Efficient Access Control Scheme with Certificateless Signcryption for Wireless Body Area Networks

GaiMei Gao[1,2], XinGuang Peng[1], and LiZhong Jin[3]
(Corresponding author: XinGuang Peng)
College of Information and Computer, Taiyuan University of Technology[1]
No.79, West Yingze Street, Taiyuan, Shanxi, China
Department of Computer Science and Technology, Taiyuan University of Science and Technology[2]
Applied Science College, Taiyuan University of Science and Technology[3]
No.66, Waliu Road, Wanbailin District, Taiyuan, Shanxi, China
(Email: sxgrant@126.com)
(Received Jan. 9, 2018; Revised and Accepted May 5, 2018; First Online Jan. 13, 2019)

Abstract

Wireless body area networks (WBANs) can collect patients' vital data of body parameters and environment parameters via small wearable or implantable sensors. To ensure the security of the vital data, an efficient access control scheme with certificateless signcryption(CLSC) is designed. The correctness of the scheme is proved by mathematical calculation. It also proves that the scheme offers confidentiality and unforgeability in the random oracle model on the basis of the hardness of the Computational Diffie-Hellman (CDH) problem and Discrete Logarithm (DL) problem respectively. Compared with the existing three access control schemes utilizing signcryption, the scheme can satisfy more security properties and has the shortest computational time and the least energy consumption for the controller.

Keywords: Access Control; Certificateless; Signcryption;Wireless Body Area Networks

1 Introduction

Wireless body area networks (WBANs) can acquire human body's vital signals through a network which consists of intelligent and low-power micro- and nano-sensors and actuators. These sensors for collecting timely data can be placed on the body or implanted in the human body (or even in the blood stream). In addition to saving lives, WBANs is prevalent in reducing health care costs by removing the costly in-hospital monitoring of patients. In IEEE 802.15.6 [13], WBANs applications are classified into two types: medical and non-medical applications. In the study, we focus on the technological requirements of medical WBANs.

Security and privacy are two important considerations in WBANs. Since the patient-related data in the WBANs plays a critical role in medical diagnosis and treatment, it is necessary to ensure the security of these data in such a way that only authorized users can access these data [4, 18, 19]. Another aspect which should be considered in WBANs is the limitation of the controller's resources, especially storage space and computational capability. In order to protect the data privacy and reduce the energy consumption of computation and communication, lightweight access control schemes are needed. The certificateless public key cryptography (CL-PKC) [5] does not require the use of the certificate which brings the burden of certificate management, and CL-PKC avoids the key escrow problem because the user's private key is not generated by himself but by the user and the key generation center (KGC). Signcryption [3], as a cryptographic technique, can provide both the functions of public key encryption and digital signature in a logical single step at a significantly lower cost compared to traditional signature-then-encryption methods. A signcryption scheme can achieve confidentiality, authentication, integrity, and non-repudiation simultaneously at a lower cost. Therefore, we design an efficient access control with certificateless signcryption (CLSC) to protect data privacy of WBANs while reducing the computational overhead and storage overhead of resource-constrained controller. Many certificateless cryptosystems [1, 9, 10], such as certificateless encryption schemes, certificateless signcryption schemes, and certificateless access control schemes were proposed.

Access control is an important part of defense for the security of network systems, which protects data security and user privacy through only authorized users can access the WBANs. Some important progresses have been made in the access control for the WBANs. In

2011, Cagalaban and Kim [2] proposed a novel efficient access control scheme for the WBANs based on identity-based signcryption (IBSC) [12] (hereafter called CK). The signcryption method adopted in the CK scheme can simultaneously authenticate the users and protect the request messages. The scheme effectively solves the problem of a single point of failure in the traditional public-key infrastructure-supported system (PKI) by providing key generation and key management services without any assumption of pre-fixed trust relationship between network devices. However, CK has the key escrow problem since it is based on the IBSC. In 2016, Li and Hong [8] demonstrated an efficient certificateless access control scheme for the WBANs by using certificateless signcryption (CLSC) with public verifiability and ciphertext authenticity (hereafter called LH). The scheme can solve the key escrow problem and avoid the use of public key certificates. The controller could verify the validity of a ciphertext before decryption. Then Li *et al.* [7] proposed a novel certificateless signcryption scheme and designed a cost-effective and anonymous access control scheme for the WBANs with the novel signcryption (hereafter called LHJ). They reported that the proposed access control scheme achieved various securities and had the least computational cost and total energy consumption of the controller. However, the above two schemes may not be good choices since they require some costly bilinear pairing operations. The computational cost of a bilinear pairing operation is approximately twenty times higher than that of scale multiplication [6]. These costly operations are a heavy burden for resource-limited sensor nodes.

In this paper, we proposed an efficient access control scheme with certificateless signcryption for WBANs. The main contributions are:

1) A CLSC scheme without using bilinear pairing operation is proposed, and an efficient access control scheme for WBANs is constructed. The use of CL-PKC eliminates the burden of certificate management and solves the key escrow problem.

2) The correctness of the CLSC scheme is verified from the aspects of the partial key, the ciphertext and the signature.

3) It is formally proved that the scheme is semantically secure against indistinguishability-certificateless signcryption-adaptive chosen ciphertext attacks (IND-CLSC-CCA2) based on the hardness of the Computational Diffie-Hellman (CDH) problem and existential unforgeability-certificateless signcryption-chosen message attack (EUF-CLSC-CMA) based on the hardness of the Discrete Logarithm (DL) problem.

4) The security attributes of the scheme are analyzed.

5) Compared with three other access control schemes utilizing signcryption, the scheme is characterized by the lowest computational cost and energy consumption for the controller.

2 Preliminary

In this section, we present some mathematical assumptions, the security model and the network model.

2.1 Computational Assumptions

Definition 1. *Computational Diffie-Hellman (CDH). Given a 3-tuple* (p, aP, bP) *for two unknown elements* $a, b \in Z_q^*$, *here* G *is a group with prime order* q *and* P *is a generator of* G, *the CDH problem is to compute the value* abP *from* aP *and* bP. *The advantage of any probabilistic polynomial time algorithm* A *in solving the CDH problem in* G *is defined as* $Adv_A^{CDH} = Pr[A(p, aP, bP) = abP | a, b \in Z_q^*]$. *The CDH assumption is that the advantage* Adv_A^{CDH} *is negligibly small for any probabilistic polynomial time algorithm* A.

Definition 2. *Discrete Logarithm (DL). Given a 2-tuple* $(P, \mu P)$ *for an unknown element* $\mu \in Z_q^*$, *here* G *is a group with prime order* q *and* P *is a generator of* G, *the DL problem is to find the value* μ. *The advantage of any probabilistic polynomial time algorithm* A *in solving the DL problem in* Z_q^* *is defined as* $Adv_A^{DL} = Pr[A(P, \mu P) = \mu | \mu \in Z_q^*]$. *The DL assumption is that the advantage* Adv_A^{DL} *is negligibly small for any probabilistic polynomial time algorithm* A.

2.2 Security Model

All CLSC schemes may be subjected to two types of attacks [20]: Type-I adversary A_1 and Type-II adversary A_2.

Type-I adversary: The adversary A_1 is not accessible the master key, but he can replace public keys at his will. Therefore, the adversary A_1 is also called malicious user.

Type-II adversary: The adversary A_2 is accessible to the master key, but he cannot replace user's public keys. It represents a malicious KGC who generates partial private key of users.

Definition 3. *Confidentiality. A certificateless signcryption scheme is semantically secure against indistinguishability-certificateless signcryption-adaptive chosen ciphertext attacks (IND-CLSC-CCA2) if there is not a probabilistic polynomial time adversary* $A_{i(i=1,2)}$ *that has the non-negligible advantage in winning the game [20].*

Definition 4. *Unforgeability. A certificateless signcryption scheme is semantically secure against existential unforgeability-certificateless signcryption-chosen message attack (EUF-CLSC-CMA) if there is not a probabilistic polynomial time adversary* $A_{i(i=1,2)}$ *with the non-negligible advantage in winning the game [20].*

2.3 Network Model

The IEEE 802.15.6 working group has considered WBANs to operate in a one-hop or two-hop star topology. The node being placed on a location like the waist is the center of the star topology and controls the communication in WBANs [13]. Here we consider the one-hop star topology and all nodes in the WBANs are directly connected to the controller which all nodes talk. The WBANs contains some sensor nodes and a controller. Sensor nodes in, on or around the body collect vital signals of the patient and regularly transfer them to the corresponding controller. The controller aggregates information from the sensor nodes and communicates with the Internet. Figure 1 shows the overview of the network model of our WBANs applications. The framework is mainly composed of three entities: a Server Provider (SP), the WBANs of a patient, and a user (e.g. a physician, a researcher or an emergency). The SP deploys the WBANs and is responsible for the registration both of users and patients. The SP plays the role of KGC in the CLCS scheme and produces the partial key for any entity which registers at the SP. We suppose that the SP is honest. However, in practices, we do not need to fully trust the SP since it only knows the partial private key of the entity.

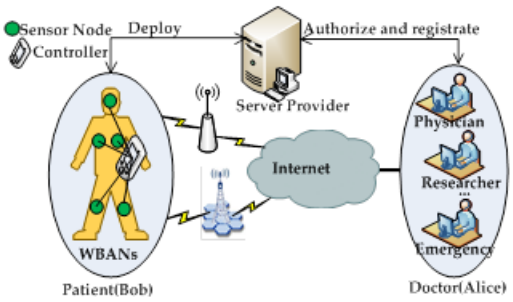

Figure 1: Network model of our WBANs applications

Here's a practical example. We assume that a patient Bob is hospitalized and the SP has deployed the WBANs of Bob. Bob's private key has generated when he registered at the SP. Sensor nodes in WBANs collect Bob's profile and medical records and transfer them to the controller. Doctor Alice has registered at the SP, and the SP has allocated expire data for Alice. When Alice needs to access the data of Bob, she first sends an access request message to Bob. Then Bob checks whether the Alice has the access privilege to his medical data. If Alice is authorized, Alice communicates with Bob to get the vital sign data in order to provide the better medical care service. Otherwise, Bob refuses the access request.

3 Construction of the Access Control Scheme

In this section, we first propose a CLSC scheme without using bilinear pairing operation. Then we construct an efficient access control scheme with the proposed CLSC scheme.

3.1 The Proposed CLSC Scheme

The CLSC scheme Π = (Setup, PartialKeyGen, KeyGen, Sign, UnSign) consists of five algorithms.

Setup: Given a security parameter k, the SP chooses cyclic group G of a large prime order q, a generator P of G, and three security hash functions $H_1 : \{0,1\}^* \times G \rightarrow Z_q^*$, $H_2 : \{0,1\}^* \rightarrow Z_q^*$ and $H_3 : Z_q^* \rightarrow \{0,1\}^{l_0+|Z_q^*|}$. Here l_0 is the number of bits of a message to be sent, and $|Z_q^*|$ is the number of bits of the element in Z_q^*. Then the SP selects the system's master key $z \in Z_q^*$ at random and computes the corresponding public key $y = zP$. Finally, the SP distributes the system parameters $params = (G, q, P, y, H_1, H_2, H_3)$ and keeps the master key z secretly.

Partial Key Generation (PartialKeyGen): When entities want to register his/her identity ID_i to the SP, he/she first sends ID_i to the SP. Then the SP selects random number $r_i \in Z_q^*$, computes $R_i = r_iP$ and $d_i = r_i + zH_1(ID_i, R_i)$. Finally, the SP sets d_i as the entity's partial private key and R_i as the entity's partial public key, and transfers (d_i, R_i) to the entity over a confidential and authentic channel.

Key Generation (KeyGen): When the entity receiving the partial key generated by SP, he/she needs to choose another part of key and generate his/her full key. The entity selects secret value $x_i \in Z_q^*$ at random and computes $X_i = x_iP$. Then the entity sets $SK_i = (d_i, x_i)$ as his/her private key and $PK_i = (R_i, X_i)$ as his/her public key.

Here, we assume that the access request is sent by doctor Alice whose identity is ID_A, and the receiver is patient Bob whose identity is ID_B in our CLSC scheme. Alice's public key is $PK_A = (R_A, X_A)$ and private key is $SK_A = (d_A, x_A)$. Bob's public key is $PK_B = (R_B, X_B)$ and private key is $SK_B = (d_B, x_B)$. Alice and Bob can verify the correctness of the partial private key and partial public key with the equation $r_AP + H_1(ID_A, R_A)y = d_AP$ and $r_BP + H_1(ID_B, R_B)y = d_BP$ respectively.

Signcryption (Sign): With the system parameters , access plaintext message m, Alice's identity ID_A and private key $SK_A = (d_A, x_A)$, Bob's identity ID_B and public key $PK_B = (R_B, X_B)$, Alice runs following steps to generate the ciphertext $\delta = (s, C, T)$.

1) Selects a random $\beta \in Z_q^*$ and computes $T = \beta P$.
2) Computes $h_1 = H_1(ID_B, R_B)$.
3) Computes $V_A = \beta(X_B + R_B + h_1 y)$.
4) Computes $h = H_2(m||T||ID_A||ID_B||X_A||X_B)$.
5) Computes $s = (x_A + \beta)/(h + d_A + x_A)$.
6) Computes $C = H_3(V_A) \oplus (m||s)$.
7) Outputs a ciphertext $\delta = (s, C, T)$.

UnSigncryption (UnSign): Taking a ciphertext δ, Bob's identity ID_B and private key $SK_B = (d_B, x_B)$, Alice's identity ID_A and public key $PK_A = (R_A, X_A)$ as inputs, Bob execute following steps to complete the verification of signcryption.

1) Computes $V_B = (x_B + d_B)T$.
2) Recover the message $m||s = H_3(V_B) \oplus C$, and complete decryption.
3) Computes $h = H_2(m||T||ID_A||ID_B||X_A||X_B)$.
4) Computes $h_1' = H_1(ID_A, R_A)$.
5) If $s(X_A + R_A + h_1' \cdot y + h \cdot P) = X_A + T$ holds, the message m is valid and Alice communicates with Bob using the session key $H_3(V_A)$ or $H_3(V_B)$. Otherwise return $\perp$.

3.2 Our Access Control Scheme

In this section, with the proposed CLSC scheme, we design an efficient access control scheme with certificateless signcryption for the WBANs. The scheme has four phases: the initialization phase, the registration phase, the authentication and authorization phase, and the revocation phase. We define ED as an expiration date. The access control scheme is summarized in Figure 2.

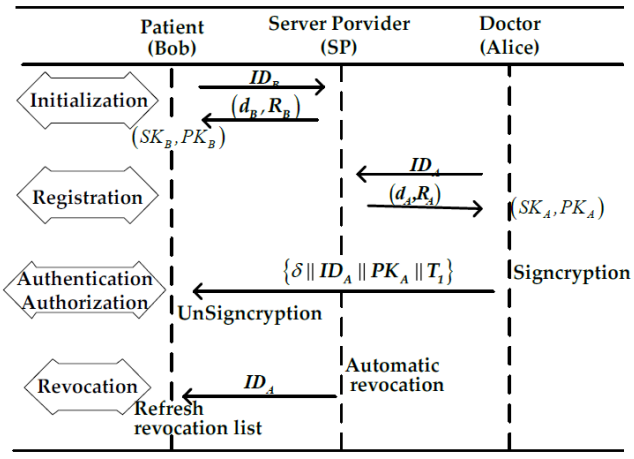

Figure 2: Certificateless access control scheme

3.2.1 Initialization Phase

In this phase, the SP runs Setup algorithm to deploy the WBANs and generate the system parameters. The patient Bob with identity ID_B gets his/her public key $PK_B = (X_B, R_B)$ and private key $SK_B = (x_B, d_B)$. In particular, Bob's communications with Internet are all done by the controller of the WBANs, so Bob also refers to the controller of the WBANs. The SP may run Setup algorithm and PartialKeyGen algorithm.

3.2.2 Registration Phase

Only when the doctor Alice is a registered user of the SP can she access the data of patient Bob. Alice submits his identity ID_A to the SP and then the SP checks whether the identity is valid. If not, the SP rejects the registration request. Otherwise, the SP sets an expiration date ED and runs PartialKeyGen algorithm to produce a partial private key (d_A, R_A). After receiving (d_A, R_A), Alice runs KeyGen algorithm to get the full private key $SK_A = (d_A, x_A)$ and the full public key $PK_A = (R_A, X_A)$.

3.2.3 Authentication and Authorization Phase

When the doctor Alice with the identity ID_A wants to access the monitoring data of the WBANs, Alice firstly produces a request message m and runs Sign algorithm to generate a ciphertext $\delta = (s, C, T)$. To resist the replay attack, we may concatenate the request message and a timestamp to form a new signcrypted message. Then Alice sends the requirement message $\{\delta||ID_A||PK_A||T_1\}$ to Bob, wherein T_1 is the current timestamp. When obtaining the access request from Alice, Bob checks $T_2 - T_1 < \Delta T$ whether holds, wherein T_2 is the current timestamp. If it does not hold, Bob terminates the session. Otherwise, Bob runs Unsign algorithm to complete unsigncryption. When the return value of Unsign algorithm is $\perp$, Bob rejects the request. Otherwise, the request is valid and Alice communicates with Bob using the session key $H_3(V_A)$ or $H_3(V_B)$. This session key has been established between Bob and Alice.

3.2.4 Revocation

The access privilege is automatically revoked by the expired date ED. For example, if the expired date ED is "2017-12-31", the user only can access the WBANs before December 31, 2017. That is to say, the SP will revoke Alice's partial private key and partial public key, which made Alice automatically illegal after December 31, 2017. For some reasons we need to revoke the Alice's access privilege before the expired date, the SP will submit the Alice's identity to Bob, which keeps a list of revoked identities for identifying the validity of users. Bob will add a record to his revocation list and this makes Alice an illegal user.

4 Performance Analysis

In this section, we will analysis the access control scheme. First is the validation of mathematical correctness. Then we demonstrate the scheme is provably secure based on CDH problem and DL problem. Third is the analysis of security property. Finally is the efficiency comparison with three other schemes.

4.1 Correctness of the Proposed CLSC Scheme

4.1.1 Correctness of the Partial Key

Both of Alice and Bob can verify the correctness of the partial key (d_i, R_i) which SP assigned to him/her by following equal.

$$\begin{aligned} & R_i + H_1(ID_i, R_i)y \\ = \; & r_iP + zPH_1(ID_i, R_i) \\ = \; & (r_i + zH_1(ID_i, R_i))P \\ = \; & d_iP. \end{aligned}$$

4.1.2 Correctness of the Ciphertext

The verification of the ciphertext in the UnSign algorithm is obtained from the following:

$$\begin{aligned} V_B &= (X_B + d_B)T \\ &= (x_B + r_B + zH_1(ID_B, R_B))\beta P \\ &= \beta(X_B + R_B + yH_1(ID_B, R_B)) \\ &= V_A. \end{aligned}$$

We will then obtain the following:

$$\begin{aligned} m||s &= H_3(V_B) \oplus C \\ &= H_3(V_A) \oplus H_3(V_A) \oplus (m||s) \\ &= m||s. \end{aligned}$$

4.1.3 Correctness of the Signature

The verification operation of the signature in the UnSign algorithm can be completed by following equation.

$$\begin{aligned} & s(X_A + R_A + h_1'y + hP) \\ = \; & \frac{x_A + \beta}{h + d_A + x_A}(x_AP + r_AP + zH_1(ID_A, R_A)P + hP) \\ = \; & \frac{x_A + \beta}{h + d_A + x_A}(x_A + d_A + h)P \\ = \; & (x_A + \beta)P \\ = \; & x_AP + \beta P \\ = \; & X_A + T. \end{aligned}$$

4.2 Proof of Security

Based on the CDH problem and DL problem in the random oracle model, we prove that the CLSC scheme satisfies confidentiality in the following Theorem 1 and Theorem 2, and unforgeability in the following Theorem 3.

Theorem 1. *(Type-I Confidentiality): In the random oracle model, if there is an adversary A_1 who can win the IND-CLSC-CCA2 game with non-negligible advantage ε, there will be an algorithm $\mathbb{F}$ which can solve the CDH problem with an advantage $Adv_{A_1}^{IND-CLSC-CCA2} \geq \frac{\varepsilon}{q_1^2 q_3}(1 - \frac{1}{q_s+1})^{q_s}\frac{1}{q_s+1}$. Here, the adversary A_1 performs at most q_i hash queries to random oracles $H_{i(i=1,2,3)}$ and q_s signcryption queries.*

Proof. Supposing that there is an adversary A_1 who can break our CLCS scheme. We want to build an algorithm $\mathbb{F}$ that use A_1 to solve CDH problem. The algorithm $\mathbb{F}$ receives an instance (P, aP, bP) of CDH problem to compute abP. $\mathbb{F}$ respectively maintains the lists $L_1, L_2, L_3, L_D, L_{SK}, L_{PK}, L_S, L_U$ to track the oracle model H_1, H_2, H_3, partial key generation, private key generation, public key generation, signcryption, and unsigncryption. Moreover, $\mathbb{F}$ sets the list L_{rec} to record the parameters of the challenge identity. Each list is empty at the beginning.

Setup: Input security parameter k. $\mathbb{F}$ executes Setup algorithm and sends the generated parameters $params = (G, q, P, y, H_1, H_2, H_3)$ to A_1. $\mathbb{F}$ can also simulate the partial key generation, key generation, public key query, public key replacement, signcryption, and un-signcryption oracle to provide responses to A_1's queries.

Find Stage: A_1 can adaptively make a polynomial bounded number of the following queries.

1) H_1 queries: When $\mathbb{F}$ receives the query $H_1(ID, R)$ from A_1, if (ID, R, h_1, c) exists in the list L_1, $\mathbb{F}$ returns h_1 to A_1. Otherwise, $\mathbb{F}$ selects random $c \in \{0, 1\}$, here $Pr[c = 1] = \delta = 1/(q_s + 1)$ [21]. When $c = 0$, $\mathbb{F}$ randomly chooses $h_1 \in Z_q^*$, returns it to A_1, and inserts (ID, R, h_1, c) into the list L_1. When $c = 1$, $\mathbb{F}$ lets $h_1 = k$ and returns k to A_1.
2) H_2 queries: When $\mathbb{F}$ receives the query $H_2(m, T, ID_A, ID_B, X_A, X_B)$ from A_1, if $(m, T, ID_A, ID_B, X_A, X_B, h_2)$ exists in the list L_2, $\mathbb{F}$ returns h_2 to A_1. Otherwise, $\mathbb{F}$ randomly selects $h_2 \in Z_q^*$, and returns it to A_1. Then $\mathbb{F}$ inserts $(m, T, ID_A, ID_B, X_A, X_B, h_2)$ into the list L_2.
3) H_3 queries: When $\mathbb{F}$ receives the query $H_3(T)$ from A_1, if (T, h_3) exists in the list L_3, $\mathbb{F}$ returns h_3 to A_1. Otherwise, $\mathbb{F}$ randomly picks $h_3 \in Z_q^*$, and returns it to A_1. Then $\mathbb{F}$ inserts (T, h_3) to the list L_3.
4) Partial Key queries: A_1 submits a request (ID, d, R). $\mathbb{F}$ checks whether the (ID, d, R) already exists in the list L_D. If it exists, $\mathbb{F}$ returns (d, R) to A_1, otherwise, since $\mathbb{F}$ does not know the master secret key, $\mathbb{F}$ randomly selects $r, z \in Z_q^*$, and computes the entity's partial

private key as $d = r + zH_1(ID, R)$. $\mathbb{F}$ inserts (ID, d, R) into the list L_D and returns (d, R) to A_1.

5) Private Key queries: A_1 submits a request (ID, d, x). $\mathbb{F}$ checks whether the (ID, d, x) already exists in the list L_{SK}. If it exists, $\mathbb{F}$ returns (d, x) to A_1. Otherwise, $\mathbb{F}$ obtains d by partial key queries, then randomly picks $x \in Z_q^*$, inserts (ID, d, x) into the list L_{SK}, and finally returns (d, x) to A_1.

6) Public Key queries: A_1 submits a request (ID, R, X). $\mathbb{F}$ responds as follows:
   - If (ID, R, X) already exists in the list L_{PK}, $\mathbb{F}$ returns (R, X) to A_1.
   - Otherwise, $\mathbb{F}$ checks the list L_d and L_{SK}. If there is the record of the entity with ID, $\mathbb{F}$ can obtain (R, x), then compute $X = xP$, insert (ID, R, X) into L_{PK}, and returns (R, X) to A_1 as a response. If there is no record of ID in the list L_d and L_{SK}, $\mathbb{F}$ checks the list L_1. If $c = 1$, $\mathbb{F}$ randomly picks $r, x \in Z_q^*$, computes $R = rP$, $X = xP$, inserts (ID, R, X) into L_{PK}, and returns (R, X) to A_1. At the same time, $\mathbb{F}$ inserts (ID, r, x, c) into L_{rec}. If $c = 0$, $\mathbb{F}$ runs private key queries, obtains (R, X), inserts (ID, R, X) into L_{PK}, and returns (R, X) to A_1.

7) Replace Public Key queries: A_1 supplies identity ID and a new public key (R', X'). $\mathbb{F}$ replaces the current public key (R, X) by the new key (R', X').

8) Signcryption queries: A_1 supplies two identities (ID_A, ID_B) and a message m. $\mathbb{F}$ checks the (ID_A, R_A) in the list L_1 and responds as follows:
   a. If $c = 0$, $\mathbb{F}$ gets (ID_A, d_A, x_A), (ID_B, R_B, X_B) respectively from the list L_{SK}, L_{PK} according to ID_A, ID_B, runs the Sign algorithm to complete signcryption, and returns ciphertext $\delta = (s, C, T)$ to A_1.
   b. If $c = 1$, $\mathbb{F}$ fails and aborts.

9) Un-Signcryption queries: A_1 supplies two identities (ID_A, ID_B) and a ciphertext $\delta = (s, C, T)$. $\mathbb{F}$ checks the (ID_B, R_B) in the list L_1 and responds as follows:
   a. If $c = 0$, $\mathbb{F}$ gets (ID_A, R_A, X_A), (ID_B, d_B, x_B) respectively from the list L_{PK}, L_{SK} according to ID_A, ID_B, runs the UnSign algorithm to complete unsigncryption, and returns the message m to A_1.
   b. If $c = 1$, $\mathbb{F}$ traverses down (V_B, h_3) of the list L_3, then computes $m||s = H_3(V_B) \oplus C$ and completes the un-signcryption. $\mathbb{F}$ selects h_1' from (ID_A, R_A, h_1', c) in the list L_1, selects R_A, X_A from (ID_A, R_A, X_A) in the list L_{PK}, selects h_2 from $(T, ID_A, ID_B, X_A, X_B, m, h_2)$ in the list L_2, where $h = h_2$, then $\mathbb{F}$ verifies whether the equation $s(X_A + R_A + h_1'y + hP) = X_A + T$ is valid. If the equation holds, then $\mathbb{F}$ outputs m, otherwise $\mathbb{F}$ starts from the next record of the list L_3 and redo Step b. If all the items in the list L_3 have not been returned, then $\mathbb{F}$ outputs $\perp$, which means un-signcryption fails.

Challenge Stage: A_1 can adaptively make two different messages m_0, m_1 with the same length and two challenge identities ID_A, ID_B. $\mathbb{F}$ firstly checks (ID_B, R_B) in the list L_1. If $c = 0$, $\mathbb{F}$ stops. Otherwise, $\mathbb{F}$ makes a Public Key queries to ensure that (x_B, r_B) already exist in the list L_{rec}. Then the algorithm $\mathbb{F}$ selects $s^*, c^* \in Z_q^*$ at random and sets $T^* = \beta P$. $\mathbb{F}$ sends the challenge ciphertext $\delta^* = (s^*, c^*, T^*)$ to A_1.

Guess Stage: A_1 can make a polynomial bounded number of queries like that in the Find stage. Finally, $\mathbb{F}$ outputs her guess c'. If $c' = c$, A_1 can make a query in H_3 with $V' = \beta(X_B + R_B + h_1 y)$. In this case, the candidate answer of the CDH problem is stored in the list L_3. $\mathbb{F}$ ignores the guessed value of A_1, selects V' from the list L_3 at random, and outputs $(V' - (x_B + r_B)T^*)/k = z\beta P$ as the answer to CDH problem, where x_B, r_B, T^*, V' are known to the algorithm $\mathbb{F}$. Otherwise, the algorithm $\mathbb{F}$ does not solve the CDH problem.

The algorithm $\mathbb{F}$ simulates the real attack situation for A_1. If $\mathbb{F}$ is not terminated in the process of simulation and can breach the confidentiality in this paper with non-negligible probability ε, $\mathbb{F}$ outputs the valid answer of the CDH problem.

Now, we evaluate the probability of success. The probability that A_1 runs partial private key queries or private key queries for ID_B is at least $1/q_1^2$. The probability that $\mathbb{F}$ successfully selects V' from the list L_3 as a candidate answer for the CDH problem is $1/q_3$. The non-termination probability is $(1-\delta)^{q_s}$ in the find stage. The non-termination probability is δ in the challenge stage. Therefore, the probability that $\mathbb{F}$ does not abort during the simulation is at least $\frac{\varepsilon}{q_1^2 q_3}(1 - \frac{1}{q_s+1})^{q_s}\frac{1}{q_s+1}$.

To sum up, if the algorithm $\mathbb{F}$ does not abort in the simulation process and A_1 can break the confidentiality of our signcryption scheme with the non-negligible advantage ε, $\mathbb{F}$ can output the valid solution of CDH problem with the advantage $Adv_{A_1}^{IND-CLSC-CCA2} \geq \frac{\varepsilon}{q_1^2 q_3}(1 - \frac{1}{q_s+1})^{q_s}\frac{1}{q_s+1}$. □

Theorem 2. *(Type-II Confidentiality): In the random oracle model, if there is an adversary A_2 who can win the IND-CLSC-CCA2 game with a non-negligible advantage*

ε, there will be an algorithm $\mathbb{F}$ that solves the CDH problem with an advantage $Adv_{A_2}^{IND-CLSC-CCA2} \geq \frac{\varepsilon}{q_1^2 q_3}(1-\frac{1}{q_s+1})^{q_s}\frac{1}{q_s+1}$. Here, the adversary A_2 performs at most q_i hash queries to random oracles $H_{i(i=1,2,3)}$ and q_s signcryption queries.

Proof. The proof idea is similar to Theorem 1 except the following aspects.

1) The adversary A_2 knows the system master key z.
2) In the Public Key queries, we set $R = zP$ other than $R = rP$, and we insert $(ID, -, x, c)$ into L_{rec} other than (ID, r, x, c).
3) In the guess stage, $\mathbb{F}$ outputs $V' - (x_B + kz)T^* = z\beta P$ as the answer to CDH problem.

□

Theorem 3. *(Unforgeability): In the random oracle model, if there is an adversary $A_{i(i=1,2)}$ who can win the EUF-CLSC-CMA game with non-negligible advantage ε, there will be an algorithm $\mathbb{F}$ that solves the DL problem with an advantage $Adv_{A_i(i=1,2)}^{EUF-CLSC-CMA} \geq \frac{\varepsilon}{9q_1^2}(1-\frac{1}{q_s+1})^{q_s}$. Here, the adversary $A_{i(i=1,2)}$ performs at most q_1 hash queries to random oracles $H_{i(i=1,2,3)}$ and q_s signcryption queries.*

Proof. Supposing that there is an adversary $A_{i(i=1,2)}$ who can break our CLCS scheme. We want to build an algorithm $\mathbb{F}$ which uses $A_{i(i=1,2)}$ to solve DL problem. The algorithm $\mathbb{F}$ receives an instance $(P, \mu P)$ of the DL problem and his goal is to compute μ.

Setup: The algorithm $\mathbb{F}$ set $y = \mu p$ for the adversary A_1. The other settings are the same as those in Theorem 1 for A_1. The algorithm $\mathbb{F}$ set $y = zp$ for the adversary A_2. The other settings are the same as those in Theorem 2 for A_2.

Queries: The adversary A_1 can adaptively make a polynomial bounded number of queries like those in Theorem 1, whereas the adversary A_2 can adaptively make the queries like those in Theorem 2.

Forgery: After a polynomial bounded number of queries, $A_{i(i=1,2)}$ outputs a faked ciphertext $\delta^* = (s^*, c^*, T^*)$ on message m^* with ID_A as the sender and ID_B as the receiver.

The algorithm $\mathbb{F}$ first checks the list L_1. If $c = 0$, $\mathbb{F}$ aborts. Otherwise, $\mathbb{F}$ can get the private key of ID_B, compute $V_B^* = (x_B + d_B)T^*$ and get h_3^* by H_3 queries with V_B^*. $\mathbb{F}$ recovers m^*, s^* by h_3^* and verifies the δ^*. If the $A_{i(i=1,2)}$ has successfully forged a user, $\mathbb{F}$ can get two legal signatures $(m^*, ID_A, ID_B, T^*, h, s_1)$ and $(m^*, ID_A, ID_B, T^*, h', s_1)$ with the Splitting Lemma [15], where $h \neq h'$. Thus, we get $T^* = \beta P = (s_1(h + d_A + x_A) - x_A)P = (s_2(h' + d_A + x_A) - x_A)P$ and $s_1(h + d_A + x_A)) = s_2(h' + d_A + x_A))$.

For Type-I attack A_1, it is $s_1(h + r_A + \mu k + x_A) = s_2(h' + r_A + \mu k + x_A)$, where $k = h_1 = H_1(ID_A, R_A)$. Only μ is unknown in this formula, so μ can be computed.

For Type-II attack A_1, it is $s_1(h + r_A + zk + x_A) = s_2(h' + r_A + zk + x_A)$, where $k = h_1 = H_1(ID_A, R_A)$. Only r_A is unknown in this formula, so r_A can be solved. We have set $R = r_A P = \mu P$ in the Public Key queries, so μ can be computed.

Now, we evaluate the probability of success. The probability that A_1 runs partial private key queries or private key queries for ID_A is at least $1/q_1^2$. The non-termination probability is $(1-\delta)^{q_s}$ in the find stage. The probability of failure is less than $1/9$ when two or more effective ciphertexts are produced with the oracle replay technique [15]. Therefore, the probability that $\mathbb{F}$ can solve the DL problem is at least $\frac{1}{9q_1^2}$. Thus, the probability that $\mathbb{F}$ successfully forges a user is at least $\frac{\varepsilon}{9q_1^2}(1-\frac{1}{q_s+1})^{q_s}$. □

4.3 Analysis of Security Properties

In the authentication and authorization phase, the session key is only known by the patient Bob and the doctor Alice, the scheme can achieve the confidentiality for future communication between them. In addition, the scheme uses the proposed CLSC scheme that is proved to have confidentiality in theorem1 and theorem2 and unforgeability in theorem 3, so the access control achieves confidentiality property and unforgeability property. The non-repudiation of the access request is guaranteed by introducing the timestamp. Owing to the characteristics of the CL-PKC, the access control can solve key escrow problem and avoid the use of public key certificates. When we design the CLSC scheme, we don't use bilinear pair operations, so our scheme avoids the bilinear pairing operation. Table 1 is the security properties comparing of the four schemes.

4.4 Efficiency Comparisons

In this section, we analyze the performance of our access control scheme in regard to energy consumption and communication overhead. Firstly, we compare the scheme with other three schemes of CK [2], LH [8] and LHJ [7] in computation efficiency and communication efficiency. The computation efficiency is determined by the computational cost of algorithm and the communication efficiency is determined by the length of ciphertext and public key. The symbol P denotes pairing operation, the symbol E denotes an exponentiation operation, the symbol M denotes a point multiplication operation. Let $|*|$ denote the length of element $*$. For example, $|G|$ denotes the length of element in group G and $|m|$ denotes the length of message space. As can be seen from Table 2, our scheme has the lower computational cost than the other three schemes for both Alice and Bob. Here, we neglect the cost of other operations because they are much smaller than the above three operations.

Table 1: Comparisons of security properties

	CK [2]	LH [8]	LHJ [7]	Our scheme
Confidentiality	√	√	√	√
Unforgeability	√	√	√	√
Authentication	√	√	√	√
Non-repudiation	√	√	√	√
No certificate	√	√	√	√
No key escrow	×	√	√	√
Without bilinear pairing	×	×	×	√

Abbreviations: √: Scheme prevents this attack or satisfies the attribute, ×: Scheme fails to prevent the attack or does not satisfy the attribute.

Table 2: Performance evaluation of the four schemes

Schemes	Computational Cost (Alice)	Computational Cost (Bob)	Communication Cost (Bob)
CK [2]	1P+3M	3P+M	$2\|G_1\| + \|ID\| + \|m\|$
LH [8]	2E	1P+1M+1E	$\|G_1\| + \|G_2\| + 3\|Z_p^*\| + \|ID\| + \|m\|$
LHJ [7]	1E+4M	2P+2M+1E	$3\|G_1\| + \|ID\| + \|m\|$
Ours	3M	4M	$5\|Z_q^*\| + \|ID\| + \|m\|$

Quantitative evaluation results for the four schemes are described below. Here, we only consider Bob's overhead, because his controller's resource is limited. We adopt the result in [14, 17] on the MICA2 mote which is equipped with an ATmega128 8-bit processor locked at 7.3728 MHz, 128KB ROM, and 4KB RAM. A pairing operation costs 1.9 s and an exponentiation operation costs 0.9 s by using a supersingular curve $y^2 + y = x^3 + x$ with an embedding degree of 4 and implementing an η_T pairing: $E(F_{2^{271}}) \times E(F_{2^{271}}) \rightarrow F_{2^{4271}}$, which is also equivalent to the 80-bit security level. According to the previous results [8], a point multiplication over the supersingular curve costs 0.81 s. Therefore, the computational time on the controller of CK [2], LH [8], LHJ [7], and our scheme are respectively $3 \times 1.9 + 1 \times 0.81 = 6.51$ s, $1 \times 1.9 + 1 \times 0.81 + 1 \times 0.9 = 3.61$ s, $2 \times 1.9 + 2 \times 0.81 + 1 \times 0.9 = 6.32$ s and $4 \times 0.81 = 3.24$ s. We also suppose that the power level of MICA2 is 3.0 V. The current draw in active mode is 8.0 mA and the current draw in receiving mode is 10 mA [15]. For energy consumption, according to the evaluation method [11,16], a pairing operation consumes $3.0 \times 8.0 \times 1.9 = 45.6$ mJ, a point multiplication operation consumes $3.0 \times 8.0 \times 0.81 = 19.44$ mJ, an exponentiation operation in G_2 consumes $3.0 \times 8.0 \times 0.9 = 21.6$ mJ. Therefore, the computational energy consumption on the controller of CK [2], LH [8], LHJ [7] and our scheme are $3 \times 45.6 + 1 \times 19.44 = 156.24$ mJ, $1 \times 45.6 + 1 \times 19.44 + 1 \times 21.6 = 86.64$ mJ, $2 \times 45.6 + 2 \times 19.44 + 1 \times 21.6 = 151.68$ mJ and $4 \times 19.44 = 77.76$ mJ respectively.

Figure 3 and Figure 4 respectively describe the computational time and energy consumption of the controller. It is clear that our scheme has the shortest computational time and least energy consumption among the four schemes.

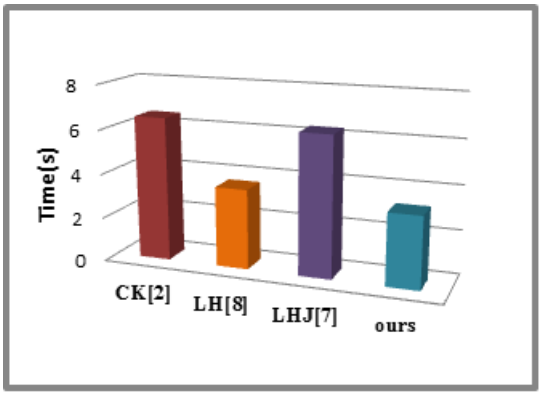

Figure 3: The computational time of the controller

For the communication cost, we suppose that $|m| = 160$ bits and $|ID| = 80$ bits. CK [2], LH [8], LHJ [7] schemes use a curve over the binary field $F_{2^{271}}$ with the G_1 of 252-bit prime order. As in [12, 17], the size of an element in group G_2 is 542 bits and can be compressed to 34 bytes. The size of an element in group G_2 is 1084 bits and can be compressed to 136 bytes. The size of an element of Z_q^* is 32 bytes. In CK [2], LH [8], LHJ [7] and our scheme, the controller needs to receive $2|G_1| + |ID| + |m|$ bits$=2 \times 34 + 10 + 20 = 98$ bytes, $|G_1| + |G_2| + 3|Z_p^*| + |ID| + |m|$ bits$=34 + 136 + 3 \times 32 + 10 + 20 = 296$ bytes, $3|G_1| + |ID| + |m|$ bits$=3 \times 34 + 10 + 20 = 132$ bytes, and $5|Z_q^*| + |ID| + |m|$ bits$=5 \times 32 + 10 + 20 = 190$ bytes respectively. From [12, 17], we know the controller

Table 3: Energy consumption of the four schemes

Schemes	Computational energy consumption (mJ)	Communication energy consumption (mJ)	Total energy consumption (mJ)
CK [2]	156.24	1.86	158.1
LH [8]	86.64	5.62	92.26
LHJ [7]	151.68	2.51	154.19
Ours	77.76	3.61	81.37

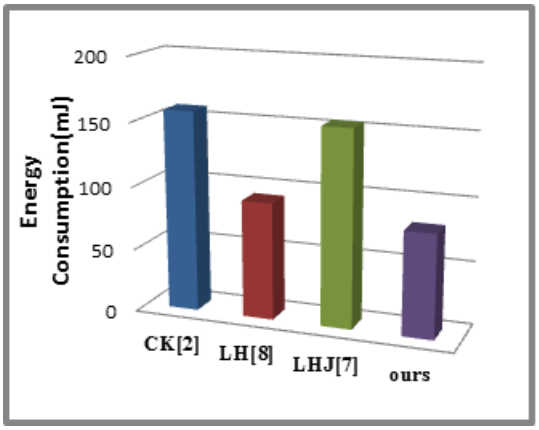

Figure 4: The energy consumption of the controller

takes $3 \times 10 \times 8/12400 = 0.019$ mJ to receive one-byte message. Therefore, in CK [2], LH [8], LHJ [7] and our scheme, communication energy consumption values of the controller are $0.019 \times 98 = 1.86$ mJ, $0.019 \times 296 = 5.62$ mJ, $0.019 \times 132 = 2.51$ mJ, and $0.019 \times 190 = 3.61$ mJ respectively. The total energy consumption of CK [2], LH [8], LHJ [7] and our schemes are $156.24 + 1.86 = 158.1$ mJ, $86.64 + 5.62 = 92.26$ mJ, $151.68 + 2.51 = 154.19$ mJ, and $77.76 + 3.61 = 81.37$ mJ respectively. Table 3 provides energy consumption of four schemes. Although the communication cost of our scheme is more than that of CK [2] and LHJ [7], the total energy consumption of our scheme is less than that of other three schemes. The controller's energy consumption of computation and communication in our scheme is almost half of that in CK [2] and LHJ [7].

5 Conclusions

In this paper, we proposed a new CLSC scheme without using bilinear pairing operation and constructed an efficient access control scheme using the proposed CLSC scheme for the WBANs. We verified the mathematical correctness of the CLSC scheme from the aspect of the partial key, the ciphertext and the signature. Then we proved that the proposed scheme offered confidentiality and unforgeability in the random oracle model on the basis of the hardness of the CDH problem and the DL problem respectively. Moreover, we have analyzed the security property and concluded that our scheme satisfy more security property than three others schemes. As far as performance analysis is concerned, our access control scheme had the shortest computational time and the least energy consumption compared with the existing three access control schemes utilizing signcryption.

Acknowledgements

This work is supported by the Key Research and Development Program of Shanxi Province under Grant No.201703D121042-1.

References

[1] S. K. Balakrishnan and V. P. Jagathy Raj, "Practical implementation of a secure email system using certificateless cryptography and domain name system", *International Journal of Network Security*, vol. 18, no. 1, pp. 99-107, 2016.

[2] G. Cagalaban and S. Kim, "Towards a secure patient information access control in ubiquitous healthcare systems using identity-based signcryption", in *Proceedings of 13th International Conference on Adv. Commun. Technol. (ICACT'11)*, pp. 863-867, 2011.

[3] L. Cheng and Q. Wen, "An improved certificateless signcryption in the standard model", *International Journal of Network Security*, vol. 17, no. 5, pp. 597-606, 2015.

[4] G.Gao, X. Peng, Y. Tian and Z. Qin, "A chaotic maps-based authentication scheme for wireless body area networks", *International Journal of Distributed Sensor Networks*, vol. 12, no. 7, pp. 2174720-2174720, 2016.

[5] M. Hassouna, B. Barry, and E. Bashier, "A new level 3 trust hierarchal certificateless public key cryptography scheme in the random oracle model", *International Journal of Network Security*, vol. 19, no. 4, pp. 551-558, 2017.

[6] D. He, J. Chen, and J. Hu, "An ID-based proxy signature schemes without bilinear pairings", *Annals of Telecommunications*, vol. 66, no. 11-12, pp. 657-662, 2011.

[7] F. Li, Y. Han, and C. Jin, "Cost-effective and anonymous access control for wireless body area networks",

IEEE Systems Journal, vol.12, no. 1, pp. 747-758, 2018.

[8] F. Li and J. Hong, "Efficient certificateless access control for wireless body area networks", *IEEE Sensors Journal*, vol. 16, no. 13, pp. 5389-5396, 2016.

[9] F. Li, J. Hong, and A. A. Omala, "Efficient certificateless access control for industrial Internet of things", *Future Generation Computer Systems*, vol. 76, pp.285-292, 2017.

[10] M. Luo, Y. Wan, and D. Huang, "Certificateless hybrid signcryption scheme with known session-specific temporary information security", *International Journal of Network Security*, vol. 19, no. 6, pp. 966-972, 2017.

[11] C. Ma, K. Xue, and P. Hong, "Distributed access control with adaptive privacy preserving property for wireless sensor networks", *Security and Communication Networks*, vol. 7, no. 4, pp. 759-773, 2014.

[12] M. Mandal, G. Sharma, and A. K. Verma, "A computational review of identity-based signcryption schemes", *International Journal of Network Security*, vol. 18, no. 5, pp. 969-977, 2016.

[13] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: a survey", *IEEE Communication Surveys & Trtorials*, vol. 16, no. 3, pp. 1658-1686, 2014.

[14] L. B. Oliveira, D. F. Aranha, et al., "TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks", *Computer Communications*, vol. 34, no. 3, pp. 485-493, 2011.

[15] Z. Shao, Y. Gao, "A provably secure signature scheme based on factoring and discrete logarithms", *Applied Mathematics & Information Sciences*, vol. 8, no. 4, pp. 1553-1558, 2014.

[16] K. A. Shim, "S2DRP: Secure implementations of distributed reprogramming protocol for wireless sensor networks", *Ad Hoc Networks*, vol. 19, pp. 1-8, 2014.

[17] K. A. Shim, Y. R. Lee, and C. M. Park, "EIBAS: An efficient identity-based broadcast authentication scheme in wireless sensor networks", *Ad Hoc Network*, vol. 11, no. 1, pp. 182-189, 2013.

[18] Y. Tian, Y. Peng, X. Peng, and H. Li, "An attribute-based encryption scheme with revocation for fine-grained access control in wireless body area networks", *International Journal of Distributed Sensor Networks*, vol. 10, pp. 713541-173541, 2014.

[19] Y. Tian, Y. Peng, G. Gao, and X. Peng, "Role-based access control for body srea networks using attribute-based encryption in cloud storage", *International Journal of Network Security*, vol. 17, no. 5, pp. 597-606, 2015.

[20] C. Zhou, G. Gao, and Z. Cui, "Certificateless signcryption in the standard model", *Wireless Personal Communications*, vol.92, no. 2, pp. 495-513, 2017.

[21] Y. Zhou, B. Yang, and W. Zhang, "Provably Secure and Efficient Certificateless Generalized Signcryption Scheme", *Chinese Journal of Computers*, vol. 39, no. 3, pp. 543-551, 2016.

Biography

Gaimei Gao received the M.E from Taiyuan University of Science and technology, China, in 2007. She is currently a ph.D.student in Taiyuan university of technology and a lecture in Taiyuan University of Science and Technology. Her current research interests are in the area of wireless body area networks and information security.

Xinguang Peng received the D.E from Beijing Institute of technology, China in 2004. He is now a professor and doctoral supervisor in college of computer science and technology, Taiyuan University of Technology, Taiyuan, China. His research interests include information security and trusted computing.

Lizhong Jin received the M.E in Computer Science and Technology in 2005 from Taiyuan University of Technology, China. He is currently a Ph.D. student at Taiyuan University of Technology. His research interests include Pattern Recognition, data mining and Big Data Analysis and Application.