Hindawi
Security and Communication Networks
Volume 2019, Article ID 5860286, 13 pages
https://doi.org/10.1155/2019/5860286

Research Article

CasCP: Efficient and Secure Certificateless Authentication Scheme for Wireless Body Area Networks with Conditional Privacy-Preserving

Yong Xie, Songsong Zhang, Xiang Li, Yanggui Li, and Yuan Chai

Department of Computer Technology and Application, Qinghai University, China

Correspondence should be addressed to Yanggui Li; liyanggui@126.com

Received 6 March 2019; Accepted 24 April 2019; Published 4 June 2019

Guest Editor: Mingwu Zhang

As the aging population of society continues to intensify, the series of problems brought about by aging is becoming more and more serious. Because the health problem of the elderly brings many social problems, people have paid close attention to it. Fortunately, as a typical smart healthcare system, wireless body area networks (WBANs) present quit nice medical care for people, especially the aged. However, personal health information is very sensitive. But, the common communication channel is used in WBANs and any malicious entity can initiate a security attack on WBANs. To ensure secure communication and privacy-preserving which are the premise of the sound development of WBANs, an improved and efficient certificateless authentication scheme with conditional privacy-preserving is proposed in this paper on the basis of analyzing the most recent presented certificateless authentication scheme for WBANs. The proposed scheme also provides batch authentication to decrease authentication and communication cost. A rigid security proof demonstrates that our proposed scheme resists every type of security attack and can provide condition privacy-preserving. The performance analysis shows that our proposed scheme has some advantages in computation and communication cost.

1. Introduction

Nowadays, the population growth rate in many countries around the world is decreasing. Most of these counties have gradually entered an aged society. World Health Organization (WHO) has predicted that human life expectancy will reach 75 year old in 2030, and about 80 million people will be 60 year old in America and 430 million in China by 2050 [1]. Sociologists have pointed out that the aging population structure will put tremendous pressure on all aspects in society, especially healthcare.

In order to provide comprehensive and accurate care for the elderly, researchers have launched various research on smart healthcare. With the rapid development of wearable sensors, especially health sensors, wireless body area networks (WBANs) have a profound significance for improving the health monitoring of the elderly [2]. Information technologies are used in WBANs and can be well applied to medical related services [3]. In WBAN, client's information, such as weight trend, diet attempt, food-intake, hematologic biochemical parameters, respiratory rate, cardiac status, blood data, etc., is transmitted to the corresponding medical service application providers (AP) by wireless communication from body sensors. The client's doctor will receive this information soon and provide timely treatment based on this information [4, 5]. The scenes of sensor nodes collect and send the client real-time physiological data to AP and the typical smart medical service based WBANs can be depicted as in Figure 1.

However, the security and privacy issues in WBANs are very serious and worthy of paid close attention. It is well known that private personal health information is very sensitive, which may cause serious problems such as family conflicts, corporate crisis, and even state instability [6]. The health data are sent to AP through insecure communication channel and suffered from intercepting, eavesdropping, modification, and other attacks with little problem. The security of health data is critical to the patient as a forged health data results in doctor's misdiagnosis and extremely may endanger

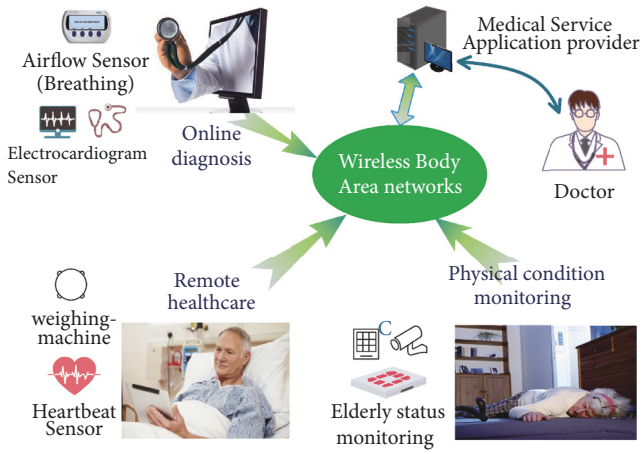

FIGURE 1: The typical smart medical services based WBANs.

the life of a patient. If WBANs cannot provide strong security protection measures, client's personal health information cannot be effectively protected, client will no longer trust WBANs, and people will no longer accept WBANs. Then, WBANs cannot get further development and cannot achieve the goal of smart medical care [7].

In order to meet the challenges of security and privacy protection in WBANs, many researchers have made continuous efforts and obtained some research results on WBANs authentication scheme. One important way is digit signature and data encryption. PKI-based authentication scheme and identity-based authentication scheme have been adopted to WBANs for a long time. But the PKI-based authentication scheme causes heavy certificate management and identity-based authentication scheme has an inevitable problem of key escrow. To solve this issue, certificateless authentication technology is introduced to WBANs and presents good application prospects. Recently, Ji *et al.* [8] proposed an efficient certificateless authentication scheme for WBANs. Ji *et al.* presented security analysis to show that their scheme can secure against all kinds of security attacks. However, their scheme cannot resist forgery attack and bath authentication attack, which is demonstrated in Section 5 in this paper. To the best of our knowledge, no universally accepted effective and secure authentication scheme for WBAN has been proposed, especially constructed by using certificateless public key cryptography [9]. Because of the strong privacy protection requirements of health data, limited communication channel, limited computing power, and fully open wireless communication environment, it is a huge challenge to build an efficient and secure certificateless authentication scheme for WBANs.

1.1. Motivations and Contributions. On reviewing Ji *et al.*'s certificateless authentication scheme [8], we decided to solve their security deficiencies while appreciating their high efficiency in message signing phase and authentication phase. In this paper, we present an improved and secure certificateless authentication scheme with conditional privacy-preserving (called CasCP). CasCP constructs signature and authentication algorithm by using elliptic curve cryptography (EEC) and no longer needs complex bilinear pairing operation. To sum up, there are three major contributions in our proposed scheme.

First, we present an improved and secure certificateless authentication scheme with conditional privacy-preserving. The proposed scheme includes five key phases for WBANs.

Second, we present a rigid security proof and detailed security analysis. It shows that CasCP can be secure against all known security attacks and providing privacy-preserving.

Third, the performance analysis shows that CasCP requires less computational and communication costs than recent similar schemes.

1.2. Organization of the Paper. The rest of the paper is arranged as follows. Related works and preliminaries are presented in Sections 2 and 3. Section 4 shows the system model and security requirements. Ji *et al.*'s certificateless authentication scheme is reviewed and analyzed in Section 5. Next, the CasCP is proposed in Section 6. Security proof and performance analysis are presented in Sections 7 and 8. At last, it draws a conclusion.

2. Related Works

In order to present a secure communication in WBANs, there are many security requirements. Among all of the security requirements, the remote authentication is the most basic and important requirement. In 1981, Lamport proposed the first remote authentication scheme [10] that allows the mobile user to authenticate with a server through a public channel and generate the session key to encrypt the later session. From then on, more and more remote authentication schemes have been proposed to apply to different environments.

Some works in [11–15] are constructed based on traditional public key cryptosystem (PKC). But there are many difficulties in the establishment, implementation, and management of traditional PKC system. In order to solve the problems in traditional PKC system for WBANs, some researchers have proposed mutual authentication scheme using identity-based public key cryptography [16, 17]. In this way, these authentication schemes solve the difficulties in traditional PKC system. However, there is another thorny problem, key escrow problem; that is, if the key generation center has been compromised, the system goes into a state of being out of control.

In 2003, Al Riyami *et al.* [18] proposed certificateless cryptography, which can erase key escrow problem in identity-based PKC. Based on the previous work [18], scholars have proposed a lot of secure authentication schemes [19, 20] by using certificateless cryptography. In 2005, Huang *et al.* [21] proposed an improved scheme over Al Riyami *et al.*'s [18] that can avoid security leaks. Huang *et al.* [20] proposed two certificateless signature schemes on assuming three-kind-adversary security model. However, it has been pointed out their scheme cannot resist key replacement attacks [22].

To decrease authentication and communication cost, Boneh *et al.* [23] presented a certificateless authentication

scheme with batch authentication in 2003. Batch authentication has been widely used for Internet of thing and other wireless networks, including WBANs. Without doubt, new security issues of batch authentication technology are unavoidable. Until now, researchers have proposed a lot of batch authentication schemes for WBANs and other wireless networks [24–26]. Based on the computational complexity of pairing, batch authentication and aggregate signature schemes [27–29] have been presented by using bilinear pairing. Xiong *et al.* [30] proposed an aggregate signature and batch authentication scheme that do not use clock synchronization and needs less computation cost than Zhang *et al.*'s [27] scheme. But, an adversary can successfully launch a forgery attack on Xiong et al.'s scheme [31, 32]. Wen *et al.* [33] constructed an aggregate signature scheme using bilinear pairing with designed verifier. Hartung *et al.* [34] presented another fault-tolerant batch authentication scheme. Tu *et al.* [29] proposed a revised authentication scheme to solve the security deficiencies of Xiong's scheme [30]. He *et al.* [35] presented a new certificateless authentication scheme for WBANs. Unfortunately, the foregoing schemes have more or less security deficiencies; some schemes cannot resist security attacks in batch authentication [36–38].

Most recently, Ji *et al.* [8] proposed a certificateless conditional privacy-preserving authentication scheme by using elliptic curve cryptography (ECC) for WBANs. Their proposed scheme has a clear advantage in computation performance when compared with the former certificateless scheme using bilinear pairing. They claimed that their proposed scheme provides conditional privacy-preserving and can resist all kinds of security attacks. However, we demonstrate that a common adversary can successfully launch a forgery attack in individual authentication and batch authentication. To solve the deficiencies of Ji *et al.*'s authentication scheme, we propose an improved certificateless authentication scheme with conditional privacy-preserving.

3. Preliminaries

3.1. Elliptic Curve Cryptosystem (ECC). In 1984, Miller proposed elliptic curve cryptography (ECC) for the first time [39]. Koblitz [40] proposed an ECC instance based on the difficulty of elliptic curve discrete logarithm problem (ECDLP) before long. Since then, researchers have proposed a lot of secure authentication schemes that are constructed with ECC since ECC is efficient to decrease computation cost [41]. The definition of ECC can be depicted as follows.

Let p be a large prime number; F_p is a finite field over p. Elliptic curve E/E_p meets equation $y^2 = x^3 + ax + b \bmod p$ with $a, b \in F_p$ and $(4a^3 + 27b^2) \bmod p \neq 0$. Let point Θ be an infinite point. Θ and other points in E/E_p form an addictive group G. Given P and Q are different points on E/E_p, $P+Q$ is defined as point addition. $m \cdot P = \underbrace{P + P + \cdots + P}_{m \text{ times}}$ is defined as scalar multiplication. n is defined as order if n is the smallest number that meets $n \cdot P = \Theta$.

3.2. Complexity Assumptions. Elliptic curve discrete logarithm problem (ECDLP): given two random points $P, Q \in E/E_p$ and $Q = x \cdot P$, without knowing $x \in_R Z_p^*$, it is hard to compute x from Q. The probability for an adversary A to solve the ECDLP problem is $Adv_A^{\text{ECDLP}} = \Pr[A(P, Q = x \cdot P) = x]$. The hardness is that to compute a from Q is negligible [42].

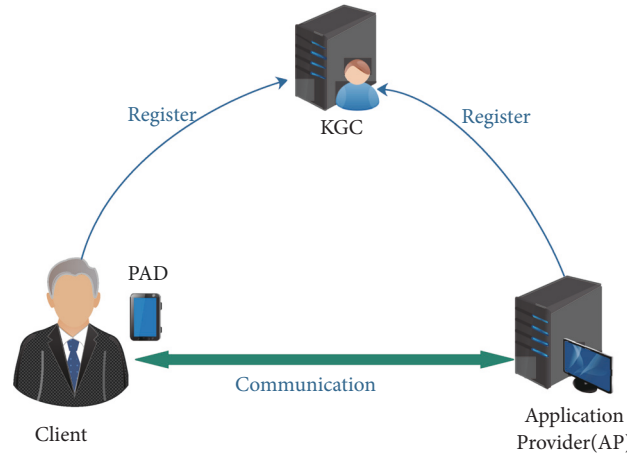

Figure 2: A common network structure of WBANs.

4. System Model and Security Model

4.1. System Model. There are three main entities in WBANs, i.e., key generation center (KGC), clients (including his/her PDA), and application providers (AP). KGC generates the system parameters and location public key and secret key for APs. Each client generates his/her secret value and then registers with KGC to obtain their public key, partial private key, and PDA with system parameter and partial key. At last, the clients could sign and send their messages to APs. In the process, AP and client should be authenticated each other and obtain an identical session key. The common network structure of wireless body area networks (WBANs) is illustrated in Figure 2.

Generally speaking, the messages in WBANs include sensitive health data. To ensure data integrity and identity authentication, these data should be signed and encrypted by PDA. The data with a signature could fall into two types: valid signature that can pass AP's authentication and invalid signature that cannot pass AP's authentication. When AP receives messages from different clients, AP can authenticate message one by one and also can adopt a more efficient way to authenticate multimessages, such as batch authentication. In our proposed scheme, batch authentication is used to improve authentication efficiency.

4.2. Security Model. In this section, we analyze the adversary model of certificateless authentication scheme for WBANs. As Al Riyami's work [18], two-level attacks exist in the certificateless PKC. One is type-I adversary (called $\mathcal{A}_{\mathcal{I}}$) who is able to simulate an "outsider" attacker; another is type-II adversary who is able to simulate an "insider" attacker (called $\mathcal{A}_{\mathcal{II}}$), who may be an "honest but curious" KGC. $\mathcal{A}_{\mathcal{I}}$ cannot get system secret key and users' partial key; however

Table 1: Notations used and description.

Symbol	Description
G	Acyclic group on an ECC with order q
P	The generator point of group G
s	The secret key of TA
P_{pub}	The public key of TA
RID_i	The real identity of a client
ID_A	The identity of a AP
PID_i	The pseudo identity of client
T	Validity period of pseudo identity
t	signature time
$H(.)$	One-way hash function

it could compromise users' secret value. $\mathscr{A}_{\mathscr{I}.\mathscr{I}}$ can get the system secret key and users' partial key but cannot get user secret value [43].

According to the ability of adversary $\mathscr{A}$ (include $\mathscr{A}_{\mathscr{I}}$ and $\mathscr{A}_{\mathscr{I}\mathscr{I}}$) and the system model of WBANs, we define security model as a game between a challenger $\mathscr{C}$ and $\mathscr{A}$ under the random Oracle model for the proposed scheme. Three steps are included in the game.

Initialization: $\mathscr{C}$ generates system parameters and system secret key. Then $\mathscr{C}$ gives the public parameters to $\mathscr{A}$.

Oracle query: $\mathscr{A}$ can make queries with h Oracle, *Create-User*, *Replace-Public-Key*, *Extract-Secret-Value*, *Extract-Partial-Key*, and *Sign* Oracle at will, unlimited query times and order. Then $\mathscr{C}$ answers $\mathscr{A}$ by the definition of game.

Output: $\mathscr{C}$ forges a signature after $\mathscr{A}$ has finished the above Oracle queries. At last, the advantage of successfully forging a valid signature is analyzed.

According to the definition of the game, $\mathscr{A}$ can breach the authentication scheme ϕ only if $\mathscr{A}$ could make a valid signature and pass authentication. Let $Adv_{\phi}^{Auth}(\mathscr{A})$ be the probability that $\mathscr{A}$ can breach ϕ during the game.

Definition 1. An authentication scheme for WBANs can be determined to be secure only if the probability $Adv_{\phi}^{Auth}(\mathscr{A})$ is negligible for any probabilistic-polynomial-time (PPT) adversary $\mathscr{A}$.

As definition of security requirement in most works for WBAN, we also agree that a secure certificateless authentication scheme for WBAN should provide anonymity, mutual authentication, traceability, and session key establishment; it also should be secure against modification attack, impersonation attack, replay attack, batch authentication attack, and other security attacks [44].

5. Review and Analysis of Ji *et al.*'s Scheme

In this section, we will review and analyze Ji *et al.*'s scheme [8]. To more clearly, Table 1 lists the notations and their descriptions adopted in Ji *et al.*'s scheme.

5.1. Review of Ji et al.'s Scheme. There are four phases in Ji *et al.*'s scheme [8], and the four phases can be briefly depicted as follows.

System Initialization Phase. TA executes this phase based on security parameter l.

(1) Choose two prime numbers p and q, define a finite field F_p, and then generate group G with order q on F_p.

(2) Let P be a generator of G, choose $s \in_R Z_q^*$, and compute $P_{pub} = sP$ as its public key. Then choose four one-way hash functions, $H_0, H_1, H_2, H_3 \longrightarrow Z_q^*$.

(3) Select $z_A \in_R Z_q^*$ for each registered AP and compute $b_A = z_A + sH_0(ID_A)$ as AP's private key and $B_A = z_A P$ as AP's public key.

Pseudo Identity Generation and Message Singing Phase. In this phase, each valid client should register with TA, then he/she can sign messages with his/her private key and send to AP. The detailed steps are as follows:

(1) The client chooses $r_i, x_i \in_R Z_q^*$, computes $X_i = x_i P$ and $PID_{i,1} = r_i P$, and then sends $\{RID_i, PW_i, PID_i, X_i\}$ to TA via a secure way.

(2) TA computes $\beta = H_0(RID_i) \oplus H_0(PW_i)$ and $PID_{i,2} = RID_i \oplus H_2(sPID_{i,1}, T_i)$, where T_i is the validity period of pseudo identity. Then TA chooses $w_i \in_R Z_q^*$ and computes $Y_i = w_i P$ and $y_i = w_i + s\alpha \bmod q$, where $\alpha_i = H_1(PID_i, X_i)$ and $PID_i = (PID_{i,1}, PID_{i,1}, T_i)$. Finally, TA loads $\{PID_i, y_i, \beta, Y_i\}$ into the client's PDA. Now, the client's private key is $SK_i = (x_i, y_i)$, and public key is $PK_i = (X_i, Y_i)$.

(3) Before signing a message, the client should input his RID_i and PW_i into his/her PDA. PDA checks whether it meets $\beta \stackrel{?}{=} H_0(RID_i) \oplus H_0(PW_i)$. If it does, the client can sign by using PDA as next step.

(4) Assume medical message be M_i; PDA chooses $d_i \in_R Z_q^*$ and timestamps t_i and computes $D_i = d_i P$, $u_i = H_3(M_i, PID_i, D_i, t_i)$, $\sigma_i = x_i + y_i + d_i \cdot u_i \bmod q$, and $K = d_i(B_A + H_0(ID_A)P_{pub})$, where K will be the session key between AP and the client. At last, PDA sends $\{PID_i, M_i, \sigma_i, D_i, t_i\}$ to AP.

Authentication Phase. AP can authenticate messages by the following two ways.

(i) Individual Authentication. When receiving a message $\{PID_i, M_i, \xi_i, D_i, t_i\}$, AP checks whether T_i and t_i are valid. If they do, AP computes $\alpha_i = H_1(PID_i, X_i)$ and $u_i = H_3(M_i, PID_i, D_i, t_i)$ and checks whether $\sigma_i P \stackrel{?}{=} X_i + Y_i + \alpha_i P_{pub} + u_i D_i$ holds or not. If it holds, AP accepts the message and computes session key $K = b_A D_i$ and then sends $MAC_K(B_A)$ to the client. At last, the client uses K as session key if the received $MAC_K(B_A)$ is identical to his/her $MAC_K(B_A)$.

(ii) Batch Authentication. When receiving n messages $\{PID_i, M_i, \xi_i, D_i, t_i\}_{i=1 \text{ to } n}$ from different clients, AP checks T_i and t_i for each message. Then AP computes $\alpha_i = H_1(PID_i, X_i)$ and $u_i = H_3(M_i, PID_i, D_i, t_i)$ for each message and checks whether the n messages meet the following equation:

$$\left(\sum_{i=1}^{n} \sigma_i\right) P = \sum_{i=1}^{n} X_i + \sum_{i=1}^{n} Y_i + \left(\sum_{i=1}^{n} \alpha_i\right) P_{pub} + \sum_{i=1}^{n} (u_i D_i) \tag{1}$$

If does, AP accepts these messages.

Password Change Phase. For security of PDA, the client can renew password PW_i locally by following steps.

(1) The client inputs RID_i and old password PW_i; the PDA checks $\beta \stackrel{?}{=} H_0(RID_i) \oplus H_0(PW_i)$. If it does, the PDA requires the client to input new password PW_i^*, then computes $\beta^* = \beta \oplus H_0(PW_i) \oplus H_0(PW_i^*)$, and replaces β with β^*.

5.2. Analysis of Ji et al.'s Scheme. In this subsection, the security deficiencies of Ji *et al.*'s scheme are analyzed.

(i) Not Be Secure against Forge Attack. Ji *et al.* show that their scheme could resist any forge attacks. However, any PPT $\mathscr{A}_{\mathscr{J}}$ could lightly win Game I in their scheme; that is, it could not be secure against forge attack. Assuming that the client's identity is PID_i, the adversary is $\mathscr{A}_{\mathscr{J}}$. $\mathscr{A}_{\mathscr{J}}$ launches the forge attack as the following steps:

(1) $\mathscr{A}_{\mathscr{J}}$ has intercepted or received a valid message $\{PID_i, M_i, \xi_i, D_i, t_i\}$, which meets verification function $\sigma_i P = X_i + Y_i + \alpha_i P_{pub} + u_i D_i$. Then $\mathscr{A}_I$ selects $w_i^* \in_R Z_q^*$, message M_i^*, and timestamps t_i^*.

(2) $\mathscr{A}_I$ computes $Y_i^* = w_i^* P - (X_i + \alpha_i P_{pub})$, $D_i^* = d_i^* P$, $u_i^* = H_3(M_i^*, PID_i, D_i^*, t_i^*)$, and $\sigma_i^* = w_i^* + u_i^* d_i^* \bmod q$, where PID_i is a valid pseudo identity. At last, $\mathscr{A}_I$ sends the forged message $\{PID_i, M_i^*, \xi_i^*, D_i^*, t_i^*\}$ to AP by using PID_i's identity.

(3) AP receives message $\{PID_i, M_i^*, \xi_i^*, D_i^*, t_i^*\}$, and checks whether the equation $\sigma_i^* P = X_i + Y_i^* + \alpha_i P_{pub} + u_i^* D_i^*$ holds or not. Let us expand the equation as follows:

$$\begin{aligned} X_i + Y_i^* + \alpha_i P_{pub} + u_i^* D_i^* &= X_i + Y_i^* + \alpha_i P_{pub} + u_i^* D_i^* \\ &= X_i + \left(-\left(\alpha_i P_{pub} + X_i\right) + w_i^* P\right) + \alpha_i P_{pub} + u_i^* D_i^* \\ &= Y_i^* + u_i^* D_i^* = \left(w_i^* + u_i^* d_i^*\right) P = \sigma_i^* P \end{aligned} \quad (2)$$

As shown above, $\mathscr{A}_{\mathscr{J}}$ can forge a valid message by using PID_i's identity easily. Therefore, Ji *et al.*'s scheme cannot resist any $\mathscr{A}_{\mathscr{J}}$'s forge attack.

(ii) Not Be Secure against Batch Authentication Attack. The adversary $\mathscr{A}_{\mathscr{J}}$ can also launch security attack in the batch authentication step of Ji *et al.*'s scheme. $\mathscr{A}_{\mathscr{J}}$ can do as the following steps.

(1) $\mathscr{A}_{\mathscr{J}}$ can forge two signatures $\sigma_1 = x_i + y_i$ and $\sigma_2 = u_i d_i$ on two messages $\{PID_i, M_i, \sigma_1, D_i, t_i\}$ and $\{PID_i, M_i, \sigma_2, D_i, t_i\}$, which cannot meet the verification. However, σ_1 and σ_2 can meet the batch authentication function of Ji *et al.*'s scheme as $\sum_1^2 \sigma_i P = \sum_1^2 X_i + \sum_1^2 Y_i + \sum_1^2 \alpha_i P_{pub} + \sum_1^2 u_i D_i = X_i + Y_i + \alpha_i P_{pub} + u_i D_i$.

Therefore, Ji *et al.*'s scheme cannot resist any $\mathscr{A}_{\mathscr{J}}$'s batch authentication attack.

6. The Improved Certificateless Authentication Scheme

In this section, an improved and secure certificateless authentication scheme for WBANs with conditional privacy-preserving (called CasCP) is proposed. The proposed CasCP consists of five phases: system initialization phase, pseudo identity generation phase, message signing phase, authentication phase, and password change phase.

Table 2: New notations and description in our scheme.

Symbol	Description
KGC	Key Generation center
$h(.)$	One-way hash function
$MAC_K(.)$	One-hash function with key K
l	Security-level parameter

To be clear, four new notations and descriptions that adopted in CasCP are listed in Table 2.

Next, the five phases are described as the following subsections.

6.1. System Initialization Phase. The KGC runs this phase with security level parameter l as follows.

(1) KGC chooses two prime numbers p and q and defines a finite field F_p and then generates group G with order q on F_p.

(2) Let P be one of generators of G. KGC chooses $s \in_R Z_q^*$ and computes $P_{pub} = sP$ as its public key. Then choose four one-way hash functions, $h_0, h_1, h_2, h_3 \longrightarrow Z_q^*$.

(3) KGC selects $z_A \in_R Z_q^*$ for each registered AP and computes $b_A = z_A + s \cdot h_0(ID_A)$ as AP's private key and $B_A = z_A P$ as AP's public key.

6.2. Pseudo Identity Generation Phase. Each WBANs client should register with KGC when he/her wants to obtain healthcare services. The client and KGC complete the pseudo identity phase as follow steps.

(1) Assume the client real identity be RID_i and his/her login password for PDA be PW_i. He/she chooses $x_i \in_R Z_q^*$, computes $X_i = x_i P$, and then sends $\{RID_i, PW_i, X_i\}$ to KGC via a secure way.

(2) Upon receiving $\{RID_i, PW_i, X_i\}$, KGC chooses $w_i \in_R Z_q^*$ and expiration time T_i and then computes $Y_i = w_i P$, $\beta = h_0(RID_i) \oplus h_0(PW_i)$, $PID_i = RID_i \oplus h_1(sX_i, T_i, Y_i)$, $\alpha_i = h_2(PID_i, X_i, Y_i, T_i)$, and $y_i = w_i + s \cdot \alpha \bmod q$. Finally, KGC loads $\{PID_i, y_i, \beta, Y_i, X_i, T_i\}$ into the client's PDA.

(3) When the client receives the PDA from KGC, he/she inputs RID_i and PW_i into PDA. Next PDA checks whether $\beta = h_0(RID_i) \oplus h_0(PW_i)$ holds or not. If it holds, the client's private key is $SK_i = (x_i, y_i)$ and public key is $PK_i = (X_i, Y_i)$. Otherwise, he/she registers again as next step.

6.3. Message Signing Phase. In this phase, the client signs messages by using PDA when he/she needs to communicate with others (such as AP) as the following steps.

(1) The client inputs RID_i and PW_i into PDA firstly. Then PDA checks whether $\beta = h_0(RID_i) \oplus h_0(PW_i)$ holds or not, where β is stored in the PDA. If it holds, the client can sign message by PDA.

(2) Assume the medical message be M_i. PDA chooses $d_i \in_R Z_q^*$ and timestamps t_i and then computes $D_i = d_i P$, $u_i = h_3(M_i, PID_i, X_i, T_i, Y_i, D_i, t_i)$, $\sigma_i = x_i + y_i + d_i \cdot$

Client and PDA		AP
Input RID_i, PW_i		
Check $\beta = ? h_0(RID_i) \oplus h_0(PW_i)$ $d_i \in Z_q^*$, $D_i = d_i P$ $u_i = h_3(M_i, PID_i, X_i, T_i, Y_i, D_i, T_i, t_i)$ $\sigma_i = x_i + y_i + d_i u_i \bmod q$ $K = d_i(B_A + h_0(ID_A)P_{pub})$ $msg_1 = \{M_i, PID_i, X_i, T_i, Y_i, D_i, t_i, \sigma_i\}$	msg_1	Check T_i, t_i $\alpha_i = h_2(PID_i, X_i, Y_i, T_i)$ $u_i = h_3(M_i, PID_i, X_i, T_i, Y_i, D_i, T_i, t_i)$ $\sigma_i P = ? X_i + Y_i + \alpha_i P_{pub} + u_i D_i$ $K^* = b_A D_i$ $msg_2 = \{MAC_{K^*}(B_A)\}$
Check $MAC_K(B_A) = ? MAC_{K^*}(B_A)$	msg_2	

Figure 3: Message signing and individual authentication phase.

$u_i \bmod q$, and $K = d_i(B_A + h_0(ID_A)P_{pub})$, where K is the session key between AP and the client. At last, PDA sends $\{M_i, PID_i, X_i, T_i, Y_i, D_i, t_i, \sigma_i\}$ to AP.

6.4. Authentication Phase. To ensure the security of data, the client and AP can authenticate each other in the proposed scheme. In order to further improve the authentication efficiency, batch authentication is provided. Next, individual authentication and batch authentication are presented.

(i) Individual Authentication. (1) When receives a message $\{M_i, PID_i, X_i, T_i, Y_i, D_i, t_i, \sigma_i\}$ from the client, AP checks whether T_i and t_i valid. If they do, AP computes $\alpha_i = h_2(PID_i, X_i, Y_i, T_i)$ and $u_i = h_3(M_i, PID_i, X_i, T_i, Y_i, D_i, t_i)$ and checks whether the verification equation

$$\sigma_i P = X_i + Y_i + \alpha_i P_{pub} + u_i D_i \tag{3}$$

holds or not. If it holds, AP accepts the message and computes session key $K^* = b_A D_i$ and then sends $MAC_{K^*}(B_A)$ to the client.

(2) After receiving $MAC_{K^*}(B_A)$ from AP, the client uses his/her K that obtained in message signing phase to compute $MAC_K(B_A)$ and then checks whether the received $MAC_{K^*}(B_A)$ is identical to his/her $MAC_K(B_A)$. If it does, the client and AP have authenticated each other successfully and obtained an identical session key K for subsequent communications.

The message signing and individual authentication phase are illustrated as Figure 3.

(ii) Batch Authentication. When receiving n messages $\{M_i, PID_i, X_i, T_i, Y_i, D_i, t_i, \sigma_i\}_{i=1 \text{ to } n}$ from different clients, AP can execute batch authentication for the n messages.

(1) AP checks T_i and t_i for each message and then computes $\alpha_i = h_2(PID_i, X_i, Y_i, T_i)$ and $u_i = h_3(M_i, PID_i, X_i, T_i, Y_i, D_i, t_i)$ for each message.

(2) AP selects a small random integer vector $v = \{v_1, v_2, \ldots, v_n\}$, which have little computation cost in scalar multiplication [41].

(3) At last, AP checks whether the n messages meet the following equation:

$$\left(\sum_{i=1}^{n} v_i \sigma_i\right) P = \sum_{i=1}^{n} v_i X_i + \sum_{i=1}^{n} v_i Y_i + \left(\sum_{i=1}^{n} v_i \alpha_i\right) P_{pub} + \sum_{i=1}^{n} (v_i u_i D_i) \tag{4}$$

If it does, AP accepts these messages.

6.5. Password Change Phase. This phase is same as Ji *et al.*'s scheme, and the description will not be repeated here.

7. Security Proof and Analysis

In this section, a formal security proof of CasCP is presented. It shows that CasCP is unforgeable against adversary $\mathcal{A}$ (included $\mathcal{A}_{\mathcal{I}}$ and $\mathcal{A}_{\mathcal{II}}$), and CasCP can meet the security requirements of WBANs.

7.1. Security Proof. Next, CasCP is assessed on the security under the random Oracle model.

Theorem 2. *Assume $\mathcal{A}_{\mathcal{I}}$ be a PPT adversary who could win Game I with nonnegligible probability. Let $\mathcal{C}$ be a challenger who could solve ECDLP problem on advantage $\varepsilon_1 \geq (1 - q_{h_1}/q)^{q_c}(1 - 1/q_c)^{q_e}(1 - q_{h2}/q)(1 - q_{h3}/q)(1/q_c)\varepsilon$, where $q_{h_1}, q_{h_2}, q_{h_3}, q_c, q_e$ are the times of executing h_1, h_2, h_3, Create-User, and Extract-Partial-Key Oracle query, respectively.*

Proof. Let $\mathcal{A}_{\mathcal{I}}$ be a PPT adversary, which attempts to forge target client ID_o's valid message. $\mathcal{A}_{\mathcal{I}}$ could win Game-I with

a probability ε. Given an ECDLP instance $(G, P, Q = sP)$, $\mathscr{C}$ runs $\mathscr{A}_{\mathscr{J}}$ as a subroutine to solve the ECDLP instance. □

Step 1. $\mathscr{C}$ executes system initialization, and publics the parameters to A_I, given an ECDLP instance $(G, P, Q = P_{pub})$ to $\mathscr{C}$, from which it tries to compute s from P_{pub}.

Step 2. $\mathscr{A}_{\mathscr{J}}$ executes Oracle queries within limited query times, then $\mathscr{C}$ will answer $\mathscr{A}_{\mathscr{J}}$ as the following rules.

(i) Hash-Queries. $\mathscr{C}$ answers $\mathscr{A}_{\mathscr{J}}$ when he/she executes Oracle queries as follows.

(a) h_1*-Query*. As $\mathscr{A}_{\mathscr{J}}$ executes this query with (ID, X), $\mathscr{C}$ looks for (ID, X) in list L_{h_1}. If L_{h_1} has the entry, $\mathscr{C}$ returns τ_{h_1} to $\mathscr{A}_{\mathscr{J}}$. Otherwise, $\mathscr{C}$ chooses τ_{h_1}, x, T at random and sets $\tau_{h_1} \longleftarrow h_1(u \cdot Q, X, T)$. Finally $\mathscr{C}$ returns τ_{h_1} to $\mathscr{A}_{\mathscr{J}}$.

(b) h_2*-Query*. As $\mathscr{A}_{\mathscr{J}}$ executes this query with (ID), $\mathscr{C}$ looks for (ID) in list L_α. If L_α has the entry, $\mathscr{C}$ returns τ_α to $\mathscr{A}_{\mathscr{J}}$. Otherwise, $\mathscr{C}$ chooses $w \in Z_q^*$ at random and computes $Y = wP$ and sets $\tau_\alpha \longleftarrow h_2(ID, Y, X, T)$. Then $\mathscr{C}$ returns τ_α to $\mathscr{A}_{\mathscr{J}}$.

(c) h_3*-Query*. As $\mathscr{A}_{\mathscr{J}}$ executes this query with (ID, M), $\mathscr{C}$ looks for (ID, M) in sign list L_s. If L_s has the entry, $\mathscr{C}$ returns τ_u to $\mathscr{A}_{\mathscr{J}}$. Otherwise, $\mathscr{C}$ chooses $d \in Z_q^*$ at random, computes $D = dP$, and sets $\tau_u \longleftarrow h_3(m, PID, X, T, Y, D, t)$, where PID, X, T, and Y can be obtained from other h queries and create-user query. Then $\mathscr{C}$ returns τ_u to $\mathscr{A}_{\mathscr{J}}$.

(ii) Create-User(ID). As $\mathscr{A}_{\mathscr{J}}$ executes this query with (ID), $\mathscr{C}$ looks for (ID) in user list L_u. If L_u has an entry with ID, $\mathscr{C}$ returns X_{ID} to $\mathscr{A}_{\mathscr{J}}$. Otherwise, $\mathscr{C}$ randomly selects $x_{ID}, w_{ID}, h1_{ID} \in Z_q^*$ and computes $PID = ID \oplus h1_{ID}$, $PK_{ID} = w_{ID} \cdot P + \alpha \cdot Q$, and $y_{ID} = \perp$. Next, $\mathscr{C}$ adds $\{ID, x_{ID}, w_{ID}, Y_{ID}, X_{ID}, PK_{ID}\}$ to the corresponding list L_u, L_{h1}, L_{h2}.

(iii) Replace-Public-Key(ID). As $\mathscr{A}_{\mathscr{J}}$ executes this query with (ID), $\mathscr{C}$ chooses $x \in Z_q^*$ at random and computes $X = x \cdot P$, Finally, $\mathscr{C}$ adds (x, X) in L_u and sends (x, X) to $\mathscr{A}_{\mathscr{J}}$. As for y, $\mathscr{C}$ returns $\perp$.

(iv) Extract-Secret-Value(ID). As $\mathscr{A}_{\mathscr{J}}$ executes this query with (ID), $\mathscr{C}$ looks for user list L_u. If L_u has the entry, $\mathscr{C}$ returns x to $\mathscr{A}_{\mathscr{J}}$.

(v) Extract-Partial-Key(ID). As $\mathscr{A}_{\mathscr{J}}$ executes this query with (ID), $\mathscr{C}$ looks for user list L_u. If $ID = ID_o$, $\mathscr{C}$ sends $\perp$ to $\mathscr{A}_{\mathscr{J}}$. Else if L_u has the entry with ID, $\mathscr{C}$ sends PK to $\mathscr{A}_{\mathscr{J}}$, else $\mathscr{C}$ runs *Create-User*(ID) query and sends PK to $\mathscr{A}_{\mathscr{J}}$.

(vi) Sign(ID, M). As $\mathscr{A}_{\mathscr{J}}$ executes this query with (ID, M), $\mathscr{C}$ looks for tuple (ID) in L_u. If $ID \neq ID_o$, $\mathscr{C}$ randomly selects $d \in Z_q^*$, computes $D = dP$, $u = h_3(M, PID, X, T, Y, D, t)$, and $\sigma = x + y + u \cdot d \bmod q$, and then adds d, D, u in L_s. If $ID = ID_o$, $\mathscr{C}$ selects $\alpha, d, u \in Z_q^*$ at randomly and computes $D = dP$, $X = \sigma \cdot P - Y - u\alpha \cdot Q - u \cdot D$ and then adds d, D to L_s. At last, $\mathscr{C}$ returns (σ, D) to $\mathscr{A}_{\mathscr{J}}$.

Step 3. Finally, $\mathscr{C}$ obtains a forged message (ID, M, D, σ) under certain restrictions that the $\mathscr{A}_{\mathscr{J}}$ never makes *Extract-Partial-key* query with ID and *Sign* query with (ID, M). If $ID \neq ID_o$, $\mathscr{C}$ stops the game. Otherwise, $\mathscr{C}$ looks for the corresponding entry in L_{h2}, L_u, L_s. If there is not the corresponding σ, it stops the game. Otherwise, σ meets the following equation:

$$\sigma \cdot P = X + Y + \alpha \cdot Q + ud \cdot P \tag{5}$$

$\mathscr{A}_{\mathscr{J}}$ can replay the game based on forgery lemma [45]; he/her could obtain another forged message (ID, M, D^*, σ^*) by selecting another σ^*, α^*, d^*.

$$\sigma^* \cdot P = X + Y + \alpha^* \cdot Q + u^* d^* \cdot P \tag{6}$$

According to (5) and (6), $\mathscr{C}$ could obtain the $s = (((\sigma - \sigma*) - (ud - u^*d^*))/(\alpha - \alpha^*)) \bmod q$; i.e., $\mathscr{C}$ could solve the ECDLP problem. Next, the probability of $\mathscr{C}$ which obtains the correct solution for $(P, Q = sP)$ is analyzed. If $\mathscr{C}$ has done successfully, two events must happen.

(i) $Ev1$: never stop the game.

(ii) $Ev2$: σ is valid.

Therefore, the advantage of $\mathscr{C}$ is $\varepsilon_1 = Pr[Ev1 \cap Ev2] = Pr[Ev1]\ Pr[Ev2 \mid Ev1]$. The occurrence probability of $Ev1$ could be gained in *Create-user*, *Extract-Partial-key*, and *Sign* Oracle query during the game. Therefore, it can obtain $Pr[Ev1] \geq (1 - q_{h_1}/q)^{q_c}(1 - 1/q_c)^{q_e}(1 - q_{h2}/q)(1 - q_{h3}/q)q)(1/q_c)$. Therefore, we can get $\varepsilon_1 \geq (1 - q_{h_1}/q)^{q_c}(1 - 1/q_c)^{q_e}(1 - q_{h2}/q)(1 - q_{h3}/q)(1/q_c)\varepsilon$.

Theorem 3. *Assume $\mathscr{A}_{\mathscr{J}\mathscr{J}}$ is a PPT super type-II adversary who can succeed in Game-II with nonnegligible probability. Let $\mathscr{C}$ be a challenger who can solve the ECDLP problem with advantage $\varepsilon_2 \geq (1 - q_{h_1}/q)^{q_c}(1 - 1/q_c)^{q_r}(1 - 1/q_c)^{q_x}(1 - q_{h2}/q)(1 - q_{h3}/q)(1/q_c)\varepsilon$, where $q_{h_1}, q_{h_2}, q_{h_3}, q_c, q_r, q_x$ denote the times of executing h_1, h_2, h_3, Create-User, Replace-Public-Key, and Extract-Secret-Value Oracle query, respectively.*

Proof. Assume $\mathscr{A}_{\mathscr{J}\mathscr{J}}$ is a type-II adversary, and $\mathscr{A}_{\mathscr{J}\mathscr{J}}$ attempts to forge target client ID_o's valid message. Then $\mathscr{A}_{\mathscr{J}\mathscr{J}}$ could win Game-II with probability ε. Given an ECDLP instance $(G, P, Q = x_o \cdot P)$, let $\mathscr{C}$ be a challenger. Next, $\mathscr{C}$ runs $\mathscr{A}_{\mathscr{J}\mathscr{J}}$ as a subroutine to solve ECDLP problem. □

Step 1. $\mathscr{C}$ executes system initialization and public parameters and s to $\mathscr{A}_{\mathscr{J}\mathscr{J}}$. Assume $(G, P, Q = x_o \cdot P)$ is given an ECDLP instance; $\mathscr{C}$ tries to compute x_o from Q.

Step 2. $\mathscr{A}_{\mathscr{J}\mathscr{J}}$ executes Oracle queries within limited query times, then $\mathscr{C}$ will answer $\mathscr{A}_{\mathscr{J}\mathscr{J}}$ as the following rules.

(i) Hash-Queries. $\mathscr{C}$ answers $\mathscr{A}_{\mathscr{J}\mathscr{J}}$ when he/she executes Oracle queries as follows.

(a) h_1*-Query*. As $\mathscr{A}_{\mathscr{J}\mathscr{J}}$ executes the query with (ID, X), $\mathscr{C}$ looks for (ID, X) in list L_{h_1}. If L_{h_1} has the entry, $\mathscr{C}$ returns τ_{h_1} to $\mathscr{A}_{\mathscr{J}\mathscr{J}}$. Otherwise, $\mathscr{C}$ chooses $\tau_{h_1}, w \in Z_q^*$ at random and computes $Y = wP$ and sets $\tau_{h_1} \longleftarrow h_1(s \cdot X, T, Y)$. Finally $\mathscr{C}$ returns τ_{h_1} to $\mathscr{A}_{\mathscr{J}\mathscr{J}}$.

(b) h_2-Query and h_3-Query. As $\mathcal{A}_{\mathcal{I}\mathcal{I}}$ executes the two queries, $\mathcal{C}$ could answer $\mathcal{A}_{\mathcal{I}\mathcal{I}}$ as he/she answers $\mathcal{A}_{\mathcal{I}}$ in Game I.

(ii) Create-User(ID). As $\mathcal{A}_{\mathcal{I}\mathcal{I}}$ executes the query with (ID), $\mathcal{C}$ looks for user list L_u. If L_u has the entry, $\mathcal{C}$ returns TK_{ID}. Otherwise, if $ID = ID_o$, $\mathcal{C}$ chooses $w \in Z_*^q$ and $X \in G$ at random and current time T, calculates $Y = w \cdot P$, $PID = ID \oplus h_1(\alpha \cdot X, T, Y)$, $\alpha = h_2(PID, X, Y, T)$, and $y = w + s\alpha \bmod q$, and sets $x = \perp$. Then, $\mathcal{C}$ will add (ID, u, y, x, α) to list L_u, L_{h2}, respectively. If $ID \neq ID_o$, $\mathcal{C}$ chooses $u, x \in Z_*^q$ at random and current time T and calculates $U = u \cdot P$, $PID = ID \oplus h_1(\alpha u \cdot P, T)$, $\alpha = h_2(PID, X, Y, T)$, $y = w + \alpha s \bmod q$, and $X = x \cdot P$. Then, $\mathcal{C}$ will add $(ID, x, w, y, X, Y, \alpha)$ to corresponding list L_u, L_{h2}, respectively.

(iii) Replace-Public-Key(ID). As $\mathcal{A}_{\mathcal{I}\mathcal{I}}$ executes the query with (ID), $\mathcal{C}$ will answer $\mathcal{A}_{\mathcal{I}\mathcal{I}}$ as the following two cases: if $ID \neq ID_o$, $\mathcal{C}$ will answer $\mathcal{A}_{\mathcal{I}\mathcal{I}}$ with the definition of Partial Key Generation and Private key Generation algorithm. If $ID = ID_o$, $\mathcal{C}$ chooses $w \in Z_q^*$ and $X \in G$ at random. Next $\mathcal{C}$ calculates $Y = w \cdot P$, $PID = ID \oplus h_1(sX, T, Y)$, $\alpha = h_2(PID, X, Y, T)$, and $y = w + s\alpha \bmod q$ and sets $x = \perp$. Finally, $\mathcal{C}$ sends (Y, X) to $\mathcal{A}_{\mathcal{I}\mathcal{I}}$.

(iv) Extract-Secret-Value(ID). As $\mathcal{A}_{\mathcal{I}\mathcal{I}}$ executes the query with (ID), $\mathcal{C}$ looks for it in user list L_u. If L_u has the entry with ID, $\mathcal{C}$ sends x to $\mathcal{A}_{\mathcal{I}\mathcal{I}}$. Or, if $ID \neq ID_o$, $\mathcal{C}$ chooses $x \in_R Z_q^*$ at random and adds it to L_u as ID's secret value. Next $\mathcal{C}$ sends x to $\mathcal{A}_{\mathcal{I}\mathcal{I}}$. If $ID = ID_o$, $\mathcal{C}$ returns $\perp$.

(v) Extract-Partial-Key(ID). As $\mathcal{A}_{\mathcal{I}\mathcal{I}}$ executes the query with (ID), $\mathcal{C}$ looks for it in L_u. If L_u has the entry with ID, $\mathcal{C}$ sends y to $\mathcal{A}_{\mathcal{I}\mathcal{I}}$. Otherwise, $\mathcal{C}$ will execute *Create-User*(ID) query and then sends y to $\mathcal{A}_{\mathcal{I}\mathcal{I}}$.

(vi) Sign(ID, m). As $\mathcal{A}_{\mathcal{I}\mathcal{I}}$ executes the query with (ID, M), $\mathcal{C}$ looks for it in L_u. If $ID \neq ID_o$, $\mathcal{C}$ chooses $d \in Z_q^*$ at random and current time t and then calculates $D = d \cdot P$, $u = h_3(M, PID, X, T, Y, D, t)$, and $\sigma = x + y + du \bmod q$. Next $\mathcal{C}$ adds d, D, σ in L_s and sends (D, σ) to $\mathcal{A}_{\mathcal{I}\mathcal{I}}$. If $ID = ID_o$, $\mathcal{C}$ chooses $d \in Z_q^*$ at random and calculates $D = d \cdot Q$, $u = h_3(M, PID, X, T, Y, D, t)$, and $\sigma = x + y + du \bmod q$ and then adds σ, D to L_s. At last, $\mathcal{C}$ returns (σ) to $\mathcal{A}_{\mathcal{I}\mathcal{I}}$.

Step 3. At last, $\mathcal{A}_{\mathcal{I}\mathcal{I}}$ obtains a forged message (ID, M, D, σ) under the constrain restrictions that $\mathcal{A}_{\mathcal{I}\mathcal{I}}$ never makes *Extract-Partial-Key* query with ID and *Sign* query with (ID, M). If $ID \neq ID_o$, $\mathcal{C}$ stops the game. Otherwise, $\mathcal{C}$ looks for the corresponding entry in L_{h2}, L_u, L_s. If there is not corresponding σ, $\mathcal{C}$ stops the game or σ meets the following authentication equation:

$$\sigma \cdot P = Q + Y + \alpha \cdot P_{pub} + ud \cdot Q \tag{7}$$

$\mathcal{A}_{\mathcal{I}\mathcal{I}}$ can replay the game based on forgery lemma [45]; he/she could obtain another forged messages (ID, M, D^*, σ^*) by selecting another u^*, d^*.

$$\sigma^* \cdot P = Q + Y + \alpha \cdot P_{pub} + u^* d^* \cdot Q \tag{8}$$

According to (7) and (8), $\mathcal{C}$ could obtain the $x_o = ((\sigma - \sigma^*)/(ud - u^* d^*)) \bmod q$; i.e., $\mathcal{C}$ could solve the ECDLP problem. Next, the probability that $\mathcal{C}$ gains the correct solution for the instance $(P, Q = X_o = x_o \cdot P)$ is analyzed. If $\mathcal{C}$ has been successful, two events must happen.

(i) $Ev1$: never abort the game.

(ii) $EV2$: σ is valid.

Therefore, $\mathcal{C}$'s advantage is $\varepsilon_1 = Pr[Ev1 \cap Ev2] = Pr[Ev1]\ Pr[Ev2 \mid Ev1]$. The probability of $Ev1$'s occurrence can be gained in *Create-user*, *Extract-Partial-key*, and *Sign* Oracle query during the game. Therefore, it can obtain $Pr[Ev1] \geq (1 - q_{h_1}/q)^{q_c}(1 - 1/q_c)^{q_r}(1 - 1/q_c)^{q_x}(1 - q_{h2}/q)(1 - q_{h3}/q)(1/q_c)$. Therefore, we can get $\varepsilon_2 \geq (1 - q_{h_1}/q)^{q_c}(1 - 1/q_c)^{q_r}(1 - 1/q_c)^{q_x}(1 - q_{h2}/q)(1 - q_{h3}/q)(1/q_c)\varepsilon$.

Now, we can draw a conclusion that CapCP can resist two-level adversary on the condition of the ECDLP assumption which is established.

7.2. Other Security Analyses. Next, we will analyze whether CapCP meets the security requirements of WBANs.

(i) Anonymity. In CasCP, a client's real identity is embedded his/her pseudo identity $PID_i = RID_i \oplus h_1(sX_i, T_i, Y_i)$. PID_i is generated by KGC, any adversaries cannot retrieve the real identity from PID_i because $sX_i = sx_iP$, $X_i = x_iP$, and $P_{pub} = sP$ make up a classic CDH problem. Therefore CapCP provides anonymity for clients.

(ii) Mutual Authentication. After receiving a message $\{M_i, PID_i, X_i, T_i, Y_i, D_i, t_i, \sigma_i\}$ from a client, AP checks the validity and integrity of the message according to individual authentication equation. If it holds, the message can be regarded as a valid message. The AP signs and returns reply message in the same way to the client, the AP can also be securely authenticated. Therefore, CasCP can satisfy mutual authentication for WBANs.

(iii) Traceability. The clients' real identities are embedded in PID by $PID_i = RID_i \oplus h_1(sX_i, T_i, Y_i)$. KGC is the only authenticated one that can retrieve the real identity from PID_i because only KGC knows the system secret key s. Therefore, CasCP provides identity traceability for KGC.

(iv) Modification Attack. Assume a forged message $\{M_i, PID_i, X_i, T_i, Y_i^*, D_i^*, t_i^*, \sigma_i^*\}$ is modified from a valid message $\{M_i, PID_i, X_i, T_i, Y_i, D_i, t_i, \sigma_i\}$ by an adversary, the verifier could easily distinguish the forged message $\{M_i, PID_i, X_i, T_i, Y_i^*, D_i^*, t_i^*, \sigma_i^*\}$ because the forged message cannot meet the authentication equation $\sigma_i P = X_i + Y_i + \alpha_i P_{pub} + u_i D_i$. Therefore, CasCP is secure against modification attack.

(v) Session Key Establishment. In CasCP, the client and AP have a session key as $K = d_i(B_A + H_0(ID_A)P_{pub})$. From the definition of K, $K = d_i b_A P$, $D_i = d_i P$, and $PK_A = b_A P$ are CDH problem instance. An adversary cannot compute a valid session key because of ECDLP assumption's hardness. Therefore, CasCP can achieve secure session key establishment.

Table 3: The execution time of cryptographic operations.

Operation	Abbreviations	Execute time
Scalar multiplication	T_m	2.576
Exponentiation operation	T_e	3.857
Bilinear pairing operation	T_p	4.163

(vi) Impersonation Attack. To impersonate a client, an adversary must generate a valid message $\{M_i, PID_i, X_i, T_i, Y_i, D_i, t_i, \sigma_i\}$ to meet the authentication equation $\sigma_i P = X_i + Y_i + \alpha_i P_{pub} + u_i D_i$. But the adversary cannot generate the valid a valid message according to Theorems 2 and 3. Therefore, CasCP is secure against impersonation attack.

(vii) Replay Attack. An adversary replays an old message $\{M_i, PID_i, X_i, T_i, Y_i, D_i, t_i, \sigma_i\}$ by new time t_i in $\{M_i, PID_i, X_i, T_i, Y_i, D_i, t_i^*, \sigma_i\}$. However, AP can find that this message is invalid by verification equation $\sigma_i P = X_i + Y_i + \alpha_i P_{pub} + u_i D_i$ according to the ECDLP assumption's hardness. That is CasCP can be secure against replay attack.

(viii) Batch Authentication Attack. When an invalid message or more messages join in batch authentication process, CasCP uses a small random integer vector to break the inherent relationship among of the signatures of messages. Therefore, an adversary cannot use the invalid or forged messages to launch batch authentication attack.

(ix) Lost PDA Attack. To use PDA, the correct RID_i and PW_i must be input into PDA. However, the adversary cannot login the PDA without knowing RID_i and PW_i, even if the adversary has breached PDA and has got the data in PDA. However, the data is nothing useful for the adversary.

8. Performance Analysis

In this section, the performance analysis of computation and communication cost is presented among four authentication schemes for WBANs that are the proposed scheme (CapCP), Ji *et al.*'s scheme [8] (2018), He *et al.*'s scheme [7] (2017), and Wu *et al.*'s scheme [46] (2016).

It is important to be fair and objective for performance analysis. Therefore, we adopt the simulation results of cryptographic operation execution time in [8]. Their simulation environments are set as follows: operation system is Windows 8, hardware is formed with 2.50 CHz Intel Core i5-2450 CPU, memory is 8.00 GB, and PBC (pairing based cryptography) is used to run the related cryptographic operations. Table 3 lists the execution times of main time-consuming cryptographic operations; the other cryptographic operations, such as point addition operation and one-way hash function which are much less than scalar multiplication, are not included in the comparison.

8.1. Computation Cost Analysis. Next, the proposed CasCP is compared with three authentication schemes for WBANs in terms of computation cost in the client's message signing phase, AP's individual authentication phase, and AP's batch authentication phase.

In Wu *et al.*'s scheme, the computation cost of the client in message signing phase comprises three scalar multiplication and two exponentiation operations; the computation cost of the AP in individual authentication phase comprises three scalar multiplication, two exponentiation operations, and one bilinear pairing operation; the n messages computation cost of the AP in batch authentication phase comprises $3n$ scalar multiplication, $2n$ exponentiation operation, and n bilinear pairing operations.

In He *et al.*'s scheme, the computation cost of the client in message signing phase comprises four scalar multiplication operations; the computation cost of the AP in individual authentication phase comprises four scalar multiplications and one bilinear pairing operations; the n messages computation cost of the AP in batch authentication phase comprises $4n$ scalar multiplication and n bilinear pairing operations.

In Ji *et al.*'s scheme, the computation cost of the client in message signing phase comprises three scalar multiplication operations; the computation cost of the AP in the individual authentication phase comprises four scalar multiplications; the n messages computation cost of the AP in batch authentication phase comprises $n+3$ scalar multiplication operations.

The proposed CasCP scheme adds a random small integer vector in batch authentication to increase its security. But the increased computational overhead is small; therefore it will not be considered in the computation cost comparison. That is, CasCP's computation costs in different phase can be considered to be the same as Ji *et al.*'s scheme. Here it is not presented; please refer to the previous analysis for Ji *et al.*'s scheme.

On the results of Table 3, the total execution time of the three phases in the four schemes is drawn, shown in Table 4.

The computation cost times of the client in message signing phase of CasCP and Ji *et al.*' scheme are 7.728 *ms*, which decrease by 49% and 25% when compared with the corresponding computation time of Wu *et al.*'s scheme and He *et al.*' scheme. The computation cost time of AP in individual authentication phase is 7.728 *ms*, which decreases by 60% and 46% when compared with the corresponding computation time of Wu *et al.*'s scheme and He *et al.*' scheme. The more intuitive computation cost comparison of the two phases in the four schemes is shown in Figure 4.

The computation cost comparisons of AP in batch authentication phase (assume $n = 30$ messages) are illustrated in Figure 5. As shown in Figure 5, our proposed CasCP and Ji *et al.*' scheme take an advantage on computation cost than Wu *et al.*'s scheme and He *et al.*'s scheme.

According to the former computation cost analysis in batch authentication phase, the proposed CasCP and Ji *et al.*'s scheme have a clear advantage than the other two schemes. Figure 6 depicts the computation costs in batch authentication phase for the different number of messages of the four schemes. Therefore, CasCP and Ji *et al.*'s scheme are more efficient than Wu *et al.*'s scheme and He *et al.*'s scheme regardless of the number of messages.

Table 4: The computation cost comparison of the four schemes.

	message signing phase (client)	individual authentication phase (AP)
Wu's Scheme	$2T_e + 3T_m \approx 15.442ms$	$1T_p + 3T_m + 2T_e \approx 19.604$
He's Scheme	$4T_m \approx 10.304ms$	$1T_p + 4T_m \approx 14.446ms$
Ji's Scheme	$3T_m \approx 7.728ms$	$3T_m \approx 7.728ms$
CasCP	$3T_m \approx 7.728ms$	$3T_m \approx 7.728ms$

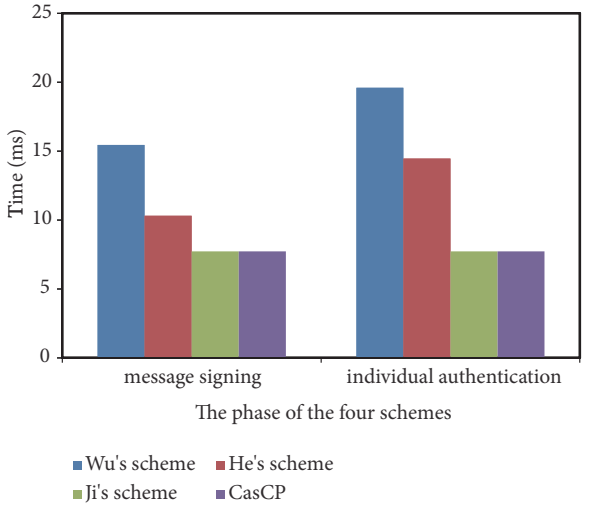

Figure 4: The computation costs of the two phases in the four schemes.

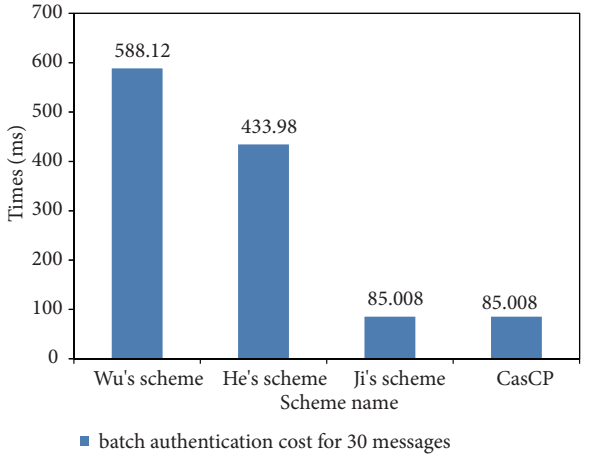

Figure 5: The computation costs of the four schemes for 30 messages in batch authentication phase.

In summary, compared with Wu *et al.*'s scheme and He *et al.*'s scheme, CasCP and Ji *et al.*'s scheme have lower computation cost in message signing phase, individual authentication phase, and batch authentication phase.

8.2. Communication Cost Comparison. In the subsection, we analyze the communication cost of the proposed CasCP and the three authentication schemes for WBANs in this subsection.

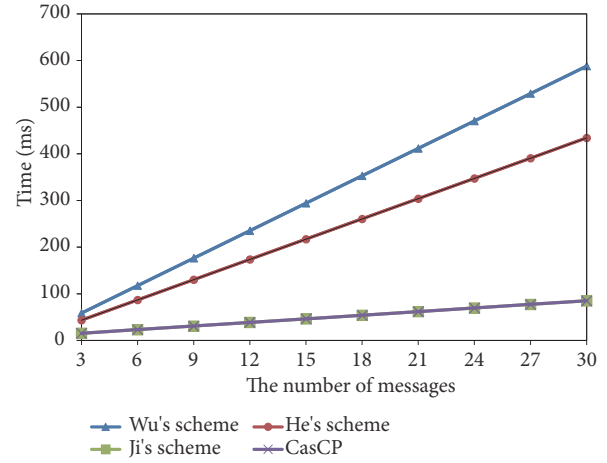

Figure 6: The computation costs of the four schemes for different number of messages in batch authentication.

According to the definitions of the above cryptographic operations, we assume that the size of p is 20 bytes, the element in G is 40 bytes, and the size of other communication elements in P is 20 bytes. For simplicity, message M_i is not included in the comparison.

In Wu *et al.*'s scheme, the message sent by a client to AP consists of $\{ID_c, V_i, auth_c, t_c\}$; the message sent by a client to AP consists of $\{R_{AP}, auth_{AP}, t_{AP}\}$. The messages include four elements in G, i.e., $(ID_c, V_i, R_{AP} \in G$, 40×3 bytes), and four elements in P, i.e., $(t_i, auth_c, T_{AP}, authe_{AP}$, 20×4 bytes); the total size of one communication round is 200 bytes.

In He *et al.*'s scheme, the message sent by a client to AP consists of $\{QID_i, T_i, t_i\}$; the message sent by a client to AP comprises $\{Y, auth_s\}$. The messages have four elements in G, i.e., $(QID_i, T_i, Y \in G$, 40×3 bytes), and two elements in P, i.e., $(t_i, auth_s$, 20×2 bytes); the total size of one communication round is 200 bytes.

In Ji *et al.*'s scheme, the message sent by a client to AP consists of $\{M_i, PID_i = \{PID_{i,1}, PID_{i,2}, X_i\}, T_i, Y_i, D_i, t_i, \sigma_i\}$, which has four elements in G, i.e., $(PID_{i,1}, X_i, Y_i, D_i \in G$, 40×4 bytes), and four elements in P, i.e., $(t_i, PID_{i,2}, T_i, \sigma_i$, 20×4 bytes). The message sent by a client to AP consists of $\{MAC_K(B_A)\}$. Therefore, the total size of one communication round is 240 bytes.

In CasCP, the message sent by a client to AP consists of $\{M_i, PID_i, X_i, T_i, Y_i, D_i, t_i, \sigma_i\}$, which has three elements in G, i.e., $(X_i, Y_i, D_i \in G$, 40×3 bytes), and four elements in P, i.e., $(t_i, PID_i, T_i, \sigma_i$, 20×4 bytes). The message sent by a client to AP consists of $\{MAC_K(B_A)\}$; the size of $\{MAC_K(B_A)\}$ is defined

Table 5: The comparison of communication cost.

	Client-AP Component	Size
Wu *et al.*'s scheme	Client ⟶ AP $\{ID_c, V_i, auth_c, t_c\}$ AP ⟶ Client $\{R_{AP}, auth_{AP}, t_{AP}\}$	200 bytes
He *et al.*'s scheme	Client ⟶ AP $\{QID_i, T_i, t_i\}$ AP ⟶ Client $\{Y, auth_s\}$	180 bytes
Ji *et al.*'s scheme	Client ⟶ AP $\{M_i, PID_i = \{PID_{i,1}, PID_{i,2}, X_i\}, T_i, Y_i, D_i, t_i, \sigma_i\}$ AP ⟶ Client $\{MAC_K(B_A)\}$	240 bytes
CapCP	Client ⟶ AP $\{M_i, PID_i, X_i, T_i, Y_i, D_i, t_i, \sigma_i\}$ AP ⟶ Client $\{MAC_K(B_A)\}$	200 bytes

Tip: M_i is excluded in comparison.

as 20 bytes. Therefore, the total size of one communication round is 200 bytes.

The communication cost comparison results of one communication round between a client and AP are shown in Table 5. Compared with Wu *et al.*'s scheme and He *et al.*'s scheme, CasCP has no advantage because the two schemes decrease communication cost by encrypting data. Tip, the encrypted data must be more than 20 bytes that we assumed. Compared with Ji *et al.*'s scheme, CasCP scheme's communication cost has decreased by 15.4%.

Overall, CasCP scheme needs less computation cost than Wu *et al.*'s scheme and He *et al.*'s scheme. CasCP incurs less communication cost than Ji *et al.*'s scheme under the premise of solving the security deficiencies of Ji *et al.*'s scheme, providing conditional privacy-preserving and batch authentication.

9. Conclusion and Future Work

To provide privacy protection, Ji *et al.* proposed a certificateless authentication scheme for WBANs. However, the security analysis in this paper demonstrates that their scheme cannot be secure against forgery attack and batch authentication attack. To solve the deficiencies, an improved certificateless authentication scheme with conditional privacy-preserving (called CasCP) constructs signature with ECC, without any bilinear pairing operation. CasCP also provides batch authentication function and conditional privacy-preserving. A rigid security proof and analysis prove that CasCP is secure against different level adversary's attacks, such as adversary $\mathcal{A}_{\mathcal{I}}$ and adversary $\mathcal{A}_{\mathcal{II}}$. Compared with similar authentication scheme, CasCP has some advantages in computation and communication cost. Therefore, the proposed CasCP is more suitable for the WBANs.

Although CasCP is efficient and more secure than similar recent proposed schemes, more efficient authentication scheme is more favored, especially lightweight authentication scheme. Therefore, our next work is to study a secure lightweight authentication scheme with batch verification function for WBANs.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

We declare that we do not have any commercial or associative interest that represents conflicts of interest in connection with the work submitted.

Acknowledgments

The work was supported in part by the National Natural Science Foundation of China under Grant 61862052 and the National Natural Science Function of Qinghai Province (2019-ZJ-7065 and 2017-ZJ-959Q).

References

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

[2] N. Dey, A. S. Ashour, F. Shi, S. J. Fong, and R. S. Sherratt, "Developing residential wireless sensor networks for ECG healthcare monitoring," *IEEE Transactions on Consumer Electronics*, vol. 63, no. 4, pp. 442–449, 2017.

[3] L. Wu, J. Wang, K.-K. R. Choo, and D. He, "Secure key agreement and key protection for mobile device user authentication," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 2, pp. 319–330, 2018.

[4] Z. Fei, B. Li, S. Yang, C. Xing, H. Chen, and L. Hanzo, "A survey of multi-objective optimization in wireless sensor networks: metrics, algorithms, and open problems," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 550–586, 2017.

[5] P. Kumar, S. Kumari, V. Sharma, A. K. Sangaiah, J. Wei, and X. Li, "A certificateless aggregate signature scheme for healthcare wireless sensor network," *Sustainable Computing: Informatics and Systems*, vol. 18, no. 1, pp. 80–89, 2018.

[6] Q. Feng, D. He, S. Zeadally, and H. Wang, "Anonymous biometrics-based authentication scheme with key distribution

for mobile multi-server environment," *Future Generation Computer Systems*, vol. 84, pp. 239–251, 2018.

[7] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Systems Journal*, vol. 11, no. 4, pp. 2590–2601, 2017.

[8] S. Ji, Z. Gui, T. Zhou, H. Yan, and J. Shen, "An efficient and certificateless conditional privacy-preserving authentication scheme for wireless body area networks big data services," *IEEE Access*, vol. 6, pp. 69603–69611, 2018.

[9] Q. Jiang, Z. Chen, B. Li, J. Shen, L. Yang, and J. Ma, "Security analysis and improvement of bio-hashing based three-factor authentication scheme for telecare medical information systems," *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, no. 4, pp. 1061–1073, 2018.

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

[11] M. Li, S. Yu, J. D. Guttman, W. Lou, and K. Ren, "Secure ad hoc trust initialization and key management in wireless body area networks," *ACM Transactions on Sensor Networks*, vol. 9, no. 2, article no. 18, 2013.

[12] H. Debiao, C. Jianhua, and H. Jin, "An ID-based client authentication with key agreement protocol for mobile client-server environment on ECC with provable security," *Information Fusion*, vol. 13, no. 3, pp. 223–230, 2012.

[13] A. S. Sangari and J. M. L. Manickam, "Public key cryptosystem based security in wireless body area network," in *Proceedings of the 2014 International Conference on Circuits, Power and Computing Technologies, ICCPCT 2014*, pp. 1609–1612, IEEE, Nagercoil, India, March 2014.

[14] J. Li, X. Chen, M. Li, J. Li, P. P. C. Lee, and W. Lou, "Secure deduplication with efficient and reliable convergent key management," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 6, pp. 1615–1625, 2014.

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

[16] X. Li, J. Niu, J. Liao, and W. Liang, "Cryptanalysis of a dynamic identity-based remote user authentication scheme with verifiable password update," *International Journal of Communication Systems*, vol. 28, no. 2, pp. 374–382, 2015.

[17] C. C. Tan, S. Zhong, H. Wang, and Q. Li, "Body sensor network security: an identity-based cryptography approach," in *Proceedings of the 1st ACM Conference on Wireless Network Security (WiSec '08)*, pp. 148–153, ACM, Alexandria, VA, USA, March-April 2008.

[18] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*, vol. 2894 of *Lecture Notes in Computer Science*, pp. 452–473, Springer, Taipei, Taiwan, 2003.

[19] G. Zheng, L. Yu, H. Xuan, and C. Kefei, "Two certificateless aggregate signatures from bilinear maps," in *Proceedings of the 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2007)*, pp. 188–193, IEEE, Qingdao, China, August 2007.

[20] X. Huang, Y. Mu, W. Susilo, D. S. Wong, and W. Wu, "Certificateless signatures: new schemes and security models," *The Computer Journal*, vol. 55, no. 4, pp. 457–474, 2012.

[21] X. Huang, W. Susilo, Y. Mu, and F. Zhang, "On the security of a certificateless signature scheme," in *Proceedings of the International Conference on Cryptology and Network Security*, vol. 3810 of *Lecture Notes in Computer Science*, pp. 13–25, Springer, Xiamen, China, 2005.

[22] K.-A. Shim, "Security models for certificateless signature schemes revisited," *Information Sciences*, vol. 296, pp. 315–321, 2015.

[23] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 416–432, Springer, Warsaw, Poland, 2003.

[24] L. Zhang and F. Zhang, "A new certificateless aggregate signature scheme," *Computer Communications*, vol. 32, no. 6, pp. 1079–1085, 2009.

[25] X. Liu, H. Zhu, J. Ma, Q. Li, and J. Xiong, "Efficient attribute based sequential aggregate signature for wireless sensor networks," *International Journal of Sensor Networks*, vol. 16, no. 3, pp. 172–184, 2014.

[26] L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, and B. Qin, "Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response," *Institute of Electrical and Electronics Engineers. Transactions on Computers*, vol. 65, no. 8, pp. 2562–2574, 2016.

[27] L. Zhang, B. Qin, Q. Wu, and F. Zhang, "Efficient many-to-one authentication with certificateless aggregate signatures," *Computer Networks*, vol. 54, no. 14, pp. 2482–2491, 2010.

[28] F. Zhang, L. Shen, and G. Wu, "Notes on the security of certificateless aggregate signature schemes," *Information Sciences*, vol. 287, pp. 32–37, 2014.

[29] H. Tu, D. He, and B. Huang, "Reattack of a certificateless aggregate signature scheme with constant pairing computations," *The Scientific World Journal*, vol. 2014, Article ID 343715, 10 pages, 2014.

[30] H. Xiong, Z. Guan, Z. Chen, and F. Li, "An efficient certificateless aggregate signature with constant pairing computations," *Information Sciences*, vol. 219, pp. 225–235, 2013.

[31] L. Cheng, Q. Wen, Z. Jin, H. Zhang, and L. Zhou, "Cryptanalysis and improvement of a certificateless aggregate signature scheme," *Information Sciences*, vol. 295, pp. 337–346, 2015.

[32] D. He, M. Tian, and J. Chen, "Insecurity of an efficient certificateless aggregate signature with constant pairing computations," *Information Sciences*, vol. 268, pp. 458–462, 2014.

[33] Y. Wen, J. Ma, and H. Huang, "An aggregate signature scheme with specified verifier," *Journal of Electronics*, vol. 20, no. 2, pp. 333–336, 2011.

[34] G. Hartung, B. Kaidel, A. Koch, J. Koch, and A. Rupp, "Fault-tolerant aggregate signatures," in *Public-Key Cryptography–PKC 2016*, vol. 9614, pp. 331–356, Springer, 2016.

[35] D. He, S. Zeadally, and L. Wu, "Certificateless public auditing scheme for cloud-assisted wireless body area networks," *IEEE Systems Journal*, no. 99, pp. 1–10, 2015.

[36] L. Shen, J. Ma, X. Liu, and M. Miao, "A provably secure aggregate signature scheme for healthcare wireless sensor networks," *Journal of Medical Systems*, vol. 40, no. 11, article no. 244, 2016.

[37] M. Zhang, Y. Zhang, Y. Jiang, and J. Shen, "Obfuscating EVES algorithm and its application in fair electronic transactions in public clouds," *IEEE Systems Journal*, pp. 1–9, 2019.

[38] Y. Liu and Q. Zhao, "E-voting scheme using secret sharing and K-anonymity," *World Wide Web*, pp. 1–11, 2018.

[39] J. G. Miller, "Culture and the development of everyday social explanation," *Journal of Personality and Social Psychology*, vol. 46, no. 5, pp. 961–978, 1984.

[40] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.

[41] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, 2015.

[42] Y. Xie, X. Li, S. Zhang, and Y. Li, "iclas: an improved certificateless aggregate signature scheme for healthcare wireless sensor networks," *IEEE Access*, vol. 7, pp. 15170–15182, 2019.

[43] D. He and D. Wang, "Robust biometrics-based authentication scheme for multiserver environment," *IEEE Systems Journal*, vol. 9, no. 3, pp. 816–823, 2015.

[44] Y. Liu, Y. Wang, X. Wang, Z. Xia, and J. Xu, "Privacy-preserving raw data collection without a trusted authority for IoT," *Computer Networks*, vol. 148, pp. 340–348, 2019.

[45] D. Pointcheval and J. Stern, "Security proofs for signature schemes," in *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques*, vol. 1070 of *Lecture Notes in Computer Science*, pp. 387–398, Springer, Saragossa, Spain, 1996.

[46] L. Wu, Y. Zhang, L. Li, and J. Shen, "Efficient and anonymous authentication scheme for wireless body area networks," *Journal of Medical Systems*, vol. 40, no. 6, article no. 134, 2016.