IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 20, 2019, accepted October 15, 2019, date of publication October 18, 2019, date of current version October 30, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2948207

Secure Authentication and Group Key Distribution Scheme for WBANs Based on Smartphone ECG Sensor

HAOWEN TAN AND ILYONG CHUNG
Department of Computer Engineering, Chosun University, Gwangju 61452, South Korea

Corresponding author: Ilyong Chung (iyc@chosun.ac.kr)

This work was supported in part by the Korean Government through the National Research Foundation of Korea (NRF) under Grant NRF-2017R1D1A3B03034005.

ABSTRACT As one of the crucial components in the emerging internet of things (IoT), wireless body area networks (WBANs) is capable of monitoring vital physiological and behavioral information of users through wearable sensors, offering a new paradigm for the next-generation healthcare systems. However, due to the inherent open wireless communicating characteristics, security and privacy issues for WBANs communication remain unsolved. Note that the deployed WBANs sensors are resource-restrained entities, which restricts its wide applications in medical environment. In this case, effective authentication scheme with efficient group key management strategy is of great significance. Moreover, with comparatively large computation ability and storage capacity, smartphone is able to perform as the vital data processing gateway for WBANs, especially in the upcoming 5G network implementation with superior transmission quality and speed. Furthermore, the WBAN sensors are responsible for continuous physiological monitoring, where the acquired biometric features could be adopted to the authentication process. For the above consideration, a secure certificateless biometric authentication and group key management for WBAN scenarios is proposed in this paper. In our design, user's smartphone takes the role of personal controller (PC) in traditional WBANs structure. The representative features of the gathered electrocardiogram (ECG) records are applied as the distinctive biometric parameter during authentication procedure. Hence efficient authentication towards participating sensors is enabled. Subsequently, fast group key management among all validated sensors is presented, where small modification is required for dynamic key updating mechanism in sensor side. Security analysis indicates that the proposed protocol can achieve desired security properties and provide resistance to various attacks. Performance analysis demonstrates that the proposed protocol is efficient compared with the state-of-the-art WBAN authentication schemes.

INDEX TERMS Wireless body area networks (WBANs), security, certificateless authentication, group key management, electrocardiogram.

I. INTRODUCTION

Wireless body area networks (WBANs) are considered as the fundamental infrastructure for future IoT-based healthcare system. In recent year, rapid developments of wireless communicating and sensor manufacturing techniques have accelerated the explosive popularization of WBANs applications and services [1]. WBANs facilitate real-time and reliable healthcare monitoring for certain users. In medical field, WBAN can be utilized to continuously monitor patients' health status and seamlessly transmit physiology information to medical institutions such as hospitals, community clinics, and emergency centers [2], [3]. In this case, the physicians could conduct remote diagnostics for patients and then provide timely medical assistance. Additionally, early warnings and precautionary measurements for certain diseases are achievable [4]. Nowadays, advanced communicating and data processing strategies, including the promising 5G networks and cloud computing techniques, have been dedicated to heterogeneous IoT environment, where WBANs

The associate editor coordinating the review of this manuscript and approving it for publication was Daniel Benevides Da Costa.

is able to conduct high-speed and stable data exchange with centralized server, offering new prospects for smart home establishment [5].

With the purpose of satisfying different requirements of diverse practical occasions, architecture of WBANs varies a lot. Generally, a typical WBAN designed is composed of healthcare center (HC), personal controller (PC) and multiple wireless medical sensors implanted inside or attached on a patient's body. These sensors are capable of conducting vital biomedical information acquisition from different aspects [6], [7]. Hence adequate physiological personal data involving heartbeat, body temperature, blood pressure can be respectively measured by sensors with dissimilar functions. Subsequently, the gathered personal physical information is transmitted and processed in HC side. Thus, unique record on user's health status is generated. Based on this, in-time medical services could be delivered to large numbers of patients simultaneously. It is worth noting that HC is considered as the secure data center and valid entity in charge of vital key information distribution [8], [9]. The confidential keying information for all the participating sensors and PCs are assumed to be securely stored in HC side all the time. The personal controller (PC) is the portable device for aggregating sensor data from individuals. Sensitive biomedical data is then delivered to remote server through PC. WBAN sensors, including implantable sensors and wearable sensors, are low-power wireless devices suffering from restriction on computation, communication, power and storage [10], [11]. Particularly, for implantable sensors, it is impractical to frequently recharge or change the built-in battery. On the other hand, an increased computation and transmission load in the sensors side will dissipate more power into heat and eventually do harm to human organs [12], [13]. As a result, low-cost operations are preferred for WBAN sensors [14].

In practical WBANs scenarios, the frequent data exchange between sensors and PC are conducted in open wireless environment, where the transmitted vital biometric data is vulnerable to various security attacks and privacy risks, especially in the WBAN occasions involving large numbers of participating devices [15]. In this case, advanced security strategies and privacy preservation techniques are vital for generalized WBAN [16]. That is, effective authentication mechanism between wireless entities is mandatory to provide preliminary protection for WBAN interaction [17]. Accordingly, various charted and uncharted secure threats such as eavesdropping, impersonation, and replaying can be prevented. After mutual authentication, efficient group key distribution and management for all the validated wearable sensors is of great significance. Therefore, the subsequent private biometric data can be securely delivered. Message broadcasting between PC and all legitimate sensors can be achieved as well.

Nowadays, among all types of wearable medical sensors, the biometric sensors for electrocardiogram (ECG) information is essential and commonly used for all WBANs scenarios [18], where ECG is defined as the real-time records of electrical activity of human heart. Note that these small electrical indicates the unique changes of cardiac muscle depolarization and repolarization during each cardiac cycle, which is also referred to as the heartbeat [19], [20]. The ECG signal is distinct for every individual, where its uniqueness result from the reflection of lots of nature factors, such as heart mass orientation, gender, ages, conductivity, behaviors and motions. The distinctiveness of ECG among individuals provides inspiration for biometric authentication design based on the acquired ECG features.

As a matter of fact, lots of researches on biometric techniques for security enhancement of WBANs have been presented, due to it superiority compared with traditional key-based authentication strategies [21]. The uniqueness of human body physiological characteristics enables studies on different aspects [22], [23]. For example, fingerprint is one of the most popular biometric technique and has been widely applied for many years. However, due to the fact that human fingerprint is constant and easily revealed, authentication based on fingerprint suffers from severe issues [24]. Note that fingerprint could be captured and impersonated from almost all objects we have touched [25]. In this case, unlike password set by user him/herself, it is not possible to modify or update the current fingerprint, resulting in inherent vulnerability. Differently, electrocardiogram (ECG) are the concealed private biometric features that can only be measured with particular sensors [26]. Moreover, ECG is able to provide dynamic synchronization seamlessly [27]. The above two major advantages enable ECG-based biometric authentication in WBAN environment. Since the ECG signals could be acquired by WBAN sensors with small effort, extra modification on hardware is not necessary. The proposed scheme in this paper is then constructed with ECG features as distinctive keying information.

Currently, rapid advancement of the upcoming 5G networks brings new perspectives for WBAN system [28], [29]. High data rate, low latency and less energy consumption can be achieved while using 5G, bringing telecommunication sector to a great level. In this case, the smartphones with 5G connection have wider usages in many aspects [30]. The smartphone could play the role of personal controller (PC) in WBAN system, due to its remarkable superiorities in communication and data processing. In this assumption, massive biometric data can be aggregated and stored in smartphone storage [31]. With relatively sufficient caching space, battery power, and computation ability, smartphones could meet practical requirements for WBANs. Hence the WBANs structure with smartphone as PC is applied in our scheme. Moreover, the modern smartphones are equipped with built-in sensors such as accelerometer, gyroscope, magnetometer and ECG sensor, where biometric parameters including ECG signal can be acquired in smartphone side. Hence it is convenient to adopt ECG features to biometric authentication in WBAN scenarios. To the best of our knowledge, lots of researches on ECG authentication design have been presented, while the studies are not applicable for mobile environment including WBANs [32].

In order to address the above issues, in this paper we propose a secure certificateless biometric authentication scheme for WBANs scenarios. In our design, certificateless technique is utilized so as to address key escrow issues from identity-based encryption [16], [33]. That is, two partial secret keys for each sensor are generated independently. Hence impersonating and forgery attacks towards certain entity is prevented [34]. Moreover, the representative electrocardiogram features are applied as the distinctive biometric parameter during authentication procedure. Hence efficient continuous authentication towards participating sensors is enabled. Subsequently, effective group key management method among all validated sensors is illustrated, where only small computation is required for dynamic key updating mechanism in sensor side. The revoked sensors cannot correctly decrypt the updated group key even with the previous assigned information [35], [36]. To the best of our knowledge, the ECG signal is properly combined with novel certificateless strategies for resource-limited WBANs sensors for the first time. Security and performance analysis prove that the proposed protocol can achieve desired security properties and is efficient in WBAN authentication scenarios.

A. OUR RESEARCH CONTRIBUTIONS

In this paper, we developed a secure certificateless biometric authentication and group key management for WBAN scenarios. Our nontrivial efforts can be briefly summarized as follows:

(1) **Secure and efficient certificateless authentication scheme without pairing:** In our design, certificateless cryptography is deployed to provide enhanced security properties. Initially, HC and sensor itself generate the partial private key respectively so as to address the key escrow problem of identity-based encryption. Hence non-repudiation characteristic is provided. Moreover, conditional privacy-preserving authentication (CPPA) is deployed. The user anonymity for all participating entities is provided through the entire authentication session, preventing illegal tracing towards particular sensors. Additionally, it is worth noting that the computation overhead of bilinear pairing calculation is three times that of the regular point multiplication calculation. Therefore, pairing technique is not adopted in our scheme during the entire process, enabling lightweight authenticating design for resource-restrained wireless sensors in WBANs.

(2) **Efficient Group key distribution with dynamic updating mechanism:** After successful validation, the unique group key is delivered to all legitimate sensors with the purpose of constructing secure communication channel among WBANs devices. In our scheme, the distributed group key is safely delivered through one broadcasting operation, which drastically reduce the communication cost compared with conventional one-to-one key distribution. Note that only the authentic sensors have the capability of correctly deriving the valid group key. The group key updating method only require small modification in smartphone, while the decrypting information in sensors side remains constant as soon as the sensors stay validated. In this case, fast revocation process is enabled without extensive computation for the remaining devices.

(3) **Biometric authentication strategy employing ECG features for modified WBAN structure:** In the modified WBAN structure, the acquired electrocardiogram signal from ECG sensors and smartphone is processed and utilized as the biometric parameter during the authentication process. To the best of our knowledge, we are the first to properly combine the ECG signal with novel certificateless authentication strategies for resource-limited WBANs.

The remainder of this paper is organized as follows. Section II briefly introduced the related research achievements. Section III illustrated some necessary preliminary works and the designed system model for the reader to obtain a better understanding of the topic. Section IV presents the proposed secure certificateless biometric authentication scheme in detail. Section V demonstrates the security analysis. Section VI displays the performance analysis. The conclusion is drawn in Section VII.

II. RELATED WORKS

In recent years, lots of research achievements have been made emphasizing on secure authentication for wireless body area network. Initially, traditional public key cryptography (TPKC) techniques are adopted to wireless mobile environment [37], which result in large computation burden for resource-constrained mobile devices. Subsequently, the designs based on elliptic curve cryptography (ECC) have been proposed, which provide same security with smaller key size compared with TPKC-based schemes [5], [35]. Meanwhile, various authentication and key management mechanisms have been developed [34], [38] under the identity-based key cryptography (ID-PKC), which was first proposed by Shamir [39]. In ID-PKC, the corresponding public key is generated by the key generation center (KGC) employing the public information such as e-mail address, social number, which drastically reduces the computation cost for both encryption and decryption process.

However, ID-PKC schemes suffer from key escrow problem since the KGC manages all users' private keys. Consequently, the concept of certificateless public key cryptography (CL-PKC) is introduced [40]. So far lots of certificateless authentication schemes have been proposed. In 2014, Liu *et al.* [11] developed a security enhanced CL-PKC protocol for WBAN scenarios. Xiong [1] proved that protocols of [11] cannot provide forward security and scalability. The improved scalable and anonymous remote authentication protocol is presented as well. Similarly, the certificateless encryption and signature scheme is proposed in [10], where efficient and scalable revocation mechanism is adopted.

Thereafter, ciphertext-policy attribute-based encryption is deployed in [15] so as to ensure the data confidentiality. Li and Hong [31] designed an efficient certificateless signcryption scheme with the corresponding access control method. Moreover, emphasizing on preservation of the user identity, an anonymous authentication scheme is built [6], which overcomes the security vulnerability in [11] and meets more security requirements. In 2018, Ji *et al.* proposed an efficient certificateless conditional privacy-preserving authentication scheme for WBAN in big data environment [41]. The proposed scheme provides batch authentication towards multiple clients, which significantly reduces the computational overhead of the service provider. Typical security properties including user anonymity, unlinkability, mutual authentication, traceability, and forward secrecy are enabled in the proposed scheme. Currently, several WBAN authentication protocols have been proposed [9], [14].

Biometrics is defined as the metrics corresponded to human characteristics. Authentication on biometrics is used as the unique way of identification and access control, where the applied biometrics factors are the distinctive, measurable parameters representing the physiological and behavioral uniqueness of individuals. Nowadays, the studies on biometric authentication has gradually attracted lots of attention from academia [42], where the adaption of various biometric features establishes advanced directive for mobile authentication. In [21], the mouse dynamic biometrics during user interaction with graphical user interface is deployed for static authentication. The captured mouse gestures are analyzed through learning vector quantization (LVQ) neural network for classification. Subsequently, Sheng *et al.* designed a biometric key generation method with semi-supervised data clustering technique [32]. Hence, multiple clusters are arranged so as to produce long-time constant keys. User variations are modeled for consistent and discriminative characteristics recovery during key generation process. Thereafter, emphasizing on continuous authentication of smartphone users, the behavioral feature set HMOG is adopted, which is capable of unobtrusively capture the user's gesture to hold the smartphone [24]. Recently, Chatterjee *et al.* presented the enhanced biometric-based authentication scheme for multi-server environment. The Chebyshev chaotic map along with the biometric authentication design is applied. Note that symmetric encryption technique with cryptographic hash function is utilized for security properties [26].

As one of the crucial physiological characteristics, electrocardiogram (ECG) has the advantage of continuously measuring the biological functions of human body. Biometric authentication strategies applying ECG as the distinctive factor have been fully investigated. Choi *et al.* proposed the biometric authentication method with the acquired noisy ECG from mobile sensors [43]. The gathered ECG signals are processed with the cascading bandpass filter for noise cancellation. Similarly, another ECG authentication algorithm for mobile devices is proposed as well [27]. In 2019, Chu *et al.* designed the ECG authentication scheme employing parallel multi-scale one-dimensional residual network [25], where three convolutional kernels with diverse kernel sizes are utilized. Additionally, center and margin loss are applied during the training process, resulting in better generalization of the extracted ECG features. Meanwhile, Hammad *et al.* presented the multimodal biometric authentication system using convolution neural network (CNN) and Q-Gaussian multi support vector machine (QG-MSVM) [28]. The feature level fusion and decision level fusion are constructed. Security of the authentication system is enhanced with the cancelable biometric techniques for templates preservation. Subsequently, with the purpose of addressing the irrevocability issue in ECG biometrics, Kim *et al.* proposed cancelable ECG biometric authentication scheme, where the generalized likelihood ratio test (GLRT) is adopted [18]. Accordingly, the proposed permutation-based revocation design for compressive sensing domain is resistant to record multiplicity attack.

Particularly, typical wireless body area networks are composed of ECG sensors deployed for medical monitoring. Therefore, additional hardware design is not required for practical implementation of ECG-based biometric authentication designs. In 2012, Zhang *et al.* presented the key agreement method with ECG cryptography for WBANs scenarios [19]. In the design, neighboring sensors are capable of establishing the common session key according to ECG signals. The previous key distribution process is not required in this way. Thereafter, emphasizing on anomalies detection in WBAN healthcare system, a centralized continuous change identification mechanism is presented [44]. Note that the simplified Markov model is applied for ECG data processing. Li *et al.* designed a physical layer-based group cooperation scheme for symmetric key generation in WBANs [30]. In the proposed scheme, physical channel information is analyzed, where the received signal strength indicator (RSSI) is used for efficient key generation. Similarly, an ECG multiple fiducial-points based random binary sequence generation (MFBSG) method is presented by Zhang *et al.* [2]. Note that the discrete wavelet transforms technique is deployed for arrival time detection towards certain fiducial points. Consequently, random binary sequences (BSes) can be generated for secure WBANs transmission. The brief summary of the discussed authentication schemes is presented in Table 1.

TABLE 1. Summary of authentication schemes.

Categories	Schemes
TPKC	[37]
ID-PKC	[5], [34], [38]
CL-PKC	[35], [11], [1], [31], [10], [6], [41], [14], [9]
Biometric	[21], [32], [24], [26]
ECG-Based	[43], [27], [25], [28], [19]

III. MODEL DEFINITION AND PRELIMINARIES

With the purpose of facilitating the reader's understanding of our design, some necessary preliminaries are described,

TABLE 2. Notations.

Notation	Description
HC	Healthcare Center
ID_p^o, ID_i^o	Constant identity of smartphone and sensor
P	Generator of $\mathbb{G}$
pw_i	Device password
a	Self-generated secret key
ID_p, ID_i, ID_{ecg}	Temporary identity of smartphone and sensors
TS_1, TS_2, TS_3, TS_4	Timestamps
r_{ecg}, r_i	Partial secret key of sensors
$H_1, H_2, H_3, H_4, H_5, H_6$	Secure Hash Functions
H_1, H_2, H_3, H_4	Secure Hash Function
R_i	Public key of sensor
$\Gamma_p^1, \Gamma_{ecg}^1, \Gamma_p^2, \Gamma_{ecg}^2$	ECG biometrics
φ_i	Decrypting key for sensor
γ	Group key
$\{\delta_0, \delta_1, ..., \delta_{m-1}\}$	Coefficients set of Coefficients set of $\kappa(x)$
$Cert_p^1, Cert_i, Cert_{gk}$	Certificates for verification

including the definition of elliptic curve cryptography (ECC), Hash function. Subsequently, the corresponding notations, system model, and network assumptions are respectively illustrated.

A. ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

Let $p > 3$ be a prime, $\mathbb{F}_p$ be the finite field of order p. $a, b \in \mathbb{F}_p$ satisfy $4a^3 + 27b^2 \neq 0$. An elliptic curve $E_p(a, b)$ over the finite field $\mathbb{F}_p$ is defined with the following equation:

$$y^2 = x^3 + ax + b,$$

where $(x, y) \in \mathbb{F}_p$. The addition operation on the curve is called point doubling when the two points are identical. Otherwise, it is called point addition. All the points on the curve, as well as the point at infinity ∞ form an additive Abelian group $E(\mathbb{F}_p)$. Note that $\infty = (-\infty)$ serves as the identity element.

In general, the security of ECC depends on the difficulties of the following problems [45]:

Definition 1 (Elliptic Curve Discrete Logarithm Problem): Given two points P and Q over $E_p(a, b)$, the ECDLP problem is to determine the integer $s \in \mathbb{F}_p$ such that $sP = Q$.

Definition 2 (Computational Diffie-Hellman Problem): Given three points P, sP and tP over $E_p(a, b)$ with $s, t \in \mathbb{F}_p$, the CDHP problem is to calculate the point stP over $E_p(a, b)$.

B. HASH FUNCTION

A one-way hash function is considered to be secure if the following properties can be achieved [46]:

1) Input a message x of arbitrary length, it is easy to compute a message digest of a fixed length output $h(x)$.
2) Given y, it is difficult to compute $x = h^{-1}(y)$.
3) Given x, it is computationally infeasible to find $x' \neq x$ such that $h(x') = h(x)$ holds.

C. NOTATIONS

As shown in Table 2, the notations used in our scheme are listed, respectively with the corresponding description.

D. SYSTEM MODEL

In our assumption, the three essential components which comprises the entire WBANs system are generally defined as the healthcare center (HC), the biological sensors, as well as the personal controller. The generalized infrastructure of the WBANs system is displayed in Fig. 1. The corresponding description of the three components are respectively illustrated below.

The healthcare center (HC) is defined as the medical service provider as well the trustworthy key management center. In practical scenarios, various healthcare institutions such as hospitals and emergency centers could play the role of HC. The significant personal data are aggregated and finally transmitted to HC, which reflects the patient's real time physiological status. In this way, seamless monitoring towards targeted user is enabled. Accordingly, the corresponding medical treatment for specific patients can be remotely executed if necessary, providing advanced security level for life rescue and first aid. Moreover, HC is the secure key generation center (KGC) in charge of crucial secret key information generation and distribution. The initial keying information for all the participating WBANs entities are organized and safely stored in HC side during the entire operation time. Note that in our design, HC is assumed to be resistant to all kinds of attacks and remains authentic and reliable anytime. Particularly, the emerging cloud computing techniques enable massive cloud storage and strengthened computation capacity, which could be applied to WBANs scenarios. That is, user's vital private data and key information are stored and processed in distributed cloud servers, bring beneficial effect for resource-constrained WBANs scenarios.

The personal controller is assumed to be the portable device with the functionality of biomedical information aggregating and communication with HC. That is, the significant physiological data collected from multiple WBANs sensors are delivered to personal controller. Note that each user in WBANs is attached with certain personal controller. Hence, all variety of personal data involving individual user are aggregated in one personal controller. Commonly, the personal controller is defined as the professional healthcare equipment with specific medical purpose. Nevertheless, as mentioned above, in our system model the smartphones perform as the personal controller in WBANs system. Hence, with sufficient data processing ability and adequate storage compared with resource-constrained traditional WBANs medical devices, the convergence between WBANs scenarios and cellular devices creates novel paradigm for universal IoT network involving heterogeneous devices. Nowadays, rapid development of the upcoming 5G networks enables high data rate, low latency and less energy consumption for emerging smartphones, which offers remarkable advantages for smartphone in biometric data aggregation and analysis. Furthermore, the smartphones are usually equipped with multiple built-in sensors for behavioral and physiological measurement, such as gyroscope, accelerometer, ECG sensor, and temperature sensor. User's biometric data including

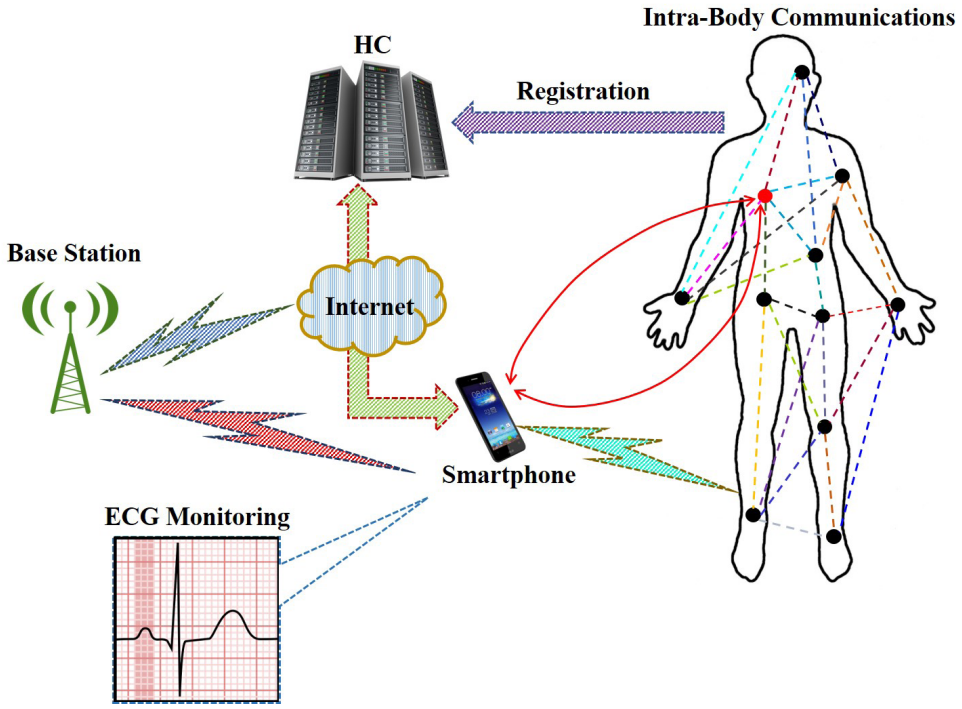


FIGURE 1. System Model.

ECG signal can be naturally acquired by smartphone with small effort. Hence, it is convenient to adopt ECG features to biometric authentication in WBAN scenarios. The WBANs system model with smartphone as personal controller is applied in our authentication scheme.

The sensors are assumed to be the wireless biomedical devices either implanted inside or attached on the user's body. These sensors have limited computation ability and restricted battery capacity. The sensors are responsible for real-time measurement to various physiology metrics towards certain user. Typically, multiple sensors, which are responsible for respectively monitoring different biometrics, are effective within human body range. All the gathered significant personal data are delivered to personal controller through open wireless connection. Note that all the gathered physiological sensor data are time-related parameters. Hence the time synchronization between all sensors is mandatory. In our assumption, the ECG sensor is deployed for electrocardiography signal measurement and collection. Consequently, the biometric authentication between ECG sensor and the deployed smartphone is enabled. Note that the validated interaction between ECG sensor plays an important role in our authentication scheme, where the crucial biometric information is assumed to be transmitted from the ECG sensor to the remaining WBANs entities. At this point, the heterogeneous authentication scheme, along with the universal group key distribution method can be achieved accordingly.

E. NETWORKS ASSUMPTION

As illustrated in Fig. 1, multiple communicating types are activated in the system model. The continuous private data exchange involving all legitimate WBANs sensors is conducted as the intra-body communication. Note that the ECG sensor is included in our design for ECG signal acquisition. As mentioned above, user's smartphone is utilized as the personal controller in our scheme. Therefore, the communication between smartphone and HC can be achieved through cellular networks or direct internet connection. Practically, the interaction between smartphone and HC can be preserved with adequate security mechanisms. However, the intra-body communications are performed in open wireless environment, resulting in vulnerability to various security risks and malicious attacks. For this consideration, secure intra-body data transmission is provided in this paper, while the communication channel between smartphone and HC is not considered.

At this point, two typical kinds of wireless communication channels are discussed in our design, including the longitudinal data processing between smartphone and sensors, as well as the vital sensor data exchange involving all participating biomedical sensors. Due to the inherent wireless characteristics, proper authentication mechanism regarding all sensors and smartphone should be presented, where the ECG feature is adopted for efficient verification. Moreover, universal communication channel among the validated sensors is indispensable. The shared group key should be distributed to all legitimate sensors for secure association. Additionally, the unique ECG sensor is performed as the intermediate device between smartphone and remaining sensors, where crucial supplementary biometric information is distributed to neighboring devices. For the above consideration, the secure ECG biometric authentication scheme is designed in this

paper, along with the corresponding group key management method.

IV. PROPOSED CERTIFICATELESS BIOMETRIC AUTHENTICATION AND GROUP KEY MANAGEMENT SCHEME

In this section, the constructed certificateless authentication scheme is described, where the ECG feature is applied as the unique synchronous factor for biometric authentication. Subsequently, the corresponding group key distribution strategy is conducted among all validated WBANs entities so as to facilitate the secure communication channel for continuous personal data exchange. For better description, the proposed mechanism can be roughly classified into four different phases including the **offline registration phase**, **ECG feature extraction phase**, **authentication phase**, and **group key distribution phase**. Accordingly, the sensor and smartphone registration, along with the nontrivial preparation for key initialization and membership management, is conducted in the offline registration phase. Note that it is mandatory for all the WBANs devices including the smartphone and sensors to register to HC first. Hence, the original private key and the designated identifier is securely assigned to each entity for subsequent authentication process. Thereafter, in the ECG feature extraction phase, ECG signal preprocessing and extracting mechanism is performed in both the smartphone and sensor side for biometric parameter generation, which can be further adopted in successive authentication design. Subsequently, the major certificateless authenticating procedure are conducted in the following authentication phase. At last, the shared group key among all validated WBANs entities is safely allocated in the final group key distribution phase. Moreover, the relevant key updating strategy is introduced with the purpose of handling the revoked or new participating sensor, where the updated group key is dynamically distributed for secure data transmission.

It is worth noting that the proposed scheme deploys the certificateless cryptography technique with resistance to key escrow issues. The adopted ECG biometric is utilized as the natural synchronous parameter during the interaction between smartphone and certain sensor. Additionally, bilinear pairing is not used so as to significantly reduce the computation overhead, which is necessary for resource-limited WBANs devices. It is worth noting that our design is presented under the scenarios with single WBANs user, where various implantable or wearable sensors are attached accordingly. Particularly, the ECG sensor is included in the system model, which performs as the specific intermediary during sensor association and key agreement. Due to the practical requirements, our scheme is presented in the scenario with single ECG sensors for better description, while the authenticating occasion with multiple ECG sensors is similar.

A. OFFLINE REGISTRATION PHASE

The offline registration phase is intended for the WBANs initialization including the essential key information arrangement, and user registration to HC. As mentioned above, it is prerequisite for all the WBANs entities to register to HC in advance. Note that HC is assumed to be validated component and the trustworthy key generation center (KGC) for the entire period. Moreover, the registration with HC is defined to be secure in the offline mode. Initially, the valid user information such as name, address, social identifier, are safely recorded in HC side. After that, the special user license ID_p^o is generated and distributed to the legitimate user. According to our design, user's smartphone plays the role of personal controller, which is strictly combined to certain user all the time. In this case, ID_p^o is one-to-one mapped to user's smartphone and remains constant the whole time. Hence, the user and his/her smartphone are considered as one entity with the assigned ID_p^o. Similarly, the WBANs sensors to be attached, whether the implantable sensors or wearable sensors, should also be registered during the offline registration process. The distinctive sensor identity ID_i^o is then randomly generated and allocated by HC. In our assumption, the number of participating sensors is denoted as n ($n > 1$), which includes one ECG sensor and $n-1$ regular sensors for other measurements. That is, $ID_i^o \in \{0,1\}^*$ and $i \in [1,n]$. Moreover, the registered sensors set up its own confidential password pw_i independently. Hence, the user personal profile containing key pair $\langle ID_i^o, pw_i \rangle_{i\in[1,n]}$ is maintained by HC. Similarly, $\langle ID_i^o, pw_i \rangle$ is kept secret in sensor side for further usage.

B. ECG FEATURE EXTRACTION PHASE

First of all, the ECG feature extraction in both smartphone and ECG sensor side is performed, where massive ECG sensor data are generated and processed. As briefly shown in Fig. 2, the sampled ECG signal involving single heartbeat is featured with three main components including the P wave, the QRS complex, as well as the T wave. In medical area, the depolarization of the atria and ventricles are respectively represented by P wave and QRS complexes, while the repolarization of the ventricles is denoted as T wave. In our design, both time-related and amplitude-based features are analyzed. The seven fiducial points of the ECG signal denoted as $\{LP, P, Q, R, S, T, TP\}$, as well as the eight essential features are illustrated in Fig. 2. Note that he six time-related features are defined as $\{RLP, RP, RQ, RS, RT, RTP\}$, which represent the intervals from R Peak to the remaining six fiducial points including LP Valley, P Peak, and Q Valley, S Valley, T Peak, TP Valley. Meanwhile, the two amplitude-based features $\{RSA, RQA\}$ are calculated as the amplitude from R Peak to S Valley and Q Valley.

At this point, the preprocessing towards the acquired massive ECG signal is conducted, which includes denoising on the raw biological data, as well as the QRS complex delineation and P and T waves delineation. The denoising operation is performed with the morphological filtering method [47]. Different structural elements are applied for various characteristics of ECG signal. The denoised signal can be derived after the removal of

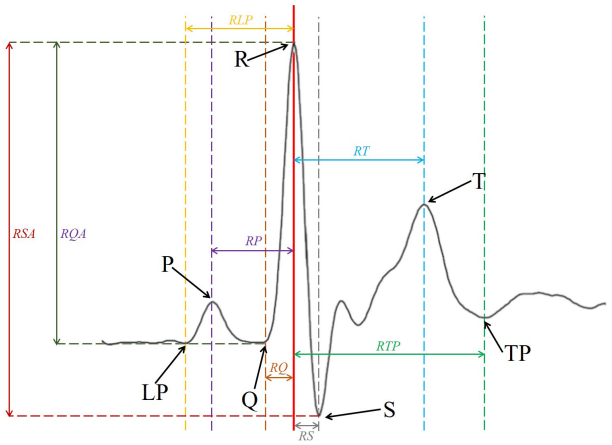


FIGURE 2. Sample of ECG signal with single heartbeat.

the residual. Thereafter, the moving-window integrating is operated for signal smoothing. Subsequently, the fiducial points detection method based on differentiation is adopted so as to distinguish the *QRS* complex from other ECG waves. Based on this, the detection towards *P* and *T* waves is conducted. Local distance transforming is utilized to derive the onset and offset of the *P* wave. Considering the fact that the ECG extraction is for mobile device, totally eight features can be derived, which includes the aforementioned time-related and amplitude-based features $\{RLP, RP, RQ, RS, RT, RTP, RSA, RQA\}$. Consequently, the ECG template is derived as $\Gamma = [\Omega_1, \Omega_2, \Omega_3, \Omega_4, \Omega_5, \Omega_6]$, where $\{\Omega_i\}_{i\in[1,6]}$ is denoted as the biometric of the extracted ECG features, which can be generated by both smartphone and the ECG sensor side for biometric authentication.

C. AUTHENTICATION PHASE

In this phase, the detailed authentication process is described step by step. Let P be the generator of a cyclic additive group $\mathbb{G}$, where $\mathbb{Z}_{\mathcal{P}}^*$ is defined as a nonnegative integer set less than a large prime number $\mathcal{P}$. The secure cryptographic hash function H_1, H_2, H_3, H_4 are respectively defined as $H_1 : \{0,1\}^* \times \mathbb{G} \rightarrow \mathbb{Z}_{\mathcal{P}}^*$, $H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_{\mathcal{P}}^*$ and $H_3 : \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \times \mathbb{G} \rightarrow \mathbb{Z}_{\mathcal{P}}^*, H_4 : \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \times \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{Z}_{\mathcal{P}}^*$.

At first, the registered smartphone with ID_p^o regarding certain user randomly generates its secret key denoted as $a \in \mathbb{Z}_{\mathcal{P}}^*$ and computes the partial secret

$$\Theta_p = aP. \tag{1}$$

Hence the corresponding temporary identity is calculated as

$$ID_p = H_1(ID_p^o || \Theta_p), \tag{2}$$

where the original static identity ID_p^o is kept secret all the time.

As mentioned above, the current ECG biometric Γ_p^1 can be derived by smartphone through analyzing the acquired ECG signal. In certain time point, the related Ψ_p^1 and the certificate $Cert_p^1$ are calculated as

$$\begin{cases} \Psi_p^1 = aH_2(\Gamma_p^1)P \\ Cert_p^1 = H_3(\Gamma_p^1 || TS_1 || ID_p || \Theta_p), \end{cases} \tag{3}$$

where TS_1 is defined as the generated time stamp when the biometric Γ_p^1 is derived.

It is assumed that totally n registered sensors with the original identity $\{ID_1^o, ID_2^o, \ldots, ID_n^o\}$ are to be authenticated, which includes one ECG sensor according to aforementioned design. For better description, the identity of the ECG sensor is defined as ID_1^o. At this point, the universal requesting message is broadcasting from smartphone to all the n participating WBAN sensors, which is denoted as

$$\left\langle Request, TS_1, ID_p, \Psi_p^1, Cert_p^1 \right\rangle. \tag{4}$$

Upon receipt of the requesting message, the specific ECG sensor checks the freshness of the received timestamp TS_1 and gathers the biometric parameter Γ_{ecg}^1 according to its own measurement. Hence the partial secret Θ_p can be derived from Ψ_p^1 as

$$\Psi_p^1 \left[H_2(\Gamma_{ecg}^1)\right]^{-1} = \frac{H_2(\Gamma_p^1)}{H_2(\Gamma_{ecg}^1)} aP = aP. \tag{5}$$

Therefore $aP = \Theta_p$ is calculated.

In the next, the ECG sensor with identity ID_1^o checks whether the following equation holds:

$$Cert_p^1 \stackrel{?}{=} H_3(\Gamma_{ecg}^1 || TS_1 || ID_p || \Theta_p), \tag{6}$$

where the self-generated Γ_{ecg}^1, the received timestamp TS_1, the identity ID_p, along with the derived partial secret Θ_p are adopted.

If the received $Cert_p^1$ is incorrect, ECG will broadcast the resending message to all WBANs devices, the current authentication session is then terminated. Or else, the ECG sensor generates its partial secret key $r_{ecg} \in \mathbb{Z}_{\mathcal{P}}^*$ randomly and computes the temporary identity ID_{ecg} as

$$ID_{ecg} = H_1(ID_1^o || r_{ecg} P), \tag{7}$$

where ID_1^o is the constant identity assigned during registration. At this point, the partial secret Θ_p and the temporary identity ID_p are securely delivered to ECG sensor side.

Subsequently, the ECG sensor computes the necessary keying information Υ_{ecg}^2, as well as the certificate $Cert_{ecg}^2$ as

$$\begin{cases} \Upsilon_{ecg}^2 = r_{ecg} pw_1 H_2(\Gamma_{ecg}^2)P \\ Cert_{ecg}^2 = H_4(\Gamma_{ecg}^2 || TS_2 || ID_{ecg} || \Theta_p || r_{ecg} pw_1 P), \end{cases} \tag{8}$$

where pw_1 denotes the relevant password for ECG sensor, Γ_{ecg}^2 denotes the biometric related to the new timestamp TS_2. The smartphone partial secret Θ_p is applied as well. Therefore, the following message is distributed to all entities including smartphone and other sensors:

$$\left\langle TS_2, ID_{ecg}, \Theta_p, \Upsilon_{ecg}^2, Cert_{ecg}^2 \right\rangle. \tag{9}$$

Upon receiving the above message, the smartphone checks the freshness of TS_2 and derives the related biometric Γ_p^2 at this time. If the received Θ_p is valid, the following calculation is performed so as to acquire $r_{ecg}pw_1P$ of the ECG sensor:

$$\Upsilon_{ecg}^2\left[H_2(\Gamma_p^2)\right]^{-1} = r_{ecg}pw_1P. \tag{10}$$

The correctness is elaborated as:

$$\begin{aligned}&\Upsilon_{ecg}^2\left[H_2(\Gamma_p^2)\right]^{-1}\\ &\quad= r_{ecg}pw_1\frac{H_2(\Gamma_{ecg}^2)}{H_2(\Gamma_p^2)}P\\ &\quad= r_{ecg}pw_1P.\end{aligned} \tag{11}$$

Subsequently, the validity of the received $Cert_{ecg}^2$ is checked as follows:

$$Cert_{ecg}^2 \stackrel{?}{=} H_4(\Gamma_p^2||TS_2||ID_{ecg}||\Theta_p||r_{ecg}pw_1P), \tag{12}$$

where the calculated $r_{ecg}pw_1P$ is used.

In this case, the mutual authentication between smartphone and specific ECG sensor is finished, where the necessary keying value $r_{ecg}pw_1P$ is securely distributed to smartphone for subsequent group key assignment. Meanwhile, the aforementioned broadcast message in equation 4 and equation 9 are also delivered to the remaining $n-1$ normal sensors. Consequently, the value of ID_p and Θ_p are published to all entities.

As for the $n-1$ sensors with identity set $\{ID_2^o, \ldots, ID_n^o\}$, the partial secret key $r_i \in \mathbb{Z}_{\mathcal{P}}^*$ $(i \in [2, n])$ is generated independently by sensor itself. Hence, the temporary identity ID_i, as well as the related public key R_i are computed as

$$\begin{cases} ID_i = H_1(ID_i^o||r_iP) \\ R_i = r_iP. \end{cases} \tag{13}$$

Therefore, the relevant keying information for $n-1$ sensors are calculated as

$$\begin{cases} \hbar_i = H_5(ID_i||TS_3||r_i\Theta_p)pw_i + H_5(ID_p||TS_3||pw_i\Theta_p)r_i \\ \wp_i = H_6(ID_i||TS_3||R_i||r_ipw_iP) \\ Cert_i = (\wp_i\hbar_i + r_ipw_i)P, \end{cases} \tag{14}$$

where $i \in [2, n]$, and TS_3 denotes the updated timestamp. The secure cryptographic hash function H_5, H_6 are respectively defined as $H_5 : \{0,1\}^* \times \{0,1\}^* \times \mathbb{G} \rightarrow \mathbb{Z}_{\mathcal{P}}$, and $H_6 : \{0,1\}^* \times \{0,1\}^* \times \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{Z}_{\mathcal{P}}^*$.

Subsequently, the message $\langle TS_3, ID_i, R_i, \wp_i, Cert_i\rangle_{i\in[2,n]}$ is delivered to smartphone. At this point, the smartphone is able to record the identity set $\{ID_2^o, \ldots, ID_n^o\}$ of the $n-1$ sensor and then consult HC to get the stored value pw_iP respectively. In this case, the final authentication process can be conducted as

$$\begin{aligned}\wp_i \stackrel{?}{=}\ & H_6(ID_i||TS_3||R_i||Cert_i\\ & - \wp_i[H_5\ (ID_i||TS_3||aR_i)\ (pw_iP)\\ & + H_5(ID_p||TS_3||a(pw_iP))R_i]).\end{aligned} \tag{15}$$

Note that the pw_iP acquired from HC, R_i derived from sensor are used in the above verification. Accordingly, the correctness is elaborated as follows:

$$\begin{aligned}&H_6(ID_i||TS_3||R_i||Cert_i - \wp_i[H_5\ (ID_i||TS_3||aR_i)\\ &\quad\times (pw_iP) + H_5(ID_p||TS_3||a(pw_iP))R_i])\\ &= H_6(ID_i||TS_3||R_i||(\wp_i\hbar_i + r_ipw_i)P\\ &\quad - \ \wp_i[H_5\ (ID_i||TS_3||aR_i)\ (pw_iP)\\ &\quad + H_5(ID_p||TS_3||a(pw_iP))R_i])\\ &= H_6(ID_i||TS_3||R_i||(\wp_i\hbar_i + r_ipw_i)P\\ &\quad - \wp_i[H_5\ (ID_i||TS_3||ar_iP)\ (pw_iP)\\ &\quad + H_5(ID_p||TS_3||a(pw_iP))r_iP])\\ &= H_6(ID_i||TS_3||R_i||(\wp_i\hbar_i + r_ipw_i)P\\ &\quad - \wp_i[H_5\ (ID_i||TS_3||ar_iP)\ (pw_iP)\\ &\quad + H_5(ID_p||TS_3||a(pw_iP))r_iP])\\ &= H_6(ID_i||TS_3||R_i||\wp_i\hbar_iP + r_ipw_iP\\ &\quad - \wp_i[H_5\ (ID_i||TS_3||ar_iP)\ (pw_iP)\\ &\quad + H_5(ID_p||TS_3||a(pw_iP))r_iP])\\ &= H_6(ID_i||TS_3||R_i||\wp_i[H_5(ID_i||TS_3||r_i\Theta_p)pw_i\\ &\quad + H_5(ID_p||TS_3||pw_i\Theta_p)r_i]P + r_ipw_iP\\ &\quad - \wp_i[H_5\ (ID_i||TS_3||ar_iP)\ (pw_iP)\\ &\quad + H_5(ID_p||TS_3||a(pw_iP))r_iP])\\ &= H_6(ID_i||TS_3||R_i||\wp_i[H_5(ID_i||TS_3||r_i\Theta_p)pw_iP\\ &\quad + H_5(ID_p||TS_3||pw_i\Theta_p)r_iP] + r_ipw_iP\\ &\quad - \wp_i[H_5\ (ID_i||TS_3||ar_iP)\ (pw_iP)\\ &\quad + H_5(ID_p||TS_3||a(pw_iP))r_iP])\\ &= H_6(ID_i||TS_3||R_i||\wp_iH_5(ID_i||TS_3||r_i\Theta_p)pw_iP\\ &\quad + \wp_iH_5(ID_p||TS_3||pw_i\Theta_p)r_iP + r_ipw_iP\\ &\quad - \wp_i[H_5\ (ID_i||TS_3||ar_iP)\ (pw_iP)\\ &\quad + H_5(ID_p||TS_3||a(pw_iP))r_iP])\\ &= H_6(ID_i||TS_3||R_i||\wp_iH_5(ID_i||TS_3||r_i\Theta_p)pw_iP\\ &\quad + \wp_iH_5(ID_p||TS_3||pw_i\Theta_p)r_iP + r_ipw_iP\\ &\quad - \wp_iH_5\ (ID_i||TS_3||ar_iP)\ pw_iP\\ &\quad - \wp_iH_5(ID_p||TS_3||a(pw_iP))r_iP)\\ &= H_6(ID_i||TS_3||R_i||\wp_iH_5(ID_i||TS_3||r_i\Theta_p)pw_iP\\ &\quad - \wp_iH_5\ (ID_i||TS_3||r_i(aP))\ pw_iP\\ &\quad + r_ipw_iP + \wp_iH_5(ID_p||TS_3||pw_i\Theta_p)r_iP\\ &\quad - \wp_iH_5(ID_p||TS_3||pw_i(aP))r_iP)\\ &= H_6(ID_i||TS_3||R_i||[\wp_iH_5(ID_i||TS_3||r_i\Theta_p)pw_iP\\ &\quad - \wp_iH_5\left(ID_i||TS_3||r_i\Theta_p\right)pw_iP]\\ &\quad + r_ipw_iP + [\wp_iH_5(ID_p||TS_3||pw_i\Theta_p)r_iP\\ &\quad - \wp_iH_5(ID_p||TS_3||pw_i\Theta_p)r_iP])\\ &= H_6(ID_i||TS_3||R_i||r_ipw_iP)\\ &= \wp_i.\end{aligned} \tag{16}$$

If sensor passes the above verification, the value of r_ipw_iP $(i \in [2, n])$ is derived at the same time, which will be

Algorithm 1 Authentication Process

Input: $\left\langle a, ID_p^o, \Gamma_p^1, TS_1 \right\rangle$
Smartphone:
Compute $\left\langle \Theta_p, ID_p, \Psi_p^1, Cert_p^1 \right\rangle$
for $i = 1$ **to** n **do**
  Forward $\left\langle Request, TS_1, ID_p, \Psi_p^1, Cert_p^1 \right\rangle$ **to** Sensor i
end for
(1) ECG Sensor:
Derive Θ_p **from** Ψ_p^1
if $Cert_p^1$ is valid **then**
  Generate $r_{ecg} \in \mathbb{Z}_{\mathcal{P}}^*$
  Compute $\left\langle ID_{ecg}, \Upsilon_{ecg}^2, Cert_{ecg}^2 \right\rangle$
  for $i = 2$ **to** n **do**
    Forward $\left\langle TS_2, ID_{ecg}, \Theta_p, \Upsilon_{ecg}^2, Cert_{ecg}^2 \right\rangle$ **to** Sensor i
  end for
else
  Break
end if
for $i = 2$ **to** n **do**
  (2) Sensor i**:**
  Generate $r_i \in \mathbb{Z}_{\mathcal{P}}^*$
  Compute $\langle ID_i, R_i, \hbar_i, \wp_i, Cert_i \rangle$
end for
Smartphone:
Verify $Cert_{ecg}^2$
Output: $r_{ecg} pw_1 P$
for $i = 2$ **to** n **do**
  if $\wp_i$ is valid **then**
    Output: $r_i pw_i P$
  else
    Break
  end if
end for

adopted in the group key distribution phase. As mentioned above, $r_{ecg} pw_1 P$ for ECG sensor is stored in smartphone as well. In this case, all n sensors have successfully passed the authentication process, which is summarized in Algorithm 1. The corresponding keying messages are recorded for the following group key distribution.

D. GROUP KEY DISTRIBUTION PHASE

In our design, frequent biomedical data exchange channel is enabled. Hence, a commonly shared group key should be generated and distributed after the aforementioned authentication phase. At this point, the assigned group key should be successfully delivered to all the legitimate sensors, while the outsiders cannot derive the essential group key correctly. Note that in our design the group key is delivered through one broadcasting to all devices, while one-to-one delivery is not necessary. Accordingly, assuming m sensors have successfully passed the above authentication, the smartphone calculates the relevant decrypting key φ_i as

$$\varphi_i = H_1(ID_i || r_i pw_i P), \tag{17}$$

where $i \in [1, m]$. In this case, φ_i is corresponded to the certain sensor with identity ID_i. With the calculated $\{\varphi_1, \ldots, \varphi_m\}$, smartphone randomly selects the group key $\gamma \in \mathbb{Z}_{\mathcal{P}}^*$ and constructs the following function:

$$\kappa(x) = (x - \varphi_1) \ldots (x - \varphi_m) + \gamma = \prod_{i=1}^{m} (x - \varphi_i) + \gamma, \tag{18}$$

which can then be extracted as

$$\begin{aligned} \kappa(x) &= \delta_0 + \delta_1 x + \ldots + \delta_{m-2} x^{m-2} + \delta_{m-1} x^{m-1} + x^m \\ &= \sum_{i=1}^{m-1} \delta_i x^i + \delta_0 + x^m, \end{aligned} \tag{19}$$

where the related coefficients set of $\kappa(x)$ formula can be illustrated as $\{\delta_0, \delta_1, \ldots, \delta_{m-1}\}$. It is obvious that for $\forall j \in [1, m]$, $\kappa(\varphi_j) = (\varphi_j - \varphi_j) \prod_{i \in [1,m] \& i \neq j} (x - \varphi_i) + \gamma = \gamma$ holds. Subsequently, the following computation is conducted as

$$Cert_{gk} = h(ID_p, TS_4, \delta_0, \ldots, \delta_{m-1}, \gamma), \tag{20}$$

where TS_4 denotes the current timestamp, h denotes the secure cryptographic hash function. The final keying packet $\left\langle ID_p, TS_4, Cert_{gk}, \delta_0, \ldots, \delta_{m-1} \right\rangle$ is then broadcast to all.

Upon receiving the packet, sensor checks the freshness of the received TS_4, as well as the correctness of $Cert_{gk}$. Thereafter, the sensors are able to reconstruct the function $\kappa(x)$ according to the derived coefficient set $\{\delta_0, \delta_1, \ldots, \delta_{m-1}\}$. In this case, each sensor calculates its own decrypting key as $\varphi_i = H_1(ID_i || r_i pw_i P)$ and adopts φ_i into

$$\kappa(\varphi_i) = \gamma, \tag{21}$$

where the distributed group key γ is derived in sensor side. It is worth noting that the formula κ can be built with the delivered coefficient set $\{\delta_0, \delta_1, \ldots, \delta_{m-1}\}$. However, only the legitimate sensors can acquire the correct group key γ with the self-computed decrypting key φ_i. As shown in Algorithm 2, the group key γ is successfully distributed.

E. GROUP KEY UPDATING STRATEGY

In practical WBANs communication scenarios, the distributed group key should be timely updated as soon as the sensor revocation or new sensor association happens. For this consideration, the efficient group key updating strategy is mandatory for WBANs authentication scheme. Note that in our design, the occasions for both sensor revoking and new sensor associating are respectively discussed. Meanwhile, comparatively small computation cost on the smartphone side is required for updating process. Furthermore, the remaining legitimate sensors can easily decrypt the new group key using the stored keying information φ_i. The updating information is delivered through one broadcast operation.

Algorithm 2 Group Key Distribution Process

Input: $\langle ID_i, r_i pw_i P\rangle$ $(i \in \{1, \ldots, m\})$
Smartphone:
for i = 1 **to** m **do**
  Compute $\varphi_i = H_1(ID_i || r_i pw_i P)$
end for
Extract $\{\delta_0, \delta_1, \ldots, \delta_{m-1}\}$
Generate $\gamma \in \mathbb{Z}_{\mathcal{P}}^*$
Compute $Cert_{gk}$
for $i = 1$ **to** m **do**
  Forward $\langle ID_p, TS_4, Cert_{gk}, \delta_0, \ldots, \delta_{m-1}\rangle$ **to** Sensor i
end for
for i = 1 **to** m **do**
  Sensor i**:**
  Compute $\varphi_i = H_1(ID_i || r_i pw_i P)$
  Output: $\gamma = \kappa(\varphi_i)$
end for

Accordingly, let $ID_\oslash$ be the temporary identity to be revoked. The current decrypting key $\varphi_\oslash$ is

$$\varphi_\oslash = H_1(ID_\oslash || r_\oslash pw_\oslash P), \tag{22}$$

which will be removed from the key set $\{\varphi_1, \ldots, \varphi_m\}$. The new group key will be randomly selected as $\gamma_\oslash$. The $\kappa(x)$ function involving the remaining $m-1$ sensors is newly calculated as

$$\kappa(x) = (x-\varphi_1)\ldots(x-\varphi_{\oslash-1})(x-\varphi_{\oslash+1})\ldots(x-\varphi_m)+\gamma_\oslash. \tag{23}$$

In this case, $\kappa(\varphi_\oslash) \neq \gamma_\oslash$, indicating that the revoked sensor $ID_\oslash$ cannot derive the updated group key with the previously acquired decrypting key $\varphi_\oslash$. Meanwhile, for $i \in [1, m]\backslash\{\oslash\}$, $\kappa(\varphi_i) = \gamma_\oslash$ holds. The remaining legitimate sensors can directly derive the newly generated key $\gamma_\oslash$ using the stored φ_i. Extra information for key distribution is not required. Forward security towards revoked sensors is provided in this way.

Similarly, let $ID_\bigcirc$ be the temporary identity of newly attending sensor, which has successfully passed the authentication in Section IV-C. The corresponding keying information $\varphi_\bigcirc$ is then added to the current key set. The new group key will be randomly selected as $\gamma_\bigcirc$. In this way, the $\kappa(x)$ function involving the $m+1$ sensors with key set $\{\varphi_1, \ldots, \varphi_m, \varphi_\bigcirc\}$ can be constructed as

$$\kappa(x) = \prod_{i=1}^{m}(x-\varphi_i)(x-\varphi_\bigcirc) + \gamma_\bigcirc. \tag{24}$$

Obviously, for $i \in [1, m] \cap \{\bigcirc\}$, $\kappa(\varphi_i) = \gamma_\bigcirc$ holds. All the valid $m+1$ sensors can acquire the update group key in this case.

Moreover, it is worth nothing that the proposed key updating strategy is able to provide efficient group key updating involving multiple sensor operations simultaneously. The revoked sensors cannot derive the new key from the keying message due to the removal of φ_i from $\kappa(x)$ function. Similarly, the newly joining sensors can acquire the updated group key using the computed φ_i. At this point, the group key updating strategy is finished.

V. SECURITY ANALYSIS

In this section, the featured security properties of the proposed certificateless authentication scheme are analyzed. The security theorems along with the corresponding proofs are formally given. Moreover, the comparisons in terms of the major security characteristics with the state-of-the-arts are presented.

A. UNFORGEABILITY WITH ADAPTIVE CHOSEN MESSAGE ATTACK

We analysis the unforgeability with chosen message attack (CMA) in the proposed authentication scheme. The previously introduced CDHP in **Definition 2** is adopted in the formal proof, along with the **forking lemma** defined as follows:

Definition 3 (Forking Lemma [48]): Let $\mathcal{A}$ be a probabilistic polynomial time Turing machine, given only the public data as input. Within a certain time bound $\mathcal{T}$, if $\mathcal{A}$ can produce, with non-negligible probability, a valid signature $(m, \sigma_1, h, \sigma_2)$, where the tuple (σ_1, h, σ_2) can be simulated without knowing the secret key, then, with an indistinguishable distribution probability, there is another machine which has control over the machine obtained from $\mathcal{A}$ replacing interaction with the signer by simulation and produces two valid signatures $(m, \sigma_1, h, \sigma_2)$ and $(m, \sigma_1, h', \sigma_2')$ such that $h \neq h'$.

Theorem 1: The proposed WBANs certificateless authentication scheme is provably unforgeable towards adaptive chosen message attack (CMA) in the assumption of random oracle model, assuming the hardness of the CDH problem.

Proof: The security of unforgeability is formally defined through the game $\mathcal{G}_1$. Let $\mathcal{A}_1$ be a probabilistic polynomial time (PPT) adversary. It is worth noting that $\mathcal{A}_1$ is assumed to has the capability to break the proposed authentication mechanism. Note that in the constructed game $\mathcal{G}_1$, the utilized hash functions are defined as the random oracles. In this way, it is claimed that by operating the following queries from adversary $\mathcal{A}_1$, the challenger $\mathcal{C}_1$ is able to break the randomness of H_5, H_6 oracles' outputs with the assistance of adversary $\mathcal{A}_1$. Moreover, the hash recording lists are maintained by $\mathcal{C}_1$. Note that $\mathcal{C}_1$ is able to simulate all the oracles. The following corresponding queries of $\mathcal{C}_1$ can be adaptively issued by $\mathcal{A}_1$:

- *H Hash Queries*: Assume that $\mathcal{A}_1$ does not has the ability to compute hash function $H_5(.)$. Hence, the response to *H Hash Queries* is simulated by maintaining a list $list_H$ of couples $\langle \triangle_i, \omega_i\rangle$ initialized to be empty. Note that $\triangle_i$ is defined as the input value pair including $\langle ID, TS, \ell\rangle$, where $\ell \in \mathbb{G}$. In this case, when the adversary $\mathcal{A}_1$ invokes the *H hash Queries* with a particular input value set $\triangle$, $\mathcal{C}_1$ will then check whether the parameter $\triangle$ exists in the existing hash list $list_H$, and perform as follows:

- If the tuple $\langle \triangle, \omega \rangle$ has already been stored in $list_H$, $\mathscr{C}_1$ outputs $\omega = H_5(ID||TS||\ell)$ to $\mathscr{A}_1$.
- Otherwise, $\mathscr{C}_1$ chooses a random $\omega \in \mathbb{Z}_{\mathcal{P}}^*$ and forwards it to $\mathscr{A}_1$. Note that the new tuple $\langle \triangle, \omega \rangle$ will be subsequently added to $list_H$.

- *h Hash Queries*: Assume that $\mathscr{A}_1$ does not has the ability to compute hash function $H_6(.)$. Hence, the response to *h Hash Queries* is simulated by maintaining a list $list_h$ of couples $\langle \nabla_i, \xi_i \rangle$ initialized to be empty. Note that ∇_i is defined as the input value pair including $\langle ID, TS, \alpha, \beta \rangle$, where $\alpha, \beta \in \mathbb{G}$. In this case, when the adversary $\mathscr{A}_1$ invokes the *h hash Queries* with a particular input value set ∇, $\mathscr{C}_1$ will then check whether the parameter ∇ exists in the existing hash list $list_h$, and perform as follows:
  - If the tuple $\langle \nabla, \xi \rangle$ has already been stored in $list_h$, $\mathscr{C}_1$ outputs $\omega = H_6(ID||TS||\alpha||\beta)$ to $\mathscr{A}_1$.
  - Otherwise, $\mathscr{C}_1$ chooses a random $\xi \in \mathbb{Z}_{\mathcal{P}}^*$ and forwards it to $\mathscr{A}_1$. Note that the new tuple $\langle \nabla, \xi \rangle$ will be subsequently added to $list_h$.
- *Extracting Queries*: Upon the *Extracting Query* with *ID* is made to $\mathscr{C}_1$, $\mathscr{C}_1$ conducts *H hash Query* on the input $\triangle^1$ and outputs the corresponding tuple $\langle \triangle^1, \omega^1 \rangle$. Note that the tuple $\langle \triangle^1, \omega^1 \rangle$ has already recorded in $list_H$ previously. Subsequently, another *H hash Query* with the corresponding tuple $\langle \triangle^2, \omega^2 \rangle$ is made, where the tuple $\langle \triangle^2, \omega^2 \rangle$ has already recorded in $list_H$ previously. Note that $\triangle^1 \neq \triangle^2$ and $\omega^1 \neq \omega^2$ hold. Thereafter, *h hash Query* is performed with the output $\langle \nabla, \xi \rangle$. Subsequently, $\mathscr{C}_1$ randomly selects $r_i, pw_i \in \mathbb{Z}_{\mathcal{P}}^*$ and computes $\hbar_i = pw_i\omega^1 + r_i\omega^2$ and $Cert_i = (r_i pw_i + \xi_i \hbar_i)P$. The calculated tuple $\langle \hbar_i, \xi_i, Cert_i \rangle$ will be sent to $\mathscr{A}_1$.

Finally, according to Definition 3, adversary is able to obtain two validated tuples $\langle \hbar_i, \xi_i, Cert_i \rangle$ and $\langle \hbar_i^*, \xi_i, Cert_i^* \rangle$ after querying $\mathscr{C}_1$, where both tuples can pass the authentication process. Accordingly, $Cert_i \neq Cert_i^*$, $\hbar_i \neq \hbar_i^*$ hold. Hence, the following equations can be presented as:

$$\begin{cases} Cert_i = (r_i pw_i + \xi_i \hbar_i)P \\ Cert_i^* = (r_i pw_i + \xi_i \hbar_i^*)P. \end{cases} \tag{25}$$

At this point, the result is shown as

$$\begin{aligned} &Cert_i - Cert_i^* \\ &\quad = (r_i pw_i + \xi_i \hbar_i)P - (r_i pw_i + \xi_i \hbar_i^*)P \\ &\quad = \xi_i \hbar_i P - \xi_i \hbar_i^* P \\ &\quad = (\hbar_i - \hbar_i^*)\xi_i P. \end{aligned} \tag{26}$$

Finally, we can get $\xi_i P = (\hbar_i - \hbar_i^*)^{-1}(Cert_i - Cert_i^*)$ as the solution, which contradicts with the hardness of the aforementioned CDH problem. Hence, the advantage of $\mathscr{A}_1$ winning the game is negligible. The proposed authentication scheme is secure against forgery attack with CMA under random oracle model. □

B. RESISTANCE TO REPLAY ATTACK

Replay attack is defined as the common network attacking type in wireless communication, which is conducted by reusing the previously acquired crucial keying information in the current authentication session. In this section, we discuss the replay attack resistance of the proposed authentication scheme as follows.

Theorem 2: The proposed WBANs certificateless authentication scheme provides resistance to replay attack during the whole authentication process. The previously acquired messages from past sessions cannot pass the current authentication process.

Proof: Assuming that in timepoint T_e, the adversary $\mathscr{A}_2$ has access to all the published parameters from the transmitted packets during the time interval $[T_s, T_e]$ ($T_s < T_e$). Note that the acquired information includes four different kinds of transmitting messages from authentication to group key distribution. That is, $\left\langle Request, TS_1, ID_p, \Psi_p^1, Cert_p^1 \right\rangle$ to ECG sensor, $\left\langle TS_2, ID_{ecg}, \Theta_p, \Upsilon_{ecg}^2, Cert_{ecg}^2 \right\rangle$ to all devices, $\langle TS_3, ID_i, R_i, \wp_i, Cert_i \rangle_{i\in[2,n]}$ to smartphone, $\left\langle ID_p, TS_4, Cert_{gk}, \delta_0, \ldots, \delta_{m-1} \right\rangle$ to all sensors. In this case, with the purpose of successfully passing the verification process in the receiver side on the future timepoint T_f ($T_e < T_f$), $\mathscr{A}_2$ conducts the following two types of processing:

- *Type-I Passive Attack:* It is assumed that the adversary $\mathscr{A}_2$ repeatedly distributes the unaltered packets to destinated verifiers. Hence, let $packet_{T_{pr}}^i$ denote the specific packet for certain previous timepoint T_{pr}, where the sequence number i represents the packet types. That is, for $\forall i \in [1, 4]$, $\forall T_{pr} \in [T_s, T_e]$, the packets set is presented as $packet_{T_{pr}}^i$, indicating that the previously acquired messages are directly sent in future authentication session without any modification. As for $\left\{packet_{T_{pr}}^i\right\}$, it is obvious that the timestamp $TS_i (i \in [1, 4])$ is contained in all kinds of packets. The destinated verifier will firstly check the freshness of TS_i in $\left\{packet_{T_{pr}}^i\right\}$. Consequently, the previous timestamp TS_i cannot meet the verification requirements. *Type-I passive attack* is prevented accordingly.
- *Type-II Active Attack:* In the assumption, the acquired packets are modified first, and then submitted to verifier. Note that the certificate *Cert* involving all the transmitted metrics are participated each time. We consider the keying message $\langle TS_3, ID_i, R_i, \wp_i, Cert_i \rangle_{i\in[2,n]}$ sent from $n-1$ sensors. TS_f is defined as the future timestamp, which will be adopted in the newly generated packet described as $\left\langle TS_f, ID_i, R_i, \wp_i, Cert_i \right\rangle_{i\in[2,n]}$. Obviously, the newly generated packet cannot pass the verification as:

$$\begin{aligned} \wp_i \neq\ & H_6(ID_i||TS_f||R_i||Cert_i \\ & - \wp_i[H_5\left(ID_i||TS_f||aR_i\right)(pw_i P) \\ & + H_5(ID_p||TS_{f3}||a(pw_i P))R_i]). \end{aligned} \tag{27}$$

Due to the inherent characteristic of secure one-way hash function, the above equation does not hold since $TS_f \neq TS_3$, indicating that the reusage towards historical information and current fresh timestamp is not achievable in our design.

TABLE 3. Comparison on security properties.

Scheme	AKES [4]	PATF [16]	LMAP [49]	Our Scheme
Unforgeability	√	√	√	√
Replay Attack Resistance	√	√	√	√
Identity Privacy Preservation	√	√	×	√
Session Key Establishment	√	√	√	√
Certificateless Authentication	×	×	√	√
Dynamic Key Updating	×	×	×	√

During each communication of our scheme, the data integrity and confidentiality are timely preserved by the corresponding timestamp and certificates. Any modification towards the acquired messages results in failure of the verification process in receiver side. Note that the analysis for the remaining packet types are similar. In conclusion, the transmitted messages are fully protected with hash function. Moreover, each packet is mapped to precise timestamp. The replaying attack can be prevented in this way. □

C. PROVISION TO IDENTITY PRIVACY PRESERVING

In practical WBANs scenarios, the open wireless communicating characteristics may lead to potential vulnerability towards illegal identity tracing by malicious entities. This way, the user privacy involving location information may be revealed. Similarly, unlinkability for the adopted user information during different authenticating sessions should be presented as well so as to offer impersonate attack resistance.

Theorem 3: The proposed authentication scheme provides resistance to illegal tracing towards specific WBANs devices. Furthermore, unlinkability for sensors in different session are accordingly provided.

Proof: As described in the aforementioned offline registration phase, the constant identity for smartphone and sensors are respectively issued as ID_p^o and ID_i^o. Note that these allocated identities remain confidential all the time. Meanwhile, the temporary identities are computed as $ID_p = H_1(ID_p^o||\Theta_p)$, and $ID_i = H_1(ID_i^o||r_iP)$. It is worth noting that the included Θ_p and r_iP are randomly generated for individual session. That is, the temporary identities for all WBANs devices are not static all the time. Hence, the tracing towards certain identity is not possible. As a result, the provision to identity privacy preserving is enabled in our scheme. □

D. SESSION KEY ESTABLISHMENT

In the designated WBANs model, the commonly shared session key between the legitimate devices is of significance. Therefore, the group key $\gamma \in \mathbb{Z}_{\mathcal{P}}^*$ is generated and distributed to all devices.

Theorem 4: The universal session key is established in the proposed scheme, where the revoked sensors cannot derive the current session key with previous acquired keying message.

Proof: Accordingly, the distributing strategy is achieved in the particular $\kappa(x)$ function, where $\kappa(x) = (x-\varphi_1)\ldots(x-\varphi_m)+\gamma$. In this case, the decryption key φ_j for all the verified devices is adopted. In receiver side, the legitimate sensors can reconstruct the $\kappa(x)$ function and derive the group key as $\kappa(\varphi_j) = \gamma$, while the revoked devices cannot decrypt the correct value according to $\kappa(\varphi^*) = (\varphi^*-\varphi_1)\ldots(\varphi^*-\varphi_m)+\gamma \neq 0+\gamma$. In other word, it is assumed the length of the decryption key φ_j is τ. The probability to successfully derive the group key is negligible as $\Pr\left[\kappa(\varphi^*) = \kappa(\varphi_j)\right] = \frac{m}{2^\tau} < \epsilon$. Hence, the secure group communication channel for frequent biomedical data exchange is applicable. □

E. CERTIFICATELESS AUTHENTICATION

The certificateless authentication feature is provided in our scheme, where key escrow issue can be prevented in this way. In this section, we analysis the certificateless authentication property as follows.

Theorem 5: The proposed scheme can provide certificateless authentication feature for WBAN devices. The compromised smartphone cannot reveal the confidential keying message of particular vehicle. Furthermore, HC cannot impersonate legitimate sensors with the stored secret key.

Proof: As illustrated above, during the authentication phase, both HC and smartphone have zero knowledge about the self-generated random partial secret key r_i in the sensor side. Meanwhile, HC and smartphone cannot derive the r_i within $R_i = r_iP$ according to ECDLP assumption. Note that r_i is kept secret during the entire process. In this way, the impersonation towards certain sensors cannot be validated. In the aforementioned group key distribution phase, the smartphone directly consults the keying information from HC and gets pw_iP, while the crucial password pw_i is kept secret. Hence, the certificateless authentication property is provided in our scheme. □

F. COMPARISON ON SECURITY PROPERTIES

In this section, the comparison in terms of the crucial security properties for WBANs authentication scenarios is presented. The proposed protocol is compared with the state-of-the-art WBANs authentication and key agreement schemes including AKES [4], PATF [16], and LMAP [49] with the purpose of demonstrating its superiority on security properties. The comparison results are presented in Table 3, indicating that the proposed scheme satisfies the desired security requirements.

VI. PERFORMANCE ANALYSIS

In this section, the corresponding performance analysis towards the proposed scheme is discussed, which mainly emphasizes on the essential parameters for resource-limited WBANs devices: **storage overhead**, **computation cost**, **communication cost**.

A. STORAGE OVERHEAD

As mentioned above, the WBANs devices are assumed to be resource-limited entities with comparatively restricted computation ability and storing capacity. Therefore, the storage overhead required during the entire authentication process should be taken into consideration. That it, for both

TABLE 4. Comparison of storage overhead.

Scheme	AKES [4]	PATF [16]	LMAP [49]	Our Scheme
Storage Cost (Smartphone)	$3768n + 536$ bits	$2848n + 392$ bits	$2976n + 224$ bits	$728n + 192m + 1616$ bits
Storage Cost (Sensor)	3664 bits	3312 bits	3040 bits	ECG:$32m + 2504$ bits Regular: $32m + 1904$ bits

TABLE 5. Comparison of computation cost.

Scheme	AKES [4]	PATF [16]	LMAP [49]	Our Scheme
Computation Cost (Smartphone)	$n\hat{e} + 6nH + 4nEx + 5nM$ $\approx (9.25n)$ ms	$np + 8nH$ $\approx (9.17n)$ ms	$1Enc + (4n + 1)p + nH + nEx$ $\approx (5.69n + 57.01)$ ms	$(2n + 1)p + (2n + 3)H + 2nM$ $\approx (2.38n + 1.2)$ ms
Computation Cost (Sensor)	$2\hat{e} + 6H + 3Ex + 3M$ $\approx (12.38)$ ms	$3p + 4H$ $\approx (7.51)$ ms	$1Dec + 4p + H + Ex$ $\approx (84.19)$ ms	ECG:$3p + 6H + Ex + 1M$ $\approx (3.59)$ ms Regular: $2p + 6H + Ex + 6M$ $\approx (2.47)$ ms

the smartphone and multiple sensors, it is not practical to store massive keying information. It is worth noting that the HC is defined as the service provider with adequate processing ability. Therefore, the analysis here emphasizes on the storage overhead in smartphone and sensor side, while the HC is not included. The state-of-the-art WBANs authentication schemes including AKES [4], PATF [16], and LMAP [49] are compared with the proposed scheme so as to demonstrate the advantage of our scheme on storage overhead.

In the offline registration phase of our scheme, the constant identity ID_p^o is allocated to smartphone for subsequent usage. Thereafter, the randomly generated secret key $a \in \mathbb{Z}_{\mathcal{P}}^*$, as well as the computed partial secret is stored. The temporary identity ID_p is generated as well. Meanwhile, the parameters in the requesting packet are stored, which includes the timestamp TS_1, and verifying information Ψ_p^1 and $Cert_p^1$. Accordingly, we define the length of the identity such as ID_p^o and ID_p is 32 bits, while length of the elements in group $\mathbb{G}$ is 256 bits. The length of keying information $Cert_p^1$, and the timestamp TS_1, are assumed to be 160 bits and 24 bits respectively. At this point, the total storage in smartphone side is calculated as $32 \times 2 + 160 \times 3 + 24 + 256 \times 2 = (1080)$ bits. In the next, the derived information from ECG sensors is presented as $\langle TS_2, ID_{ecg}, \Theta_p, \Upsilon_{ecg}^2, Cert_{ecg}^2 \rangle$, which includes timestamp TS_2, the biometric Γ_{ecg}^2, along with the keying information Υ_{ecg}^2 and certificate $Cert_{ecg}^2$. Besides, the unique value $r_{ecg}pw_1$ P for ECG sensor is collected. Hence, the storage for this session is calculated as $24+32+160\times2+256\times2 = (888)$ bits. Similarly, in the authentication process with the remaining $n-1$ sensors, $\langle TS_3, ID_i, R_i, \wp_i, Cert_i \rangle_{i\in[2,n]}$ is delivered. The required storage for all $n-1$ sensors is $(24+32+160+256\times4)(n-1) = (728n-728)$ bits. Finally, length of the decrypting key φ_i, and the generated group key $\gamma \in \mathbb{Z}_{\mathcal{P}}^*$, are set to be 160 bits. The coefficient δ_i for $\kappa(x)$ are set to be 32 bits. The storage overhead during group key distribution phase is $160m + 32m + 160 \times 2 + 32 + 24 = (192m + 376)$ bits. In conclusion, the total storage cost in smartphone is $(1080)+(888)+(728n-728)+(192m+376) = (728n + 192m + 1616)$ bits.

TABLE 6. Comparison of communication cost.

Scheme	AKES [4]	PATF [16]	LMAP [49]	Our Scheme
Communication Rounds	$4n$	$4n$	$4n + 1$	$n + 2$

On the other hand, the storage cost for ECG sensor and other regular sensors are different. For ECG sensor, the storage overhead can be calculated as $32 \times 4 + 24 \times 3 + 160 \times 8 + 32m + 256 \times 4 = (32m + 2504)$ bits, which covers the entire authentication process and group key distribution phase. As for the $n-1$ regular sensors, the storage overhead is $32 \times 4 + 24 \times 2 + 160 \times 6 + 32m + 256 \times 3 = (32m + 1904)$ bits. The comparison results with the existing WBANs authentication schemes are shown in Table 4. It is obvious that less storage overhead is required in the proposed scheme.

B. COMPUTATION COST

In this section, we analyze the computation cost of the proposed authentication scheme by discussing the necessary calculations required for WBANs authentication and group key distribution. Note that in our design, the computation in ECG sensor and regular sensor is different, which are respectively discussed then. For better description, the point multiplication and the pairing operation are respectively denoted as p and $\hat{e}$. The one-way hash function, multiplication, and exponential operation are respectively denoted as H, M, and Ex. Meanwhile, Enc and Dec are shortened for symmetric encryption and decryption. Accordingly, we adopt the operation execution time from [50]. Hence the estimated execution time can be calculated. The comparison results on computation cost is shown in Table 5, showing that our scheme requires relatively smaller computation cost compared with other schemes, which is of significance to the practical scenarios with resource-limited WBANs devices.

C. COMMUNICATION COST

In this section, we discuss the required communication rounds for the WBANs authentication in smartphone side, where totally n sensors are assumed to be successfully verified. Initially, the requesting message is delivered through

one broadcasting operation. Thereafter, interaction with each participating sensor requires only 1 communication round, where the offline registration phase is not included. The final group key distribution is conducted with one broadcast operation as well. In this way, the total communication rounds involving n sensors is $n + 2$ in our design. Accordingly, the comparison result on communication cost is given in Table 6, demonstrating that less communication rounds are required in our scheme comparing with the state-of-the-arts.

VII. CONCLUSION

In this paper, a secure certificateless biometric authentication and group key management for WBAN scenarios is proposed. In our design, the novel WBANs communication infrastructure is adopted. The distinctive physiological electrocardiogram feature for specific user is deployed in the authentication process. Subsequently, efficient group key management involving the legitimate sensors is presented, where minor computation cost is required for dynamic key updating in sensor side. Security analysis indicates that the proposed authentication scheme can achieve desired security properties and provide resistance towards various attacks. Performance analysis illustrates that the proposed scheme is efficient compared with the state-of-the-art WBAN authentication schemes.

REFERENCES

[1] H. Xiong, "Cost-effective scalable and anonymous certificateless remote authentication protocol," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 12, pp. 2327–2339, Dec. 2014.

[2] G. Zheng, G. Fang, R. Shankaran, M. A. Orgun, J. Zhou, L. Qiao, and K. Saleem, "Multiple ECG fiducial points-based random binary sequence generation for securing wireless body area networks," *IEEE J. Biomed. Health Inform.*, vol. 21, no. 3, pp. 655–663, May 2017.

[3] M. Wazid, A. K. Das, and A. V. Vasilakos, "Authenticated key management protocol for cloud-assisted body area sensor networks," *J. Netw. Comput. Appl.*, vol. 123, pp. 112–126, Dec. 2018.

[4] W. Drira, É. Renault, and D. Zeghlache, "A hybrid authentication and key establishment scheme for WBAN," in *Proc. IEEE 11th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Jun. 2012, pp. 78–83.

[5] X. Cao, X. Zeng, W. Kou, and L. Hu, "Identity-based anonymous remote authentication for value-added services in mobile networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 7, pp. 3508–3517, Sep. 2009.

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

[7] A. K. Das, A. K. Sutrala, V. Odelu, and A. Goswami, "A secure smartcard-based anonymous user authentication scheme for healthcare applications using wireless medical sensor networks," *Wireless Pers. Commun.*, vol. 94, no. 3, pp. 1899–1933, 2017.

[8] H. Tan, D. Choi, P. Kim, S. Pan, and I. Chung, "Comments on 'dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks,'" *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 7, pp. 2149–2151, Jul. 2017.

[9] F. Li, Y. Han, and C. Jin, "Cost-effective and anonymous access control for wireless body area networks," *IEEE Syst. J.*, vol. 12, no. 1, pp. 747–758, Mar. 2018.

[10] H. Xiong and Z. Qin, "Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 7, pp. 1442–1455, Jul. 2015.

[11] J. Liu, Z. Zhang, X. Chen, and K. S. Kwak, "Certificateless remote anonymous authentication schemes for WirelessBody area networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 332–342, Feb. 2014.

[12] H. Tan, Z. Gui, and I. Chung, "A secure and efficient certificateless authentication scheme with unsupervised anomaly detection in VANETs," *IEEE Access*, vol. 6, pp. 74260–74276, 2018.

[13] M. H. Ibrahim, S. Kumari, A. K. Das, M. Wazid, and V. Odelu, "Secure anonymous mutual authentication for star two-tier wireless body area networks," *Comput. Methods Programs Biomed.*, vol. 135, pp. 37–50, Oct. 2016.

[14] M. E. S. Saeed, Q.-Y. Liu, G. Tian, B. Gao, and F. Li, "Remote authentication schemes for wireless body area networks based on the Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4926–4944, Dec. 2018.

[15] C. Hu, H. Li, Y. Huo, T. Xiang, and X. Liao, "Secure and efficient data communication protocol for wireless body area networks," *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 2, no. 2, pp. 94–107, Apr./Jun. 2016.

[16] Q. Jiang, N. Kumar, J. Ma, J. Shen, D. He, and N. Chilamkurti, "A privacy-aware two-factor authentication protocol based on elliptic curve cryptography for wireless sensor networks," *Int. J. Netw. Manage.*, vol. 27, no. 3, p. e1937, 2017.

[17] H. Tan and I. Chung, "A secure and efficient group key management protocol with cooperative sensor association in WBANs," *Sensors*, vol. 18, no. 11, p. 3930, 2018.

[18] H. Kim and S. Y. Chun, "Cancelable ECG biometrics using compressive sensing-generalized likelihood ratio test," *IEEE Access*, vol. 7, pp. 9232–9242, 2019.

[19] Z. Zhang, H. Wang, A. V. Vasilakos, and H. Fang, "ECG-cryptography and authentication in body area networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 6, pp. 1070–1078, Nov. 2012.

[20] A. K. Das, V. Odelu, and A. Goswami, "A secure and robust user authenticated key agreement scheme for hierarchical multi-medical server environment in TMIS," *J. Med. Syst.*, vol. 39, no. 9, p. 92, Sep. 2015.

[21] B. Sayed, I. Traoré, I. Woungang, and M. S. Obaidat, "Biometric authentication using mouse gesture dynamics," *IEEE Syst. J.*, vol. 7, no. 2, pp. 262–274, Jun. 2013.

[22] A. K. Das, S. Chatterjee, and J. K. Sing, "A new biometric-based remote user authentication scheme in hierarchical wireless body area sensor networks," *Ad Hoc Sensor Wireless Netw.*, vol. 28, nos. 3–4, pp. 221–256, 2015.

[23] H. Tan, Y. Song, S. Xuan, S. Pan, and I. Chung, "Secure D2D group authentication employing smartphone sensor behavior analysis," *Symmetry*, vol. 11, no. 8, p. 969, 2018.

[24] Z. Sitová, J. Šedenka, Q. Yang, G. Peng, G. Zhou, P. Gasti, and K. S. Balagani, "HMOG: New behavioral biometric features for continuous authentication of smartphone users," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 5, pp. 877–892, May 2016.

[25] Y. Chu, H. Shen, and K. Huang, "ECG authentication method based on parallel multi-scale one-dimensional residual network with center and margin loss," *IEEE Access*, vol. 7, pp. 51598–51607, 2019.

[26] S. Chatterjee, S. Roy, A. K. Das, S. Chattopadhyay, N. Kumar, and A. V. Vasilakos, "Secure biometric-based authentication scheme using Chebyshev chaotic map for multi-server environment," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 5, pp. 824–839, Sep./Oct. 2018.

[27] J. S. Arteaga-Falconi, H. Al Osman, and A. El Saddik, "ECG authentication for mobile devices," *IEEE Trans. Instrum. Meas.*, vol. 65, no. 3, pp. 591–600, Mar. 2016.

[28] M. Hammad, Y. Liu, and K. Wang, "Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint," *IEEE Access*, vol. 7, pp. 26527–26542, 2019.

[29] H. Tan, D. Choi, P. Kim, S. Pan, and I. Chung, "An efficient hash-based RFID grouping authentication protocol providing missing tags detection," *J. Internet Technol.*, vol. 19, no. 2, pp. 481–488, 2018.

[30] Z. Li, H. Wang, and H. Fang, "Group-based cooperation on symmetric key generation for wireless body area networks," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1955–1963, Dec. 2017.

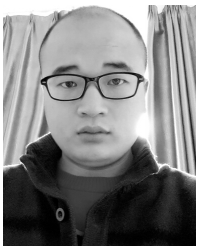
[31] F. Li and J. Hong, "Efficient certificateless access control for wireless body area networks," *IEEE Sensors J.*, vol. 16, no. 13, pp. 5389–5396, Jul. 2016.

[32] W. Sheng, S. Chen, G. Xiao, J. Mao, and Y. Zheng, "A biometric key generation method based on semisupervised data clustering," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 45, no. 9, pp. 1205–1217, Sep. 2015.

[33] H. Tan, D. Choi, P. Kim, S. Pan, and I. Chung, "Secure certificateless authentication and road message dissemination protocol in VANETs," *Wireless Commun. Mobile Comput.*, vol. 2018, no. 1, 2018, Art. no. 7978027.

[34] J.-H. Yang and C.-C. Chang, "An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem," *Comput. Secur.*, vol. 28, no. 3, pp. 138–143, 2009.

[35] L. Zhang, J. Liu, and R. Sun, "An efficient and lightweight certificateless authentication protocol for wireless body area networks," in *Proc. 5th Int. Conf. Intell. Netw. Collaborative Syst.*, Sep. 2013, pp. 637–639.
[36] J. Shen, H. Tan, Y. Zhang, X. Sun, and Y. Xiang, "A new lightweight RFID grouping authentication protocol for multiple tags in mobile environment," *Multimedia Tools Appl.*, vol. 76, no. 21, pp. 22761–22783, 2017.
[37] G. Horn and B. Preneel, "Authentication and payment in future mobile systems," in *Proc. Eur. Symp. Res. Comput. Secur.*, 1998, pp. 277–293.
[38] H. Wang, "Identity-based distributed provable data possession in multi-cloud storage," *IEEE Trans. Services Comput.*, vol. 8, no. 2, pp. 328–340, Mar./Apr. 2015.
[39] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology—CRYPTO*. Berlin, Germany: Springer, 1984, pp. 47–53.
[40] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Advances in Cryptology—ASIACRYPT*. Berlin, Germany: Springer, 2003, pp. 452–473.
[41] 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.
[42] W. Meng, D. S. Wong, S. Furnell, and J. Zhou, "Surveying the development of biometric user authentication on mobile phones," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1268–1293, 3rd Quart., 2015.
[43] H.-S. Choi, B. Lee, and S. Yoon, "Biometric authentication using noisy electrocardiograms acquired by mobile sensors," *IEEE Access*, vol. 4, pp. 1266–1273, 2016.
[44] F. A. Khan, N. A. H. Haldar, A. Ali, M. Iftikhar, T. A. Zia, and A. Y. Zomaya, "A continuous change detection mechanism to identify anomalies in ECG signals for WBAN-based healthcare environments," *IEEE Access*, vol. 5, pp. 13531–13544, 2017.
[45] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Int. J. Inf. Secur.*, vol. 1, no. 1, pp. 36–63, 2001.
[46] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," *J. Comput. Syst. Sci.*, vol. 18, no. 2, pp. 143–154, Apr. 1979.
[47] Y. Wang, L. Wang, X. Chen, and W. Zhu, "P wave detection and delineation based on distances transform," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Aug. 2016, pp. 2197–2201.
[48] N.-W. Lo and J.-L. Tsai, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 5, pp. 1319–1328, May 2016.
[49] J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun, "A lightweight multi-layer authentication protocol for wireless body area networks," *Future Gener. Comput. Syst.*, vol. 78, pp. 956–963, Jan. 2018.
[50] M. Scott, N. Costigan, and W. Abdulwahab, "Implementing cryptographic pairings on smartcards," in *Cryptographic Hardware and Embedded Systems—CHES*. Berlin, Germany: Springer, 2006, pp. 134–147.



HAOWEN TAN received the B.E. and M.E. degrees in computer science from the Nanjing University of Information Science and Technology, Nanjing, China, in 2013 and 2016, respectively. He is currently pursuing the Ph.D. degree with the Department of Computer Engineering, Chosun University, Gwangju, South Korea. His research interests include information security, wireless body area networks, radio frequency identification, and vehicular ad hoc networks.

ILYONG CHUNG received the B.E. degree from Hanyang University, Seoul, South Korea, in 1983, and the M.S. and Ph.D. degrees in computer science from The City University of New York, in 1987 and 1991, respectively. From 1991 to 1994, he was a Senior Technical Staff with the Electronic and Telecommunication Research Institute (ETRI), Dajeon, South Korea. Since 1994, he has been a Professor with the Department of Computer Science, Chosun University, Gwangju, South Korea. His research interests include computer networking, security systems, and coding theory.