Computer Systems
Science and Engineering

Tech Science Press

DOI: 10.32604/csse.2023.040483
Article

An Efficient Heterogeneous Ring Signcryption Scheme for Wireless Body Area Networks

Qingqing Ning, Chunhua Jin*, Zhiwei Chen, Yongliang Xu and Huaqi Lu

Faculty of Computer & Software Engineering, Huaiyin Institute of Technology, Huai'an, 233003, China
*Corresponding Author: Chunhua Jin. Email: xajch0206@163.com

Received: 20 March 2023; Accepted: 15 May 2023; Published: 28 July 2023

Abstract: Wireless body area networks (WBANs) are an emerging technology for the real-time monitoring of physiological signals. WBANs provide a mechanism for collecting, storing, and transmitting physiological data to healthcare providers. However, the open wireless channel and limited resources of sensors bring security challenges. To ensure physiological data security, this paper provides an efficient Certificateless Public Key Infrastructure Heterogeneous Ring Signcryption (CP-HRSC) scheme, in which sensors are in a certificateless cryptosystem (CLC) environment, and the server is in a public key infrastructure (PKI) environment. CLC could solve the limitations of key escrow in identity-based cryptography (IBC) and certificate management for public keys in PKI. While PKI is suited for the server because it is widely used on the Internet. Furthermore, this paper designs a ring signcryption method that allows the controller to anonymously encrypt physiological data on behalf of a set of sensors, but the server does not exactly know who the sensor is. The construction of this paper can achieve anonymity, confidentiality, authentication, non-repudiation, and integrity in a logically single step. Under the computational Diffie-Hellman (CDH) problem, the formal security proof is provided in the random oracle model (ROM). This paper demonstrates that this scheme has indistinguishability against adaptive chosen ciphertext attacks (IND-CCA2) and existential unforgeability against adaptive chosen message attacks (EUF-CMA). In terms of computational cost and energy usage, a comprehensive performance analysis demonstrates that the proposed scheme is the most effective. Compared to the three existing schemes, the computational cost of this paper's scheme is reduced by about 49.5%, 4.1%, and 8.4%, and the energy usage of our scheme is reduced by about 49.4%, 3.7%, and 14.2%, respectively.

Keywords: Wireless body area networks; certificateless cryptosystem; public key infrastructure; security; ring singncryption

1 Introduction

WBANs are a collection of different smart medical sensors placed in patients' bodies [1–3]. These sensors are small, portable, and intercommunicating devices that can be implanted or worn to monitor the critical signs of a patient. WBANs can assist doctors in checking patients' health states in real-time by the analysis of physiological data, including heart rate and sleep quality, etc. They also can be applied in the fields of health management and sports tracking. The sensors can collect a patient's movement trail and transmit the physiological information to the servers for analysis and treatment [4–6]. WBANs bring convenient for some patients since they no longer need to go to the hospital often. In addition, they improve the efficacy of healthcare because some diseases and emergency medical responses can be performed remotely. Therefore, WBANs are vital for the creation of a highly trustworthy, ubiquitous healthcare system. Because collected physiological data by the WBANs is sensitive and must be kept secret, unauthorized parties cannot access these data [7–9]. On open channels, users from different network domains are susceptible to various security attacks during the transmission of physiological information, and some of the collected data is scattered. Most body area network connections rely on the star network connection of the central node. If the aggregation node is breached during the communication process, and the data is stolen and tampered with by malicious users, it may cause serious consequences. In addition, resource differences must also be considered, as sensors have resource constraints such as limited computing, storage, bandwidth, and energy capacity, while servers have powerful computing and storage capabilities [10]. Therefore, it isn't simple to design an efficient heterogeneous security scheme to satisfy these features [11,12]. To further ensure that the patient's medical data will not be leaked, this article can use ring signcryption technology to optimize the scheme.

1.1 Related Work

Due to the important role of health data stored in WBANs in medical treatment, researchers must address security issues in WBANs before truly developing them. Recently, people have proposed some secure WBANs schemes from different perspectives. It's worth mentioning that Hu et al. [13] described an approach to preserve the user and WBAN's communication. Their proposal is attribute-based encryption (ABE) [14]. But ABE couldn't be the best option due to its expensive cryptographic operations. These expensive activities are a challenge for sensor nodes with limited resources [15,16]. Rehman et al. [17] proposed an efficient lightweight key agreement and authentication scheme for WBAN. Their scheme has shown effectiveness in resisting various known network attacks, such as sensor node simulation attacks, but still has significant computational overhead.

Wu et al. [18] proposed a lightweight dual-factor authentication scheme for WBANs. Their scheme claims to be resistant to internal attacks, offline guessing attacks and session key leakage attacks, but the scheme cannot guarantee forward security. Signing first and then encrypting is a traditional solution. This scheme is inefficient because the calculation time and communication consumption are equal to the sum of signature consumption and encryption consumption. To address the problem of the traditional scheme's low efficiency, the initial signcryption scheme proposed by Zheng [19] has demonstrated that signcryption consumption is significantly less than the total signature and encryption consumption. At once, the signcryption scheme reduces the computational complexity and communication demands during data transmission by a significant amount.

Tan et al. [20] designed an identity-based signcryption scheme for WBANs. Unlike traditional PKI, which requires a certificate to associate an identity with the public key, IBC eliminates complex certificate management. The user's public key is generated from identity information, including id numbers, phone numbers, and so on. A trusted third party that generates a user's private key is referred to as a private key generator (PKG). IBC is perfectly suited for resource-constrained WBANs, and because PKG has the private key of every user, IBC will inevitably encounter key escrow problems [21,22]. Liu et al. [23] designed the authentication scheme for WBANs using CLC. Every user must be authorized to gain access to health data stored on servers. The advantage of Liu's scheme is the use of CLC, and there is no public key certificate problem or key escrow problem [24,25]. The CLC still requires KGC, which is tasked with creating a partial private key from the master key and an individual's identification. The user then creates a secret value and mixes it with a partial private key to create the complete private key [26]. Because KGC lacks the secret value, it couldn't obtain a complete private key. So, the key escrow issue is overcome.

To ensure integrity, non-repudiation, confidentiality, and authentication during the communication process, this article provides an effective CP-HRSC system from the WBANs in CLC to an Internet server in PKI. Compared to current schemes [27], this paper's solution not just to guarantees a greater level of security and reduces computation and communication costs.

1.2 Motivation and Contribution

This paper aims to design an efficient CP-HRSC scheme for WBANs. This paper's goal is not only to solve the above-mentioned problems, but also to reduce the computational and communication cost in a way that provides integrity and confidentiality. In addition, this paper's solution adopts heterogeneous systems and ring signcryption technologies, which are better suited for transmitting data in WBANs. WBANs represent the sender and servers represent the receiver. This paper's contributions are listed below:

(1) This article provides a heterogeneous signcryption scheme between the WBANs and server, in which the server is in PKI and the WBANs are in CLC. CLC could solve the limitations of key escrow problems in IBC and public key certificate management in PKI.
(2) The ring signcryption is a mechanism that allows the controller to anonymously signcrypt physical data on behalf of a set of sensors. This preserves the sensor's privacy by keeping its identity hidden from the server. Instead, the server just knows that the data was signcrypted by a member of a ring of sensors, it can not determine the exact identity of the sensor who signcrypts the message.
(3) This paper's scheme provides anonymity, confidentiality, integrity, non-repudiation, and authentication. It is proven IND-CCA2 and EUF-CMA in ROM.
(4) The analysis of performance indicates that this paper's solution is the most effective in terms of computational cost and energy usage. Compared with the other three related schemes [27–29], the computational cost of our scheme is reduced by about 49.5%, 4.1%, and 8.4%, and energy usage of our scheme is reduced by about 49.4%, 3.7%, and 14.2%, respectively.

1.3 Organization

The remainder of the paper is structured as follows: Section 2 describes the network model and security requirements. A CP-HRSC scheme is proposed in Section 3. In Section 4, this article analyzes the security and performance of the scheme. The application of this paper's scheme is shown in Section 5. Finally, the conclusion is described in Section 6.

2 Preliminaries

In this chapter, this article describes network model and security requirements.

2.1 *Network Model*

Fig. 1 depicts the conventional WBANs model. Most of the network model is made up of three objects: patients, service providers (SP), and users (e.g., a hospital, a nurse, a doctor, a research institution, etc.). The WBANs consist of a controller and several sensor nodes [30,31]. The sensors and controller can communicate with each other, and the controller can also communicate with the Internet to transmit patients' medical data to the server. If a user wishes to access patients' health records, the server must provide permission. When a user wishes to obtain WBAN's monitoring data, it must first submit a query message to the server. The server then verifies whether or not the user is permitted to access the WBANs. If so, the server transmits the gathered information to the user in a safe manner. If not, it will be rejected.

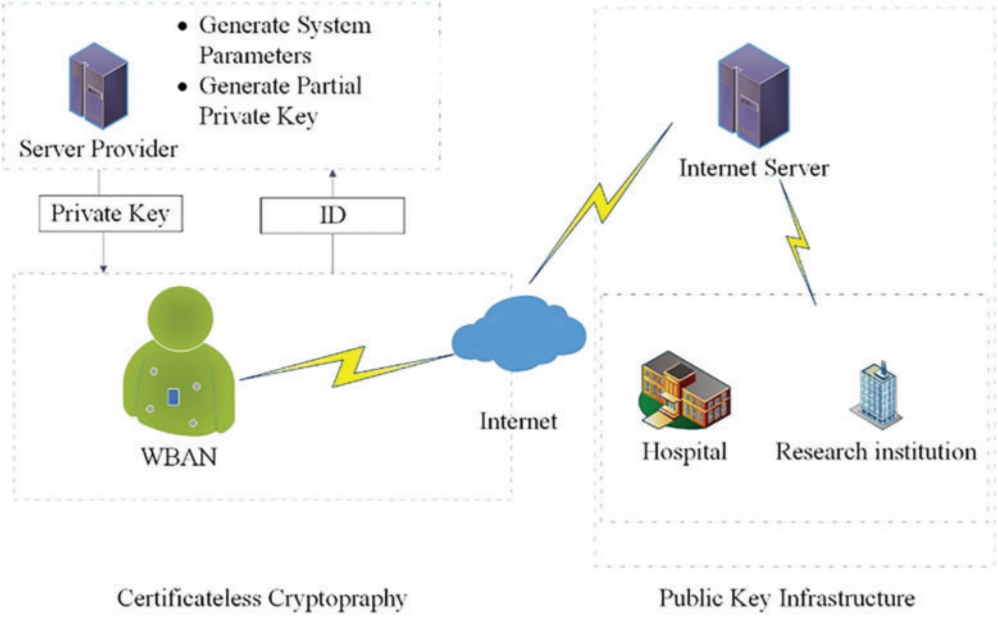
• Generate System Parameters
• Generate Partial Private Key
Server Provider
Private Key
ID
WBAN
Internet
Internet Server
Hospital
Research institution
Certificateless Cryptopraphy
Public Key Infrastructure

Figure 1: Network model

2.2 *Security Requirements*

Five security features (anonymity, confidentiality, integrity, non-repudiation, and authentication) must be satisfied by the sensors and server. The confidentiality of query messages keeps them secret from everyone except for the sender and receiver. Authentication guarantees that just those who have been granted permission can view the medical data stored in the WBANs. Integrity ensures that a user's query message was not modified by unauthorized users. Non-repudiation prevents users from denying their true identity. So, once a user has already sent a request message to WBANs, this activity cannot be denied.

2.3 *Bilinear Pairings*

Suppose that there are two groups, G_1 and G_2 in existence. G_1 is an additive group, while G_2 is multiplicative group that has the same prime order p, P is the generator of G_1. This article states that $e : G_1 \times G_1 \rightarrow G_2$ has the common attributes:

a. Bilinearity: $\forall r, c \in Z_p^*, \forall K, M \in G_1, e(rK, cM) = e(K, M)^{rc}$.

b. Non-degeneracy: $\exists K, M \in G_1$ such that $e(K, M) \neq 1$.
c. Computability: There exists a feasible algorithm to find $e(K, M), \forall K, M \in G_1$.

This paper's scheme's security is dependent just on the difficulty of the following CDH problem. Offered G_1 of order p prime and P, CDH problem in G_1 is to calculate mnP offered (P, mP, nP).

Definition 1. If no adversary $\mathcal{A}$ can solve (ϵ, t)-CDH problem in t-polynomial time with an advantage of at least ϵ, then CDH assumption holds.

3 Proposed Scheme

In this chapter, this article first introduces the basic definition and security concepts of the CP-HRSC scheme, which enables the sender in CLC to transmit the message to the recipient in PKI. Next, this article designs the efficient CP-HRSC scheme and demonstrates its security in ROM. Table 1 contains a listing of this paper's scheme's necessary notations.

Table 1: The symbols mentioned in the article

Symbol	Description
e	A bilinear pairing
s	Master private key of PKG
p	The prime order of G_1 and G_2
Z_p^*	A group of integers that do not contain zero
k	A security parameter
H_i	Hash function ($i = 1, 2, 3$)
G_1	An addition group
$\|\|$	Connection symbol
G_2	A multiple group
L	A sender group with identities $ID_i (i = 1, 2, \ldots, n)$
P	A generator of group G_1
P_{pub}	A master public key of PKG
S_{ID}	A private key of identity ID
x_r	A private key of the receiver
pk_r	A public key of the receiver
$\oplus$	XOR operator

3.1 Syntax

A basic CP-HRSC system comprises eight algorithms listed below.

(1) Setup: It is an initialization algorithm run by PKG. The input is the algorithm's parameter k. The output consists of a master key s and system parameter *params* with P_{pub}.
(2) CLC-PPKE: It is an algorithm for the extraction of partial private keys that is run by PKG. It accepts as input the user's ID as well as s, and it produces a partial private key D_{ID}.
(3) CLC-SVS: It is an algorithm for setting up a secret value that the users are responsible for running. The algorithm accepts an identity ID as its input and produces a secret value x_{ID}.

(4) CLC-PKS: It is an algorithm for setting up a private key that is run by users, and it generates complete private key S_{ID} from D_{ID} and x_{ID} that are supplied by the users.
(5) CLC-PKG: It is an algorithm for the generation of public keys that requires the users to supply a secret value x_{ID} as an input and produces a public key PK_{ID} as its output.
(6) PKI-KG: It is an algorithm for the production of keys that is used by PKI users. The user will select a secret key x and then generate pk that corresponds to it.
(7) SC: A sender's probabilistic signcryption algorithm takes plaintext message m, a set of identities $L = \{ID_1, ID_2, ID_3, \ldots, ID_n\}$ that form the ring, sender's $S_{ID_s}(1 \leq s \leq n)$, and then pk_r and outputs the ciphertext σ.
(8) USC: Receiver runs probabilistic unsigncryption algorithm that accepts σ, $L = \{ID_1, ID_2, \ldots, ID_n\}$, and x_r as input and returns m or $\perp$ if σ is incorrect ciphertext.

These algorithms should fulfill the CP-HRSC stability condition. If $\sigma = SC(m, S_{ID_s}, L, pk_r)$, then $m = USC(\sigma, L, x_r)$.

3.2 Security Notions

CP-HRSC scheme should comply with confidentiality (IND-CCA2) and unforgeability (EUF-CMA). To suit CP-HRSC, this article slightly modifies the [32] concepts.

Definition 2. A CP-HRSC scheme is (ϵ, t, q_u)-IND-CCA2 secure if no probabilistic t-polynomial time adversary $\mathcal{A}$ has advantage at least ϵ after at most q_u in the confidentiality game.

Definition 2 grasps the insider security for confidentiality of signcryption since $\mathcal{A}$ knows all senders' private keys. The insider security ensures the forward security of the signcryption scheme, i.e., confidentiality is kept in case the sender's private key is disclosed.

This article takes into consideration the game for both adversary $\mathcal{A}$ and challenger $\mathcal{C}$ for confidentiality.

Initial: Assuming a secure parameter k, $\mathcal{C}$ executes Setup algorithm and passes *params* along to $\mathcal{A}$.

Phase 1: $\mathcal{A}$ executes a limited amount of queries that are polynomially constrained.

(1) Partial private key extraction queries: $\mathcal{A}$ selects ID and sends it to $\mathcal{C}$. $\mathcal{C}$ executes the CLC-PPKE algorithm and sends D_{ID} to $\mathcal{A}$.
(2) Private key setup queries: $\mathcal{C}$ executes the CLC-PKS algorithm when $\mathcal{A}$ gives it an identity ID and provides $\mathcal{A}$ the full private key. (If necessary, $\mathcal{C}$ may first run the CLC-PPKE and CLC-SVS algorithms).
(3) Public key queries: $\mathcal{A}$ selects an ID and transmits it to $\mathcal{C}$. $\mathcal{C}$ then performs CLC-PKG algorithm and provides resulting public key to $\mathcal{A}$. (If necessary, $\mathcal{C}$ might initiate the CLC-SVS algorithm first).
(4) Public key replacement queries: $\mathcal{A}$ can change pk_{ID} to a value that it chooses.
(5) Key extraction queries: When $\mathcal{C}$ gets an ID from $\mathcal{A}$, it runs the PKI-KE algorithm and sends $\mathcal{A}$ the private key s_{ID} that goes with that identity ID.
(6) Signcryption queries: $\mathcal{A}$ selects the message m, an identity for the sender (ID_j), and an identity for the receiver (ID_j). $\mathcal{C}$ then executes CLC-PKS and CLC-PKG algorithms in order to obtain the sender's s_{ID_i} and pk_{ID_i}. Then $\mathcal{C}$ sends $\mathcal{A}$ outcome from $SC(m, s_{ID_i}, ID_i, pk_{ID_i}, ID_j)$. If the corresponding public key has been changed, $\mathcal{C}$ might not know the sender's secret value. In this instance, $\mathcal{A}$ is needed to give it to us.

(7) Unsigncryption queries: $\mathcal{C}$ executes the PKI-KE and CLC-PKG to obtain private key s_{ID_j} and pk_{ID_i}, after $\mathcal{A}$ selects σ and $L = \{ID_1, ID_2, \ldots, ID_n\}$, sender's ID_i, and receiver's ID_j. $\mathcal{C}$ sends $\mathcal{A}$ the outcome of $USC(\sigma, ID_i, pk_{ID_i}, s_{ID_j}, ID_j)$. The output is either m or $\perp$.

Challenge: The conclusion of phase 1 is determined by $\mathcal{A}.\mathcal{A}$ creates two plaintexts of identical (m_1, m_2) and identities $L^* = \{ID_1^*, ID_2^*, ID_3^*, \ldots, ID_{n-1}^*, ID_n^*\}$, the sender's ID_s^* and the receiver's ID_r^* that it desires to be challenged on. Keep in mind that during phase 1, ID_r^* should never be sent in response to a key extraction query. $\mathcal{C}$ picks an unpredictable bit $\beta \in \{0, 1\}$, then calculates $\sigma^* = SC(m_\beta, L^*, s_{ID_S^*}, ID_s^*, pk_{ID_S^*}, ID_r^*)$, that is then passed to $\mathcal{A}$.

Phase 2: Similar to phase 1, $\mathcal{A}$ can consider an adaptive amount of polynomially bounded enquires. To gain access to the m, it cannot do key extraction query on ID_r or unsigncryption query on $(\sigma^*, L^*, ID_s, ID_r)$ until pk_{ID_s} has been refreshed during the challenge phase.

Guess: $\mathcal{A}$ generates β, if $\beta' = \beta$, then $\mathcal{A}$ wins game.

The benefit for $\mathcal{A}$ is given by $Advantage(\mathcal{A}) = |2(Pr[\beta' = \beta] - 1/2)|$, in which $Pr[\beta' = \beta]$ stands for such possibility which $\beta' = \beta$.

Definition 3. If no probability t-polynomial time adversary can acquire a minimum of ϵ in confidentiality game by performing at more than private key extraction queries q_{ppk}, public key replacement queries q_{pkr}, key extraction queries q_k, SC queries q_{sc}, USC queries q_{usc}, the CP-HRSC technique is considered $(\epsilon, t, q_{ppk}, q_{pkr}, q_k, q_{sc}, q_{usc})$-Type-I-EUF-CMA secure. Since the adversary knows the private keys of all senders, the above definition covers insider security for SC confidentiality. Confidentiality even though the sender's private key has been damaged because of the forward security provided by the SC method, which is guaranteed by insider security.

Since the senders are part of the CLC environment, designers must take into account two categories of adversaries to ensure unforgeability. Type-I adversary represents an opponent who does not have access to s of KGC. It can replace users' pk with other (legal) pk of its choosing. Type-II opponent represents a trusted and inquisitive KGC with knowledge of its master private key. However, it isn't a solution for the user's public key.

Take into consideration how the unforgeability game that $\mathcal{C}$ and $\mathcal{A}_{\mathcal{I}}$ play against one another.

Initial: Using the security parameter k, $\mathcal{C}$ executes Setup procedure and passes results to $\mathcal{A}_{\mathcal{I}}$ in the form of *params*.

Attack: $\mathcal{A}_{\mathcal{I}}$ executes a number of inquiries that have a polynomially constrained execution, similar to the confidentiality game.

Forgery: $\mathcal{A}_{\mathcal{I}}$ exports σ^* and $L^* = \{ID_1^*, ID_2^*, \ldots, ID_n^*\}$, ID_s, ID_r and is effective if such prerequisites are satisfied:

(1) $USC(\sigma^*, ID_s, pk_{ID_s}, s_{ID_r}, ID_r) = m^*$.
(2) $\mathcal{A}_{\mathcal{I}}$ just hasn't submitted a setup request for a private key to be used by any identities in the set L^*.
(3) $\mathcal{A}_{\mathcal{I}}$ can't do each q_{pkr} for any identity in the set L^* prior to the forgery phase and q_{ppk} in a certain phase.
(4) $\mathcal{A}_{\mathcal{I}}$ hasn't requested for q_{sc} on (m^*, L^*).

The possibility that $\mathcal{A}_{\mathcal{I}}$ will emerge victorious can be seen to be its advantage.

Definition 4. If no probability t-polynomial time adversary $\mathcal{A}_{\mathcal{II}}$ can acquire a minimum of ϵ in an unforgeability game by performing at more than q_{pk}, SC queries q_{sc}, then the CP-HRSC technique is considered $(\epsilon, t, q_{pk}, q_{sc})$-Type-II-EUF-CMA secure.

In the end, let's think about a unforgeability game that $\mathcal{C}$ and an adversary of Type-II play against one another.

Initial: $\mathcal{C}$ executes the Setup procedure with k and provides $\mathcal{A}_{\mathcal{II}}$ with *params* and s.

Attack: $\mathcal{A}_{\mathcal{II}}$ executes a polynomially bounded number of inquiries, public key queries and SC queries similar to the confidentiality game. In addition, the q_{ppk}, q_{pkr}, and q_{usc} are unnecessary because $\mathcal{A}_{\mathcal{II}}$ can perform these tasks on their own.

Forgery: $\mathcal{A}_{\mathcal{II}}$ exports σ^* and $L^* = \{ID_1^*, ID_2^*, \ldots, ID_n^*\}$, ID_s, ID_r and is effective if such prerequisites are satisfied:

(1) $USC(\sigma^*, ID_s, pk_{ID_s}, s_{ID_r}, ID_r) = m^*$.
(2) $\mathcal{A}_{\mathcal{II}}$ just hasn't submitted a setup request for a private key to be used by any identities in the set L^*.
(3) $\mathcal{A}_{\mathcal{II}}$ hasn't requested for q_{sc} on (m^*, L^*).

The possibility that $\mathcal{A}_{\mathcal{II}}$ will emerge victorious can be seen to be its advantage.

Definition 5. If an adversary who is not a member of the sender group is unable to identify the real sender with a probability greater than the random chance for any set of n identities, m and σ, then the CP-HRSC scheme is completely anonymous for that set of inputs. In this way, the adversary has a probability of $1/n$ in identifying the original sender.

3.3 The Proposed Scheme

To build a practical CP-HRSC scheme, this article adopts Chow's scheme [29] and employs subsequent eight algorithms.

Setup: Given k, the PKG chooses G_1 and G_2 of prime order p (with G_1 additive and G_2 multiplicative), P, $e : G_1 \times G_1 \to G_2$, and hash functions $H_1 : \{0,1\}^* \to G_1$, $H_2 : \{0,1\}^* \to Z_p^*$ and $H_3 : \{0,1\}^* \to \{0,1\}^{\alpha+\gamma}$. Here, α indicates the amount of bits in the message that must be delivered, and γ indicates the amount of data required to express a feature of G_1. PKG chooses $s \in Z_p^*$ randomly and computes $P_{pub} = sP$. PKG publishes $params = \{G_1, G_2, p, e, \alpha, \gamma, P, P_{pub}, H_i(i = 1, 2, 3)\}$ and guarantees s secrets.

CLC-PPKE: User submits ID to the PKG. The PKG computes $Q_{ID} = H_1(ID)$ and sends $D_{ID} = sQ_{ID}$ to user.

CLC-SVS: The user with ID chooses $x_{ID} \in Z_p^*$ as secret value.

CLC-PKS: The above algorithm provides the user with the whole private key $S_{ID} = (x_{ID}, D_{ID})$ only when given it D_{ID} and x_{ID}.

CLC-PKG: Given x_{ID}, the algorithm computes $PK_{ID} = x_{ID}P$.

PKI-KE: Receiver chooses a random $x_r \in Z_p^*$ as private key sk_r and sets $pk_r = x_rP$.

SC: Consider the sender group $L = \{ID_1, ID_2, \ldots, ID_n\}$ with n identities. To submit m to a receiver with pk_r on behalf of L, the real sender indexed by s (ID_s) performs subsequent operations:

(1) Select $r \in Z_p^*$ at random, calculate $F = rP$.

(2) As to $j \in \{1, 2, 3, \ldots, n-1, n\} \backslash \{s\}$, select $U_j \in G_1$ and query H_2 to obtain $h_j = H_2(m, F, U_j, L)$.

(3) Compute $U_s = rQ_{ID_s} - \sum_{j=1, j \neq s}^{n} \left(U_j + h_j Q_{ID_j}\right)$.

(4) Compute $h_s = H_2(m, F, U_s, L)$.

(5) Compute $V = (h_s + r) D_{ID_s}$.

(6) Compute $w = H_3(F, pk_r, pk_s, x_s pk_r)$, $z = (m \parallel V) \oplus w$.

(7) Output $\sigma = (F, U_1, U_2, \ldots, U_n, z)$.

USC: The receiver with x_r executes subsequent actions upon receiving $\sigma = (F, U_1, U_2, \ldots, U_n, z)$ and $L = \{ID_1, ID_2, \ldots, ID_n\}$:

(1) Compute $w = H_3(F, pk_r, pk_s, x_r pk_s)$.

(2) Compute $(m \parallel V) = z \oplus w$.

(3) As to $j \in \{1, 2, 3, \ldots, n\}$, compute $h_j = H_2(m, F, U_j, L)$.

(4) Check if $e(P, V) = e\left(P_{pub}, \sum_{j=1}^{n} \left(U_j + h_j Q_{ID_j}\right)\right)$ holds. If pass, output m. Or else, reject σ and output $\perp$.

This is where this article demonstrates that the current proposal is correct. As $F = rP$, $rpk_r = rx_r P = x_r F$. Because of $V = (h_s + r) D_{ID_s}$, so

$$e(P, V) = e(P, (h_s + r) D_{ID_s}) = e(P, (h_s + r) s Q_{ID_s}) = e(P_{pub}, rQ_{ID_s} + h_s Q_{ID_s}).$$

Moreover, since $U_s = rQ_{ID_s} - \sum_{j=1, j \neq s}^{n} \left(U_j + h_j Q_{ID_j}\right)$, so

$$\hat{e}(P, V) = \hat{e}(P_{pub}, h_s Q_{ID_s} + U_s + \sum_{j=1, j \neq s}^{n} \left(U_j + h_j Q_{ID_j}\right) = \hat{e}\left(P_{pub}, \sum_{j=1}^{n} \left(U_j + h_j Q_{ID_j}\right)\right).$$

4 Analysis of the Protocol

4.1 Security Analysis

Going to the follow Theorems 1 and 2, this article demonstrates that the suggested CP-HRSC scheme meets the standards for secrecy, anonymity, and unforgeability. This was achieved by adhering to the reasoning process that began with Theorem 1.

Theorem 1. (Confidentiality) In ROM, if $\mathcal{A}$ has a non-negligible benefit ϵ against by IND-CCA2 security of this paper's CP-HRSC scheme when trying to run in a time step t and going to perform q_u and q_{H_j} to hash function $H_j (j = 1, 2, 3)$, then there appears to exist $\mathcal{C}$ that can solve CDH problem with an additional benefit in time $t' < t + O(q_{H_3} + q_u) t_p$, where t_p represents the expense of pairing computation. The above algorithm could solve the CDH problem with a benefit $\epsilon' > \epsilon \left(1 - \frac{q_u}{2^k}\right)$.

Proof. Therefore, in the demonstration, this article would then illustrate what $\mathcal{C}$ are using $\mathcal{A}$ as just a subprogram to overcome random instances (P, aP, bP) from both CDH problems.

Initial: $\mathcal{C}$ provides $\mathcal{A}$ with master secret key η, *params* with $P_{pub} = \eta P$ and pk_r. Here η is selected at random by $\mathcal{C}$, it simulates the private key of recipient.

Phase 1: $\mathcal{C}$ assumes the role of $\mathcal{A}$'s opponent with in secrecy play described in Section 3. $\mathcal{C}$ maintains $L_j (j = 1, 2, 3)$ to emulate, correspondingly, the hash function $H_j (j = 1, 2, 3)$. Remember that $\mathcal{C}$ must keep the same behavior as well as prevent accidents. It is this paper's belief that $\mathcal{A}$ will enquire about $H_1(ID)$ first before using ID for other queries.

$\mathcal{C}$ checks whether the list L_1 appears to include pair (ID_j, e_j) when $\mathcal{A}$ tries to apply an H_1 query on ID_j.

(1) H_1 queries: $\mathcal{C}$ checks whether the list L_1 appears to include pair (ID_j, e_j) when $\mathcal{A}$ tries to apply an H_1 query on ID_j. One if the matching pair has been discovered, $\mathcal{C}$ comes back e_j to $\mathcal{A}$. If not, $\mathcal{C}$ selects $e \in Z_p^*$, adds (ID_j, e) into L_1, and gets back eP to $\mathcal{A}$.

(2) H_2 queries: When $\mathcal{A}$ asks H_2 query on (m, F, L, U_j), $\mathcal{C}$ checks L_2. If there is a matching entry for this query, then $\mathcal{A}$ will receive a comparable response as before. If not, $\mathcal{C}$ gives back t. Both of query and the response are going to be saved in L_2.

(3) H_3 queries: When $\mathcal{A}$ executes H_3 on (F, pk_r, D), $\mathcal{C}$ carries out next operations:

   a. If $e(aP, bP) = e(D, P)$, $\mathcal{C}$ gets back D and stops. $\mathcal{C}$ has worked out CDH problem that was given.

   b. $\mathcal{C}$ yields w and updates $\star$ with D if the list L_2 includes the elements $(F, pk_r, \star, w)$ and as such $e(F, pk_r) = e(D, P)$.

   c. If $\mathcal{C}$ reaches this stage of execution, $\mathcal{C}$ chooses w from $\{0, 1\}^{\alpha} \times G_1$ and gets back it to $\mathcal{A}$. Both query and response are going to be stored in L_3.

(4) USC queries: $\mathcal{A}$ selects $\sigma = (T, U_1, U_2, \ldots, U_n, z)$ and $L = \{ID_1, ID_2, \ldots, ID_n\}$. Then $\mathcal{C}$ does the following:

a. $\mathcal{C}$ checks for different values of D to find one where $e(F, pk_r) = e(D, P)$ by cycling through (F, pk_r, D, w) iterations in L_3. In the event that such a record is located, the correct value for w can be determined. This w is used by $\mathcal{C}$ to decrypt σ, $(m \parallel V) = z \oplus w$. If (F, pk_r, D) is not present in L_3, $\mathcal{C}$ picks a number w at random from the range $\{0, 1\}^{\alpha} \times G_1$, appends $(F, pk_r, \star, w)$ to the end of the list L_3, and uses this new random key to decrypt the provided σ.

b. Obtain $h_j = H_2(m, F, U_j, L)$ for each $j \in \{1, 2, 3, \ldots, n\}$ by querying H_2 and test whether $e(P, V) = e\left(P_{pub}, \sum_{j=1}^{n}\left(U_j + h_j Q_{ID_j}\right)\right)$ holds. If the equation in previous sentence is correct, send the message m back to $\mathcal{A}$. In that case, this ciphertext should be rejected.

Challenge: $\mathcal{A}$ produces (m_0, m_1) as well as identities denoted by L. $\mathcal{C}$ begins by selecting U and z at random from G_1 and G_2, respectively. $\mathcal{C}$ next the transmits $\mathcal{A}$ the challenge ciphertext after establishing $F = aP$.

Phase 2: Similar as phase 1, $\mathcal{A}$ is able to adaptively ask the polynomially bounded amount of q_{usc} to acquire the proper plaintext, but it is unable to ask a query on (σ, L). $\mathcal{C}$ continues to employ identical methods from phase 1 when responding to $\mathcal{A}$'s queries.

Guess: $\mathcal{A}$ generates β', and $\mathcal{C}$ will not pay attention to it.

Unless $\mathcal{A}$ executes H_3 query on (F^*, pk_r, bF^*), the simulation is flawless. If this tuple is absent from the list L_3, $\mathcal{A}$ will gain no advantage. But even so, whether this situation arises, the first phase of simulating H_3 will lead to $\mathcal{C}$ finding a solution to the CDH issue. During entire phase, its likelihood of failure for q_{usc} seems to be no higher than $q_u/2^k$.

Theorem 2. (Unforgeability) This paper's scheme fulfills the EUF-CMA security requirements in ROM while also satisfying CDH assumptions.

Proof. This theorem's proof can be found in Lemmas 1 and 2, which are listed in the previous sentence.

Lemma 1. In the ROM, there exists $\mathcal{C}$ that could resolve CDH problem with an advantage $\epsilon' \geqslant \epsilon \frac{1}{e^n}\left(\frac{n}{q_k+n}\right)^n\left(1-\frac{q_s(q_s+q_{H_2})}{2^k}\right)$ in a time $O(t)$ if $\mathcal{A}_{\mathcal{I}}$ has ϵ against Type-I-EUF-CMA security of this paper's CP-HRSC scheme when running in t and performing q_k, q_s, and q_{H_j}.

Proof. Within that demonstration, this article would then illustrate what $\mathcal{C}$ could use $\mathcal{A}_{\mathcal{I}}$ as its own function call to rectify random instance (P, aP, bP) of CDH problems. This will be done by using the example given below.

Initial: $\mathcal{C}$ provides $\mathcal{A}_{\mathcal{I}}$ with *params* having $P_{pub} = aP$, x_r of the recipient, and the public key $pk_r = x_rP$. Then, x_r is selected at random from Z_p^* by $\mathcal{C}$. It should be noted that $\mathcal{C}$ doesn't have access to the value of one that imitates s used by PKG.

Attack: Inside the unforgeability game described in Section 4, $\mathcal{C}$ acts as an imitation of the challenger $\mathcal{A}_{\mathcal{I}}$ faced. $\mathcal{C}$ retains $L_j (j = 1, 2, 3)$ in order to imitate respective hash functions $H_j (j = 1, 2, 3)$. $\mathcal{C}$ should keep the same pace and stay away from collisions. This paper is working under the assumption that (1) H_1 queries are separate from one another and (2) $\mathcal{A}_{\mathcal{I}}$ will first request $H_1(ID)$ and then use the ID in those other queries.

(1) H_1 queries: $\mathcal{A}_{\mathcal{I}}$ selects an identify *IDj* and provides it to $\mathcal{C}$. Then, $\mathcal{C}$ chooses a bit $\mu \in \{0, 1\}$ with probabilities of 0 (ρ) and 1 ($1 - \rho$). (The value of ρ would be defined at a point later.) When $\mu = 0$, $\mathcal{C}$ selects e_j at random and returns $H_1(ID_j) = e_jP$, $\mathcal{C}$ selects at random $e_j \in Z_p^*$ and returns $H_1(ID_j) = e_jbP$. In both instances, (ID_j, e_j, μ) must be included to L_1.
(2) H_2 queries: $\mathcal{C}$ examines L_2 when $\mathcal{A}_{\mathcal{I}}$ executes an H_2 query on (m, F, U_j, L). If a record for this query is discovered, $\mathcal{C}$ will receive the same response. Or else, $\mathcal{C}$ gets back t generated at random from Z_p^*. The query and associated response are going to be saved in L_2.
(3) H_3 queries: $\mathcal{C}$ examines L_3 when $\mathcal{A}_{\mathcal{I}}$ executes an H_3 query on $(F, pk_r, pk_s, x_r pk_s)$. If a record for this query is discovered, $\mathcal{C}$ will receive the same response. $\mathcal{C}$ gets back k generated at random from $\{0, 1\}^\alpha \times G_1$. Both of query and the response are going to be saved in L_3.
(4) Key extraction queries: $\mathcal{C}$ obtains (ID_j, e_j, μ) from the list L_1 when accepting an identity ID_j from $\mathcal{A}_{\mathcal{I}}$. If $\mu = 0$, $\mathcal{C}$ gives back the private key $S_{ID_j} = e_jaP$. If not, $\mathcal{C}$ can't figure out private key, so it fails and ends.
(5) SC queries: $\mathcal{A}_{\mathcal{I}}$ selects m and $L = \{ID_1, ID_2, \ldots, ID_n\}$. $\mathcal{C}$ performs subsequent operations:
   a. Select $r \in Z_p^*$ at random and calculate $F = rP$.
   b. Select $s \in \{1, 2, \ldots, n\}$ at random.
   c. Each $j \in \{1, 2, \ldots, n\} \backslash \{s\}$, select $U_j \in G_1$ and query H_2 to obtain $h_j = H_2(m, L, F, U_j)$.
   d. Select h_s and z from Z_p^*, calculate $U_s = zP - h_sQ_{ID_s} - \sum_{j=1, j\neq s}^{n}\left(U_j + h_jQ_{ID_j}\right)$ and append (m, F, U_s, L, h_s) to the list L_2. Before that, $h_s = H_2(m, L, F, U_s)$.
   e. Then, compute $V = zaP$.
   f. Through q_{H_3}, $w = H_3(F, pk_r, pk_s, x_s pk_r)$.
   g. Compute $z = (m \parallel V) \oplus w$.
   h. Output $\sigma = (F, U_1, U_2, \ldots, U_n, z)$.

Forgery: $\mathcal{A}_{\mathcal{I}}$ outputs $\sigma = (F^*, U_1^*, U_2^*, \ldots, U_n^*, z^*)$ and $L^* = \{ID_1^*, ID_2^*, ID_3^*, \ldots, ID_{n-1}^*, ID_n^*\}$.

Similar to [33], this proof is completed using forking derivation for ring signature. If $\mathcal{A}_{\mathcal{I}}$ generates valid signature during t with a non-negligible advantage $\epsilon \geq 7C_n^{q_{H_2}}/2^k$, this paper can create $\mathcal{A}_{\mathcal{I}}'$ that generates $(m^*, U_1^*, U_2^*, \ldots, U_n^*, V^*)$ and $\left(m^*, U_1^*, U_2^*, \ldots, U_n^*, \overline{V}^*\right)$ during time *2t* with probability $\epsilon' \geq \epsilon^2/66C_n^{q_{H_2}}$ such that $h_s = \overline{h}_s = H_2\left(m^*, F^*, U_s^*, L^*\right)$ for $s \in \{1, 2, 3, \ldots, n\}$ and $h_j \neq \overline{h}_j = H_2\left(m^*, F^*, U_j^*, L^*\right)$ for each $j \in \{1, 2, 3, \ldots, n\} \backslash \{s\}$. Here $C_n^{q_{H_2}}$ represents the number of n-permutations of q_{H_2} factors, $C_n^{q_{H_2}} = q_{H_2} \times (q_{H_2} - 1) \times \ldots \times (q_{H_2} - n + 1)$.

Using $\mathcal{A}_{\mathcal{I}}'$ generated from $\mathcal{A}_{\mathcal{I}}$, the CDH issue may be resolved through calculating $abP = e_s^{-1}\left(h_s - \overline{h}_s\right)^{-1}\left(V^* - \overline{V}^*\right)$, in which e_s has been obtained from L_1 besides searching for (ID_s, e_s, μ).

This paper will now calculate ρ's value. The possibility that $\mathcal{C}$ will succeed in at least all q_k is no greater than ρ^{q_k}. During the forgery phase, this paper needs to make sure that $\mathcal{A}_{\mathcal{I}}$ hasn't made q_k for any identity in L^*. The probability is equal to $(1 - \rho)^n$. This simulation has a probability of $\rho^{q_k}(1 - \rho)^n$ that $\mathcal{C}$ would then succeed. This value reaches its maximum at $\overline{\rho} = q_k/\,(q_k + n)$. Using this $\overline{\rho}$, $\left(\frac{q_k}{q_k + n}\right)^{q_k}\left(1 - \frac{q_k}{q_k + n}\right)^n = \frac{1}{\left(1 + \frac{n}{q_k}\right)^{\frac{q_k}{n}n}}\left(\frac{n}{q_k + n}\right)^n$.

Moreover, using $lim_{\lambda \to 0}(1 + \lambda)^{1/\lambda} = e$, this paper finds that $\frac{1}{\left(1 + \frac{n}{q_k}\right)^{\frac{q_k}{n}}} \geq \frac{1}{e}$ for extremely large q_k. Therefore, the possibility that $\mathcal{C}$ wins in virtual competition is at least $\frac{1}{e^n}\left(\frac{n}{q_k + n}\right)^n$.

And if $\mathcal{C}$ has a collision on H_2, then all q_{sc} could fail for $\mathcal{C}$, making that possibility H_2 is $q_s(q_s + q_{H_2})/2^k$.

Therefore, $\epsilon' \geqslant \epsilon\frac{1}{e^n}\left(\frac{n}{q_k + n}\right)^n\left(1 - \frac{q_s(q_s + q_{H_2})}{2^k}\right)$.

Lemma 2. In the ROM, there exists $\mathcal{C}$ that could resolve the CDH problem with an advantage $\epsilon' \geqslant \epsilon\frac{1}{e^n}\left(\frac{n}{q_k + n}\right)^n\left(1 - \frac{q_s q_{H_2}}{2^k}\right)$ in a time $O(t)$, if $\mathcal{A}_{\mathcal{II}}$ has ϵ against Type-II-EUF-CMA security of this paper's CP-HRSC scheme when running in t and performing q_k, q_s, and q_{H_j}.

Proof. Within that demonstration, this paper would then illustrate what $\mathcal{C}$ could use $\mathcal{A}_{\mathcal{II}}$ as its own function call to rectify random instance (P, aP, bP) of CDH problem. This will be done by using the example given below.

Initial: $\mathcal{C}$ provides $\mathcal{A}_{\mathcal{II}}$ with *params* by setting $P_{pub} = sP$ and $pk_r = bP$. $\mathcal{C}$ chooses s at random. Furthermore, $\mathcal{C}$ obtains public/private key pair (pk_r^*, sk_r^*) of recipient by executing the PKI-KG algorithm and sending them to $\mathcal{A}_{\mathcal{II}}$. $\mathcal{C}$ then selects challenge identity $ID^* \in \{0, 1\}^*$ at random and provides it to $\mathcal{A}_{\mathcal{II}}$.

Attack: $\mathcal{C}$ simulates the opponent of $\mathcal{A}_{\mathcal{II}}$ in Type-II-EUF-CMA game. $\mathcal{C}$ maintains $L_j (j = 1, 2, 3)$ to imitate relevant hash functions $H_j (j = 1, 2, 3)$. $\mathcal{C}$ also keeps an initially empty list L_k to store public key information. And this paper presumes H_1 queries are distinct and $\mathcal{A}_{\mathcal{II}}$ would then request H_1 prior to using *ID* in subsequent queries.

(1) H_1 queries: When $\mathcal{A}_{\mathcal{II}}$ submits an H_1 query on ID_j, $\mathcal{C}$ verifies if L_1 contains a pair (ID_j, e_j). When matching pair is discovered, $\mathcal{C}$ gets back e_j to $\mathcal{A}_{\mathcal{II}}$. If not, $\mathcal{C}$ selects $e \in Z_p^*$, adds (ID_j, e) into L_1, and gets back eP to $\mathcal{A}_{\mathcal{II}}$.

(2) H_2 queries: When $\mathcal{A}_{\mathcal{II}}$ asks H_2 query on (m, F, U_j, L), $\mathcal{C}$ checks L_2. If such an entrance matching this query is found, $\mathcal{A}_{\mathcal{II}}$ will receive same response. If not, $\mathcal{C}$ gives back t from Z_p^*. The query and associated response are going to be saved in L_2.

(3) H_3 queries: $\mathcal{C}$ examines L_3 when $\mathcal{A}_{\mathcal{II}}$ executes an H_3 query on $(F, pk_r, pk_s, x_r pk_s)$. If a record for this query is discovered, $\mathcal{C}$ will receive the same response. $\mathcal{C}$ gets back k generated at random from $\{0,1\}^{\alpha} \times G_1$. Both of query and the response are going to be saved in L_3.

(4) Public key queries: $\mathcal{A}_{\mathcal{II}}$ selects ID_i as well as transmits it all to $\mathcal{C}$. $\mathcal{C}$ comes back pk_{ID_i} to $\mathcal{A}_{\mathcal{II}}$ if L_k includes (ID_i, pk_{ID_i}, xID_i). If not, $\mathcal{C}$ selects $r_i \in Z_p^*$. At η-th q_k, $\mathcal{C}$ answers by $pk_\eta = r_i aP$. For queries pk_i with $i \neq \eta$, $\mathcal{C}$ answers by $pk_i = r_i P$ where $x_i = r_i$, puts (ID_i, pk_i, x_i) into L_k.

(5) SC queries: $\mathcal{A}_{\mathcal{II}}$ selects m and $L = \{ID_1, ID_2, \ldots, ID_n\}$. $\mathcal{C}$ performs subsequent operations:
   a. Select $r \in Z_p^*$ at random and calculate $F = rP$.
   b. Select $s \in \{1, 2, 3, \ldots, n-1, n\}$ at random.
   c. For each $j \in \{1, 2, \ldots, n\} \backslash \{s\}$, select $U_j \in G_1$ and query H_2 to obtain $h_j = H_2(m, L, F, U_j)$.
   d. Select h_s and z from Z_p^*, calculate $U_s = zP - h_s Q_{ID_s} - \sum_{j=1, j\neq s}^{n} \left(U_j + h_j Q_{ID_j}\right)$ and append (m, F, U_s, L, h_s) to the list L_2. Before that, $h_s = H_2(m, F, U_s, L)$.
   e. Then, compute $V = zsP$.
   f. Through q_{H_3}, $w = H_3(F, pk_r, pk_s, x_s pk_r)$.
   g. Compute $z = (m \parallel V) \oplus w$.
   h. Output $\sigma = (F, U_1, U_2, U_3, \ldots, U_n, z)$.

Forgery: $\mathcal{A}_{\mathcal{II}}$ outputs $\sigma^* = (F^*, U_1^*, U_2^*, U_3^*, \ldots, U_{n-1}^*, U_n^*, z^*)$ and $L^* = \{ID_1^*, ID_2^*, \ldots, ID_n^*\}$. It's indeed simple to demonstrate that $\mathcal{A}_{\mathcal{II}}$ will be unaware that σ^* isn't valid deniable authenticator for sk_i and receiver unless it asks for $H_3(F, r_i aP, bP, r_i abP)$. The solution to the CDH problem could be added to L_3. Then $\mathcal{C}$ looks up L_3 for tuples of $(F, r_i aP, bP, K)$. $\mathcal{C}$ examines both of them to evaluate whether or not $e(r_i P, K) = e(r_i aP, bP)$. If the condition is satisfied, $\mathcal{C}$ will come to a halt and will output the solution $K = abP$ to the CDH problem. $\mathcal{C}$ will fail and come to a stop if there is no such tuple that satisfies equality.

During the forgery phase, this paper needs to make sure that $\mathcal{A}_{\mathcal{II}}$ hasn't made q_k for any identity in L^*. The probability is equal to $(1-\rho)^n$. This simulation has a probability of $\rho^{q_k}(1-\rho)^n$ that $\mathcal{C}$ would then succeed. This value reaches its maximum at $\overline{\rho} = q_k / (q_k + n)$. Using this $\overline{\rho}$, $\left(\frac{q_k}{q_k+n}\right)^{q_k}\left(1-\frac{q_k}{q_k+n}\right)^n = \frac{1}{\left(1+\frac{n}{q_k}\right)^{\frac{q_k}{n}n}}\left(\frac{n}{q_k+n}\right)^n$.

Moreover, using $lim_{\lambda\to 0}(1+\lambda)^{1/\lambda} = e$, this paper finds that $\frac{1}{\left(1+\frac{n}{q_k}\right)^{\frac{q_k}{n}}} \geq \frac{1}{e}$ for extremely large q_k. Therefore, the possibility that $\mathcal{C}$ wins in virtual competition is at least $\frac{1}{e^n}\left(\frac{n}{q_k+n}\right)^n$.

And if $\mathcal{C}$ has a collision on H_2, then all q_{sc} could fail for $\mathcal{C}$, making that possibility H_2 is $q_s q_{H_2}/2^k$.

Therefore, $\epsilon' \geqslant \epsilon \frac{1}{e^n}\left(\frac{n}{q_k+n}\right)^n\left(1-\frac{q_s q_{H_2}}{2^k}\right)$.

4.2 Performance Analysis

This article analyzes the performance and security of this paper's system in this section. In Table 2, this article tries to compare this paper's computation and communication costs to that of RG [27], YC [28], and CZ [29].

Table 2: Performance comparison

Schemes	SC			USC			Communication overhead	Environment
	PM	E	P	PM	E	P		
RG [27]	$2n+2$	0	0	$3n+5$	0	0	$\|m\| + (2n+1)\|G_1\| + Z_p^*$	CLC-CLC
YC [28]	$n+4$	0	1	n	0	2	$\|m\| + n\|G_1\| + 2Z_p^*$	IBC-IBC
CZ [29]	$n+1$	3	3	$2n$	0	2	$\|m\| + (2n+1)\|G_1\|$	CLC-CLC
CP-HRSC	$n+2$	0	0	n	0	2	$\|m\| + (n+2)\|G_1\|$	CLC-PKI

This article indicates E exponentiation in G_2, PM point multiplication in G_1, and P pairing computation. In addition, other operations are neglected, because of these operations consume most process time. In which, G_1 is the additive group on the elliptic curve, and the multiplication group is denoted by G_2. $|m|$ indicates the number of bits of messages. This article provides a quantitative assessment of RG [27], YC [28], CZ [29], and this paper's scheme. This paper just considers the sensor component because its resources are restricted. This article uses MICA2 as the test platform for communication between sensors and servers in WBANs and refers to the experimental results in [34]. The MICA2 node includes an 8-bit AVR processor and a 128KB programmable flash. It has a 2.4 GHz transmission channel frequency.

According to [34], P requires 1.9 s and an E requires 0.9 s when applying a curve $b^2 + b = a^3 + a$ with an embed degree of 4 and using η_T pairing: $E(\mathbb{F}_{2^{271}}) \times E(\mathbb{F}_{2^{271}}) \rightarrow \mathbb{F}_{2^{4 \cdot 271}}$, which is the same as a security level of 80 bits. Moreover, according to [34,35], PM requires 0.81 s. So, the calculation time on the sensor of RG [27], YC [28], and CZ [29] and this paper's scheme are $(2n+2)*0.81 = 1.62n+1.62\,s$, $(n+4)*0.81+1.9 = 0.81n+5.14$, $(n+1)*0.81+3*1.9+3*0.9 = 0.81n+9.21\,s$, and $(n+2)*0.81 = 0.81n+1.62$ s. When $n = 100$, the calculation time of RG [27], YC [28], CZ [29] and this paper's scheme are 163.62, 86.14, 90.21, and 82.62 s, respectively. In terms of calculation time, this paper's scheme has reduced by 49.5%, 4.1%, and 8.4% respectively.

Throughout [34], this article assumes that the power rating of MICA2 is 3.0 V, sending mode current consumption is 8.0 mA. In terms of energy consumption, pairing uses $3.0 * 8.0 * 1.9 = 45.6\,mJ$, exponentiation needs $24.0 * 0.9 = 21.6$ and PM uses $24.0 * 0.81 = 19.44$ mJ. Therefore, the computational energy cost on the sensor of RG [27], YC [28], CZ [29], and this paper's scheme are $(2n + 2) * 19.44 = 38.88n + 38.88$ mj, $(n + 4) * 19.44 + 45.6 = 19.44n + 123.36$ mj, $(n + 1) * 19.44 + 3 * 21.6 + 3 * 45.6 = 19.44n + 221.04$ mj, and $(n + 2) * 19.44 = 19.44n + 38.88$ mJ.

For the expense of communication, this article uses a curve on binary field $\mathbb{F}_{2^{271}}$, G_1 is a prime order of 252 bits. The size of an element in group G_1 is 542 bits, which can be reduced to 34 bytes. G_2 is now 136 bytes long. So in RG [27], YC [28], CZ [29], and this paper's scheme, the sensor will have to submit out $|m| + (2n + 1)|G_1| + Z_p^*$ bits $= 20 + (2n + 1) * 34 + 32$ bytes $= 68n + 86$ bytes, $|m| + n|G_1| + 2Z_p^*$ bits $= 20 + n * 34 + 2 * 32$ bytes $= 34n + 84$ bytes, $|m| + (2n + 2)|G_1| = 20 + (2n + 2) * 34 = 68n + 88$ bytes, $|m| + (n + 2)|G_1| = 20 + (n + 2) * 34 = 34n + 88$ bytes. According to [34], the sensor requires $3*27*8/12400 = 0.052$ mJ to send a one-byte message. For communication energy consumption, RG [27] is $(68n+86) * 0.052 = 3.536n+4.472$ mJ, YC [28] is $(34n+84) * 0.052 = 1.768n+4.368$ mJ, CZ [29] is $(68n+88)*0.052 = 3.536n+4.576$ mJ, this paper's scheme is $(34n+88)*0.052 = 1.768n+4.576$ mJ. The entire energy use of RG [27], YC [28], CZ [29] and this paper's scheme are $38.88n + 38.88 +$

$3.536n + 4.472 = 42.416n + 43.352$ mJ, $19.44n + 123.36 + 1.768n + 4.368 = 21.208n + 127.728$ mJ, $19.44n + 221.04 + 3.536n + 4.576 = 22.976n + 225.616$ mJ,$21.208n + 19.44n + 38.88 + 1.768n + 4.576 = 43.456$ mJ. When $n = 100$, the communication energy consumption of RG [27], YC [28], CZ [29] and this paper's scheme are 4284.952, 2248.528, 2523.216, and 2164.256 mJ, respectively. In terms of communication energy consumption, this paper's scheme has reduced by 49.4%, 3.7%, and 14.2% respectively.

According to the computation time and energy consumption from senor to server, this article makes two graphs to visually represent the data. Figs. 2 and 3 compare the computational times and energy consumption of RG [27], YC [28], and CZ [29] and this paper's scheme (this article assumes $|m| = 160$ bits). It is obvious that this paper's scheme requires the fewest computations. Based on Figs. 2 and 3, this paper's scheme requires just 82.62 s to signcrypt a message with 100 identities. The entire amount of energy consumed is 2164.256 mJ. Both consumptions of energy and time are tolerable for practical uses. As the number of identities increases, the efficiency of the proposed scheme in this article decreases. In subsequent research, the steps of the algorithm can be further optimized through aggregation or attribute-based methods to further improve its efficiency.

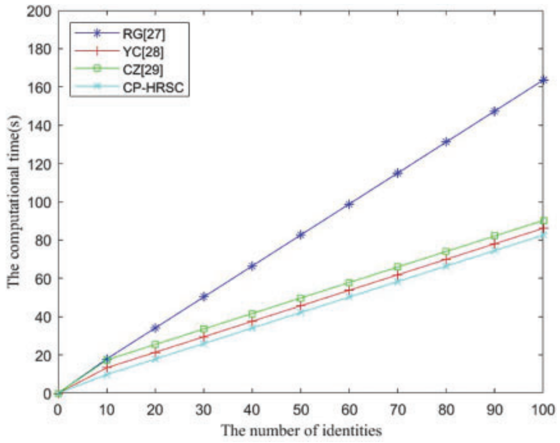

Figure 2: The computational time *vs.* number of identities

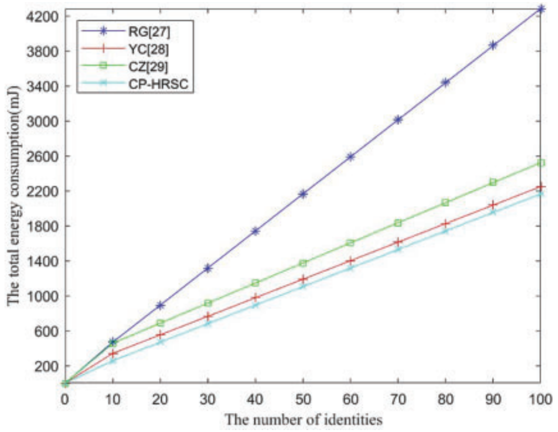

Figure 3: The total energy consumption *vs.* number of identities

5 Application

The application scenario of this paper's scheme consists of three parts, including the controller of WBANs, server, and SP. WBANs consist of numerous sensor nodes and at least one controller. The controller transmits data collected by sensor nodes to the server. The server stores the received data and uses it for medical institutions. SP provides identity registration, key distribution, and storage for controllers and the server.

(1) Initialization Phase

SP needs to provide private keys for the controller and server. Before that, SP executes the Setup algorithm to generate s and $params$.

(2) Registration Phase

After the controller registers the identity ID, SP checks its ID and executes the CLC-PPKE algorithm to generate $D_{ID} = sQ_{ID}$. Then, the controller executes CLC-PKS algorithm to generate $S_{ID} = (x_{ID}, D_{ID})$, including D_{ID} and its secret value x_{ID}. After the server registers ID_r, SP executes the PKI-KG algorithm to generate sk_r and $pk_r = x_rP$ for the server.

(3) Transmission Phase

The controller uses its own private key to run the SC algorithm to generate $\sigma = (F, U_1, U_2, \ldots, U_n, z)$ and transmit σ to the server. After the server receives data and executes the USC algorithm to recover to m and verify whether $e(P, V) = e\left(P_{pub}, \sum_{i=1}^{n}\left(U_i + h_iQ_{ID_i}\right)\right)$ holds. If pass, accept σ and output m. Otherwise, reject σ.

(4) Revocation Phase

The registered identity has timeliness. If the time expires, the registration information will be automatically revoked and the private key of the controller will not be available. Therefore, access to the WBAN must be revoked before its expiration.

6 Conclusion

In this paper, this paper provides a new scheme to secure communication from sensors to servers using the proposed HRSC scheme. HRSC system permits the sender in the CLC environment to communicate with recipient in the PKI environment, and greatly improves the anonymity of WBANs since a sensor can anonymously signcrypt a message on behalf of a set of sensors including itself, but the server doesn't know exactly who the sensor is. This paper's construction can achieve anonymity, confidentiality, authentication, non-repudiation, and integrity in a logical single step. This article demonstrates the scheme is IND-CCA2 and EUF-CMA secure in ROM under the CDH problem. As compared with the existing three schemes RG, YC and CZ, the computational cost of the sensor node in this paper's scheme is reduced by about 49.5%, 4.1%, and 8.4%, respectively and the energy consumption of the sensor node in this paper's scheme is reduced by about 49.4%, 3.7%, and 14.2%, respectively. Therefore, this paper's scheme is the most efficient and it can be well applied in WBANs. Furthermore, there are plans to study blockchain technology and combine it with current solutions.

Funding Statement: This work is supported by the Postgraduate Research & Practice Innovation Program of Jiangsu Province (Grant No. SJCX22_1677).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] I. Ullah, M. A. Khan, A. M. Abdullah, F. Noor, N. Innab *et al.,* "Enabling secure communication in wireless body area networks with heterogeneous authentication scheme," *Sensors*, vol. 23, no. 3, pp. 1121, 2023.

[2] K. Hasan, M. J. M. Chowdhury, K. Biswas, K. Ahmed, M. Saiful Islam *et al.,* "A blockchain-based secure data-sharing framework for software defined wireless body area networks," *Computer Networks*, vol. 211, pp. 109004, 2022.

[3] W. Wang, Y. Yang, Z. Yin, K. Dev, X. Zhou *et al.,* "BSIF: Blockchain-based secure, interactive, and fair mobile crowdsensing," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 12, pp. 3452–3469, 2022.

[4] W. Wang, Q. Chen, Z. Yin, G. Srivastava, T. R. Gadekallu *et al.,* "Blockchain and PUF-based lightweight authentication protocol for wireless medical sensor networks," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8883–8891, 2021.

[5] H. Xu, Q. He, X. Li, B. Jiang and K. Qin, "BDSS-FA: A blockchain-based data security sharing platform with fine-grained access control," *IEEE Access*, vol. 8, pp. 87552–87561, 2020.

[6] C. M. Chen, S. Liu, X. Li, S. H. Islam and A. K. Das, "A Provably-secure authenticated key agreement protocol for remote patient monitoring IoMT," *Journal of Systems Architecture*, vol. 136, pp. 102831, 2023.

[7] H. Xiong, C. Jin, M. Alazab, K. Yeh, H. Wang *et al.,* "On the design of blockchain-based ECDSA with fault-tolerant batch verification protocol for blockchain-enabled IoMT," *IEEE Journal of Biomedical and Health Informatics*, vol. 26, no. 5, pp. 1977–1986, 2021.

[8] K. Das, R. Ray and S. Moulik, "Optimal relaying nodes selection for IEEE 802.15.6-based two-hop star topology WBAN," *Internet of Things*, vol. 22, pp. 100740, 2023.

[9] F. Cherifi, M. Omar, T. Chenache and S. Radji, "Efficient and lightweight protocol for anti-jamming communications in wireless body area networks," *Computers & Electrical Engineering*, vol. 98, pp. 107698, 2022.

[10] W. Han, J. Wang, S. Hou, T. Bai, G. Jeon *et al.,* "An PPG signal and body channel based encryption method for WBANs," *Future Generation Computer Systems*, vol. 141, pp. 704–712, 2023.

[11] D. Javaheri, P. Lalbakhsh, S. Gorgin, J. Lee and M. Masdari, "A new energy-efficient and temperature-aware routing protocol based on fuzzy logic for multi-WBANs," *Ad Hoc Networks*, vol. 139, pp. 103042, 2023.

[12] E. M. George and L. Jacob, "Interference and priority aware resource allocation in coexisting WBANs using game models," *Physical Communication*, vol. 53, pp. 101750, 2023.

[13] C. Hu, F. Zhang, X. Cheng, X. Liao and D. Chen, "Securing communications between external users and wireless body area networks," in *HotWiSec '13*, pp. 31–36, New York, NY, USA: Association for Computing Machinery, 2013.

[14] B. Qin, R. H. Deng, S. Liu and S. Ma, "Attribute-based encryption with efficient verifiable outsourced decryption," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 7, pp. 1384–1393, 2015.

[15] M. Li, W. Lou and K. Ren, "Data security and privacy in wireless body area networks," *IEEE Wireless Communications*, vol. 17, no. 1, pp. 51–58, 2010.

[16] X. Fu, Y. Wang, L. You, J. Ning, Z. Hu *et al.,* "Offline/online lattice-based ciphertext policy attribute-based encryption," *Journal of Systems Architecture*, vol. 130, pp. 102684, 2022.

[17] Z. U. Rehman, S. Altaf and S. Iqbal, "An efficient lightweight key agreement and authentication scheme for WBAN," *IEEE Access*, vol. 8, pp. 175385–175397, 2020.

[18] F. Wu, X. Li, A. K. Sangaiah, L. Xu, S. Kumari *et al.,* “A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks,” *Future Generation Computer Systems*, vol. 82, pp. 727–737, 2017.

[19] Y. Zheng, “Digital signcryption or how to achieve cost (signature & encryption) << cost(signature) + cost (encryption),” In: B. S. Kaliski (Ed.), in *Advances in Cryptology—CRYPTO ’97*, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 165–179, 1997.

[20] C. C. Tan, H. Wang, S. Zhong and Q. Li, “Ibe-lite: A lightweight identity-based cryptography for body sensor networks,” *IEEE Transactions on Information Technology in Biomedicine*, vol. 13, no. 6, pp. 926–932, 2009.

[21] X. Yang, X. Chen, J. Huang, H. Li and Q. Huang, “Fs-ibeks: Forward secure identity based encryption with keyword search from lattice,” *Computer Standards & Interfaces*, vol. 86, pp. 103732, 2023.

[22] D. Pavithran, J. N. Al-Karaki and K. Shaalan, “Edge-based blockchain architecture for event-driven IoT using hierarchical identity based encryption,” *Information Processing & Management*, vol. 58, no. 3, pp. 102528, 2021.

[23] J. Liu, Z. Zhang, X. Chen and K. S. Kwak, “Certificateless remote anonymous authentication schemes for wireless body area networks,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 332–342, 2014.

[24] S. S. Al-Riyami and K. G. Paterson, “Certificateless public key cryptography,” In: C. S. Laih (Ed.), in *Advances in Cryptology—ASIACRYPT 2003*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 452–473, 2003.

[25] H. Yu and W. Li, “A certificateless signature for multi-source network coding,” *Journal of Information Security and Applications*, vol. 55, pp. 102655, 2020.

[26] L. Deng, S. Feng and Z. Chen, “Certificateless encryption scheme with provable security in the standard model suitable for mobile devices,” *Information Sciences*, vol. 613, pp. 228–238, 2022.

[27] R. Guo, L. Xu, X. Li, Y. Zhang and X. Li, “An efficient certificateless ring signcryption scheme with conditional privacy-preserving in vanets,” *Journal of Systems Architecture*, vol. 129, pp. 102633, 2022.

[28] Y. Cai, H. Zhang and Y. Fang, “A conditional privacy protection scheme based on ring signcryption for vehicular ad hoc networks,” *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 647–656, 2021.

[29] C. Zhou, G. Gao, Z. Cui and Z. Zhao, “Certificate-based generalized ring signcryption scheme,” *International Journal of Foundations of Computer Science*, vol. 29, no. 6, pp. 1063–1088, 2018.

[30] J. S. Sun, T. Zhu and M. Wozniak, “Intelligent spacing selection model under energy saving constraints for the selection of communication nodes in the internet of things,” *Mobile Networks and Applications*, vol. 27, no. 2, pp. 628–636, 2022.

[31] A. Dhandapani, P. Venkateswari, T. Sivakumar, C. Ramesh and P. Vanitha, “Cooperative self-scheduling routing protocol based IoT communication for improving life time duty cycled energy efficient protocol in sdn controlled embedded network,” *Measurement: Sensors*, vol. 24, pp. 100475, 2022.

[32] C. K. Li, G. Yang, D. S. Wong, X. Deng and S. S. M. Chow, “An efficient signcryption scheme with key privacy and its extension to ring signcryption,” *Journal of Computer Security*, vol. 18, no. 3, pp. 451–473, 2010.

[33] S. S. M. Chow, S. M. Yiu and L. C. K. Hui, “Efficient identity based ring signature,” in *Applied Cryptography and Network Security*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 499–512, 2005.

[34] K. A. Shim, Y. R. Lee and C. M. Park, “Eibas: An efficient identity-based broadcast authentication scheme in wireless sensor networks,” *Ad Hoc Networks*, vol. 11, no. 1, pp. 182–189, 2013.

[35] N. Gura, A. Patel, A. Wander, H. Eberle and S. C. Shantz, “Comparing elliptic curve cryptography and RSA on 8-bit CPUS,” in *Cryptographic Hardware and Embedded Systems—CHES 2004*, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 119–132, 2004.