient and robust certificateless signature scheme for iiot environments. *IEEE Access*, 7:91074–91079, 2019.

[19] Hongzhen Du, Qiaoyan Wen, Shanshan Zhang, and Mingchu Gao. A new provably secure certificateless signature scheme for internet of things. *Ad Hoc Networks*, 100:102074, 2020.

[20] Gowri Thumbur, G Srinivasa Rao, P Vasudeva Reddy, NB Gayathri, and DV Rama Koti Reddy. Efficient pairing-free certificateless signature scheme for secure communication in resource-constrained devices. *IEEE Communications Letters*, 24(8):1641–1645, 2020.

Parichehr Dadkhah received the B.Sc. and M.Sc. degrees in electrical engineering from Isfahan University of Technology (IUT), Isfahan, Iran, in 2013 and 2017, respectively. She is now a Ph.D. candidate in electrical engineering in Isfahan University

of Technology, Isfahan, Iran. HONORS: First rank among the M.Sc. graduates of the Communications Systems and 5th rank among the B.Sc. graduates of the Electrical Engineering, in IUT.

Mohamad Dakhilalian received Ph.D. degrees in Communication from Department of Electrical and Computer Engineering, Isfahan University of Technology, Isfahan - Iran in 1998. The title of his Ph.D. thesis is ,Statistical Analysis of Pseudo-random Sequences and Design of Chaotic generators. He received M.Sc. degrees in Communication engineering (Channel Coding) from Department of Engineering, Tarbiat Modares University, Tehran - Iran in 1993. The title of his M.Sc. thesis is ,Analysis and Simulation of Convolution Codes in a Specific Command and Image Wireless System. He received B.Sc. degrees in Communication engineering from Department of Electrical and Computer Engineering, Isfahan University of Technology (IUT), Isfahan, Iran in 1989. HONORS: First rank in the B.Sc. graduates of the Department of Electrical and Computer Engineering, Isfahan University of Technology, 1990, Third rank in the M.Sc. graduates of the Department of Engineering, Tarbiat Modares University, 1993. and First rank in the Ph.D. of the Department of Electrical and Computer Engineering, Isfahan University of Technology, 1998.

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.