This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.

Certificateless Remote Anonymous Authentication Schemes for Wireless Body Area Networks

Jingwei Liu *Member of IEEE*, Zonghua Zhang, Xiaofeng Chen *Member of IEEE*, and Kyung Sup Kwak *Member of IEEE*

***Abstract*—Wireless body area network (WBAN) has been recognized as one of the promising wireless sensor technologies for improving healthcare service thanks to its capability of seamlessly and continuously exchanging medical information in real time. However, the lack of an clear in-depth defense line in such a new networking paradigm would make its potential users worry about the leakage of their private information, especially to those unauthenticated or even malicious adversaries. In this paper, we present a pair of efficient and light-weight authentication protocols to enable remote WBAN users to anonymously enjoy healthcare service. In particular, our authentication protocols are rooted with a novel certificateless signature (CLS) scheme, which is computational efficient and provably secure against existential forgery on adaptively chosen message attack in the random oracle model. Also, our designs ensure that application or service providers have no privilege to disclose the real identities of users. Even the network manager, which serves as private key generator in the authentication protocols, are prevented from impersonating legitimate users. The performance of our designs are evaluated through both theoretic analysis and experimental simulations, and the comparative studies demonstrate that they outperform the existing schemes in terms of better trade-off between desirable security properties and computational overhead, nicely meeting the needs of WBANs.**

***Index Terms*—Anonymous Authentication, Certificateless Signature, Wireless Body Area Network, Healthcare.**

I. Introduction

By using wireless personal area network (WPAN) technologies for communications on, near and around the human body, T. G. Zimmerman firstly proposed Wireless body area network (WBAN) in 1996 [1]. The work then immediately drew much attention from both academia and industry. For instance, IEEE802.15 has developed a family of short distance communication standards. In particular, 802.15.6 was formally standardized in 2012 after five years effort of engineers from sixty companies. It is about the low power wireless sensor nodes used in WBAN to gather biomedical information for various applications in hospitals, residential and work environments [2], [3], [4], [5]. Basically there are two categories of WBAN applications, i.e., medical and non-medical ones [6]. Medical applications need to collect vital information of a patient continuously and forward it to a remote monitoring station for further analysis. This huge amount of data can be used to prevent the occurrence of myocardial infarction and treat various diseases such as gastrointestinal tract, cancer, asthma, and neurological disorder. Non-medical applications include monitoring forgotten things data file transfer, gaming, and social networking applications. For example, in gaming, sensors in WBAN can collect coordinates movements of different parts of the body and subsequently make the movement of a character in the game, e.g. , moving soccer player or capturing the intensity of a ball in table tennis. The use of WBAN in social networking allows people to exchange digital profile or business card only by shaking hands. Figure 1 illustrates one typical medical application scenario of WBAN, where biological information of concern like heartbeat rate and blood pressure are gathered by the sensors around the body (in-body networks) and transmitted to body area network (BAN) controller nodes (out-body networks), such as PDA and smart phones, which serve as gateway for anonymously accessing the services provided by external networks and servers.

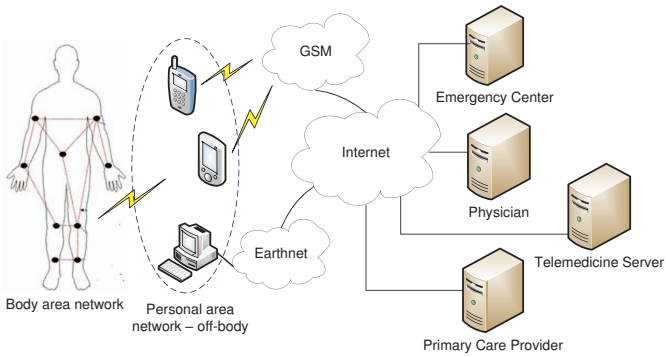

Fig. 1: A WBAN example for healthcare

Despite the past non-trivial effort, WBAN is still in its infancy, attracting increasing research attention [7]. In particular, among the open issues, leakage of privacy is one of the major concerns of potential users, impeding the further development and practical application of such networks. This issue is especially challenging in WBAN due to its unique characteristics, such as open medium channel, signal noise, mobile terminals, flexible infrastructure, and so on, leading to many novel security vulnerabilities and threats. For example, in remote healthcare applications, authorized patients should anonymously access and share medical services, and the doctors only need to know the bio-information of the patient, whereas all the rest private information such as name and ID number must be kept unknown. In another word, the

Jingwei Liu and Xiaofeng Chen are with the State Key Lab of ISN, Xidian University, China. Zonghua Zhang is with the Institute Mines-Telecom/TELECOM Lille1, France. Kyung Sup Kwak is with the School of Information and Communication Engineering, Inha University, Korea. E-mail: jwliu@mail.xidian.edu.com, xfchen@xidian.edu.cn, zonghua.zhang@gmail.com, kskwak@inha.ac.kr.

Manuscript received Sep. 9, 2012; revised Mar. 24, 2013.

Digital Object Indentifier 10.1109/TPDS.2013.145

legitimate users should be allowed to preserve their privacy to the maximum extent. One of the most effective solutions to achieve that is *remote anonymous authentication schemes*, which are considered in this paper.

A. Related Work

Theoretically, remote user authentication can be implemented by traditional public-key cryptosystems (PKC) [8], [9]. But most of the designs are infeasible in mobile networks, because PKC needs to compute modular exponentiation, which may consume more computational resource than what mobile devices can offer. Then various authentication schemes based on elliptic curve cryptosystem (ECC) have been proposed as alternatives [10], [11], [12], [13], [14], [15], [16], [17], which have better performance thanks to the smaller key size used in ECC [18]. For example, 160-bit ECC achieve the same security level as 1024-bit RSA. However, ECC-based ones also require a certification authority (CA) to maintain a pool of certificates for users' public keys, and the users need extra computation to verify the certificates of others.

We have also seen a vast amount of work on anonymous authentication protocols of RFID systems [19], [20], [21], [22], [23], [24], [25], [26], which are used to verify that RFID tags are legitimate or not without knowing their actual identities. However, most symmetric-cryptosystem based RFID authentication schemes [20], [21], [22], [23] always assume RFID readers to be fully trusted and involve onerous management. In [24], based on PKC, anonymity of tags is preserved against readers by using anonymous credentials. But this design may incur high computational and management complexity. Based on the recently proposed anoymizer-approach, the authors of [25] proposed an anonymous authentication scheme, but it involves an additional device called anonymizer, which frequently interacts with the tags to ensure anonymity and unlinkability of tags. Thus, it's clear that most of the exiting RFID authentication schemes can not be simply applied to the remote WBAN application scenario.

It has been shown that the performance of ECC-base schemes can be enhanced through ID-based cryptosystem [27], especially those ID-based signatures (IBS) over ECC [28], [29], [30], [31], [32], [33], [34], [35], [36]. As some of the earlier studies such as [28], [29], [30] have key escrow problems, Al-Riyami et al. [31] introduced certificateless public key cryptography (CL-PKC) to deal with this fundamental limitation of IBS-based schemes. Also, an IBS scheme without trusted private key generator (PKG) was proposed to solve the inherent key escrow problem [32]. In particular, an efficient certificateless signature (CLS) scheme, which is more efficient than IBS proposed in [31], was presented in [34], and [35] reported an efficient and simple certificateless public-key signature scheme (with security proof in the random oracle model). In [36], Wang et al. proposed an efficient CLS scheme based on bilinear pairings, claiming that its efficiency can be improved by pre-computing the pairing $e(P, P) = g$ which are then used as system parameters.

B. Our Contribution

By carefully exploring the intrinsic characteristics of WBANs and examining the existing remote authentication schemes, we present two novel certificateless remote anonymous authentication protocols. Our non-trivial efforts can be summarized as follows.

- We develop a new CLS scheme as the cryptographic primitive, which is cost-effective, efficient and provably secure against existential forgery on adaptively chosen message attack in the random oracle model by assuming CDHP is intractable. The detailed design is given in Section III, along with efficiency comparisons with the existing well-known schemes.
- The proposed CLS scheme then serves as a design basis for two remote anonymous authentication protocols, which are particularly suitable for resource-constrained mobile clients. In particular, the protocols use an anonymous account index instead of a WBAN client's real identity to access WBAN service, thereby preventing the potential privacy leakage to application providers (AP) and network managers (NM). The protocols design is reported in Section IV.
- A formal security analysis on our proposed protocols is conducted, laying a theoretic foundation for examining the soundness and performance of the similar designs. The concrete analysis is presented in Section V, and a set of experimental simulations is reported in Section VI to complement with the theoretic analysis.

II. Preliminaries

To facilitate the understanding of our designs, we briefly give the basic definitions and properties of bilinear pairings over elliptic curve group.

A. Notation

For easier illustration, Table I lists some important notation which will be given further explanation where they occur for the first time.

B. Bilinear Pairings

The bilinear pairings namely Weil pairing and Tate pairing of algebraic curves is defined as a map $e : G_1 \times G_1 \rightarrow G_2$, where G_1 is a cyclic additive group generated by P, whose order is a prime q, and G_2 is a cyclic multiplicative group of the same order q. Let a, b be elements of $\mathbb{Z}_q^*$. We assume that the discrete logarithm problems (DLP) in both G_1 and G_2 are hard. Bilinear pairings have the following properties:

1) Bilinear: $e(aR, bS) = e(R, S)^{ab}$, $\forall R, S \in G_1$ and $a, b \in \mathbb{Z}_q^*$. This can be related as $\forall R, S, T \in G_1, e(R+S, T) = e(R, T)e(S, T)$ and $e(R, S + T) = e(R, S)e(R, T)$;
2) Non-degenerate: There exists $R, S \in G_1$, such that $e(R, S) \neq I_{G_2}$, where I_{G_2} denotes the identity element of group G_2;
3) Computable: There is an efficient algorithm to compute $e(R, S)$ for all $R, S \in G_1$.

TABLE I: Notation

$\mathbb{F}_p$	prime finite field	p	odd prime number
$E(\mathbb{F}_p)$	elliptic curve defined over the field $\mathbb{F}_p$	$\mathcal{O}$	the point at infinity
G	the group of elements formed by the points on the elliptic curve $E(\mathbb{F}_p)$	P	generator of G
G_1	cyclic additive group of order q	Q	generator of G
G_2	cyclic multiplicative group of order q	R	point on curve $E(\mathbb{F}_p)$
Q_{PKG}	public key of Public Key Generator (PKG)	s_{PKG}	private key of PKG
$\mathcal{A}_i$	adversary in Certificateless Signature Scheme (CLS)	$\mathcal{C}$	challenger in CLS
H	secure hash function, $\mathsf{H}: \{0,1\}^* \times G_1 \rightarrow G_1$	σ	digital signature
h	secure hash function $\mathsf{h}: \{0,1\}^* \times G_1 \rightarrow \mathbb{Z}_q^*$	m	message

C. Intractable Problems

Let G_1 be a cyclic additive group generated by P, whose order is a prime q. Assume that the inversion and multiplication in G_1 can be computed efficiently. To prove the security of our schemes, We need the following intractable problems in G_1:

- Discrete Logarithm Problem (DLP): Given two elements $R, S \in G_1$, to find an integer $n \in \mathbb{Z}_q^*$, such that $S = nR$, whenever such an integer exists.
- Computational Diffie-Hellman Problem (CDHP): Given P, aP, bP for a, $b \in \mathbb{Z}_q^*$, to compute abP.
- Decisional Diffie-Hellman Problem (DDHP): Given P, aP, bP, cP for a, b, $c \in \mathbb{Z}_q^*$ to decide whether $c \equiv ab \bmod q$.
- Pairing Inversion Problem (PIP)[37]: Given a pairing e and a value $c \in \mathbb{Z}_q^*$, find $R, S \in G_1$ with $e(R, S) = c$.

III. Design Basis: Certificateless Signature Scheme

This section presents our new certificateless signature scheme, laying down a design foundation for our remote anonymous authentication protocols presented in Section IV.

A. Our New Certificateless Signature Scheme

A CLS scheme primarily consists of six algorithms: Setup, Set-Partial-Private-Key, Set-Partial-Public-Key, Partial-Private-Key-Extract, CL-Sign and CL-Verify, which are specified as follows.

Setup: Let $(G_1, +)$ and $(G_2, \cdot)$ denote cyclic groups of prime order $q > 2^l$, where l is the security parameter. Let P be a generator of G_1 and $e: G_1 \times G_1 \rightarrow G_2$ be a pairing operator that satisfies the properties of *Bilinear* and *Non-degenerate*. PKG selects two secure hash functions $\mathsf{H}: \{0,1\}^* \times G_1 \rightarrow G_1$ and $\mathsf{h}: \{0,1\}^* \times G_2 \rightarrow \mathbb{Z}_q^*$. It picks a random integer $s_{PKG} \in \mathbb{Z}_q^*$, as its private key – the master key and computes $Q_{PKG} = s_{PKG}P$, as its public key. PKG then publishes $\{l, G_1, G_2, q, P, e, \mathsf{H}, \mathsf{h}, Q_{PKG}\}$ as the system parameter, while s_{PKG} is kept secret.

Set-Partial-Private-Key: The signer also selects a random integer $s_1 \in \mathbb{Z}_q^*$, as his partially secret key.

Set-Partial-Public-Key: The signer computes $Q_1 = s_1 P$, as his partially public key.

Partial-Private-Key-Extract: This algorithm is performed by PKG when a signer requests the secret key corresponding to his identity. Suppose the signer's identity is given by the string id, which is the other partially public key. The other partially secret key of the identity is then given by $S_2 = s_{PKG}Q_2$, where $Q_2 = \mathsf{H}(id, Q_1)$. It is computed by PKG and distributed to the signer in a secret channel. For a signer, $\langle id, Q_1 \rangle$ is his public key and $\langle s_1, S_2 \rangle$ is his private key. The extraction step is typically done once for each identity.

CL-Sign: To sign a message m, the signer chooses a random integer $k \in \mathbb{Z}_q^*$ and computes as follows:

$$1. \quad r = e(Q_2, Q_{PKG})^k \tag{1}$$

$$2. \quad v = \mathsf{h}(m||r, P) \tag{2}$$

$$3. \quad U = kS_2 - vs_1Q_2 \tag{3}$$

The pair $(v, U) \in (\mathbb{Z}_q^*, G_1)$ is then taken as the signature.

CL-Verify: On receiving a message m and signature $\langle v, U \rangle$, the verifier performs in the following way:

$$1. \quad \text{Computes} \quad Q_2 = \mathsf{H}(id, Q_1) \tag{4}$$

$$2. \quad \text{Accepts the signature if and only if}$$
$$v = \mathsf{h}(m||e(U, P) \cdot e(Q_2, Q_1)^v, P). \tag{5}$$

It is straightforward to check that the verification equation holds for a valid signature. We can also easily prove that our proposed CLS scheme satisfies completeness:

$$\begin{aligned} v &= \mathsf{h}(m||e(U, P) \cdot e(Q_2, Q_1)^v, P) \\ &= \mathsf{h}(m||e(kS_2 - vs_1Q_2, P) \cdot e(Q_2, vs_1P), P) \\ &= \mathsf{h}(m||e(ks_{PKG}Q_2, P), P) \\ &= \mathsf{h}(m||r, P) \end{aligned} \tag{6}$$

B. Security Proof of Our New CLS Scheme

In this part, we prove that our new CLS is existentially unforgeable against adaptively chosen message attacks in the random oracle model [38] based on the hardness of CDHP. As defined in [31], [35], [39], we supposed there is an adversary $\mathcal{A}$ attempts to forge a valid signature with the help of PKG. The proof details can be shown as following.

Theorem 1. *The proposed CLS scheme is existentially unforgeable against adaptively chosen message attack of adversary $\mathcal{A}$ in the random oracle model, assuming the hardness of the CDHP.*

Proof. Suppose $\mathcal{A}$ is a probabilistic polynomial time Turing machine whose input only consists of public data. It can break

the proposed CLS scheme with non-negligible probability. Let H and h be random oracles. We assume that $\mathcal{A}$ can calculate a piece of additional information S_2 with the master key s_{PKG}. $\mathcal{C}$ gives the parameters $\{l, G_1, G_2, q, P, e, \mathsf{H}, \mathsf{h}, Q_{PKG}\}$ and $\langle id, Q_1, S_2\rangle$ to $\mathcal{A}$. $\mathcal{C}$ attempts to simulate all the oracles to obtain s_1Q_2 to have the same ability of signing arbitrary message m as the real signer. In particular, $\mathcal{A}$ can query as follows:

– H-Queries: $\mathcal{A}$ can query the random oracle H at any time. $\mathcal{C}$ simulates the random oracle by keeping a list of couples $\langle \top_i, Q_{(2,i)}\rangle$ called $\mathsf{L_H}$, where $\top_i$ is a couple of $\langle id_i, Q_{(1,i)}\rangle$. When the oracle is queried with input $\top$, $\mathcal{C}$ responds as follows:

1) If the query $\top$ is already in the item of $\langle \top, Q_{(2,i)}\rangle$ in $\mathsf{L_H}$, $\mathcal{C}$ outputs $Q_{(2,i)}$.
2) Otherwise, $\mathcal{C}$ selects a random $Q_2 \in G_1$, outputs Q_2 and adds $\langle \top, Q_2\rangle$ to $\mathsf{L_H}$.

– Extract-Queries: $\mathcal{A}$ can query the partially private key of any public key $\langle id_i, Q_{(1,i)}\rangle$. $\mathcal{C}$ outputs the partially private key $S_{(2,i)}$ corresponding to identity id_i by running algorithm Partial-Private-Key-Extract.

– h-Queries: $\mathcal{A}$ can query the random oracle h at any time. $\mathcal{C}$ simulates the random oracle by keeping a list of couples $\langle \perp_i, v_i\rangle$ that is called $\mathsf{L_h}$, where $\perp_i$ is a couple of $\langle x_i, Y_i\rangle$, where $x_i \in \{0,1\}^*$ and $Y_i \in G_1$. When the oracle is queried with an input $\perp$, $\mathcal{C}$ responds as follows:

1) If the query $\perp$ is already in the item of $\langle \perp, v_i\rangle$ in $\mathsf{L_h}$, $\mathcal{C}$ outputs v_i.
2) Otherwise $\mathcal{C}$ selects a random $v \in \mathbb{Z}_q^*$, outputs v and adds $\langle \perp, v\rangle$ to $\mathsf{L_h}$.

– CL-Sign-Queries: $\mathcal{C}$ simulates the signature oracle by responding to the signature query of any message m, and answers the query as follows:

1) $\mathcal{C}$ picks up a random $U \in G_1$ and $v \in \mathbb{Z}_q^*$ where v is not equal to any existing output of h oracle.
2) $\mathcal{C}$ computes $r = e(U, P) \cdot e(Q_2, Q_1)^v$. If $\perp = \langle m||r, P\rangle$ equals to any previous input of h oracle, then returns to step 1).
3) $\mathcal{C}$ adds $\langle \perp, v\rangle$ to $\mathsf{L_h}$.
4) $\mathcal{C}$ outputs $\langle v, U\rangle$ as the signature for message m.

Thus, the valid triple $\langle r, v, U\rangle$ can be generated without knowing the partially private key s_1. The signing oracle, simulated by $\mathcal{C}$, has high quality; $\mathcal{A}$ is fully satisfied with the CL-Sign-Queries' answers. It can fully exert its forgery ability.

Eventually, with non-negligible probability, $\mathcal{A}$ outputs a signature $\sigma = \langle r, v, U\rangle$ with a message $m \in M$, where $\text{CL-Verify}_{(id,Q_1)}(m, v, U) = True$. In this case, $\mathcal{A}$ generates v through h-Queries, S_2 through Extract-Queries with input $\langle id, Q_1\rangle$, but it does not make Sign-Queries with input m.

$\mathcal{C}$ then replays the process so that $\mathcal{A}$ should produce two valid signatures $\sigma = \langle r, v, U\rangle$ and $\sigma' = \langle r, v', U'\rangle$ with $v \neq v'$, naturally leading to the following equations:

$$\begin{left}\left\{\begin{array}{l} U = kS_2 - vs_1Q_2 \\ U' = kS_2 - v's_1Q_2 \end{array}\right. \\ \Rightarrow \quad R_1 = s_1Q_2 = (v' - v)^{-1}(U - U')\end{left} \tag{7}$$

Using $\langle R_1, S_2\rangle$, $\mathcal{C}$ can generate a valid signature $\langle v, U\rangle$ for any message m, where $v = \mathsf{h}(m, e(Q_2, kQ_{PKG})), U = kS_2 - vR_1$ and k is chosen randomly in $\mathbb{Z}_q^*$, just as the real signer uses $\langle s_1, S_2\rangle$. $\mathcal{C}$ can solve the CDHP as follows in the above equations:

$$\left\{\begin{array}{l} Q_1 = aP = s_1P \\ Q_2 = bP \end{array}\right. \Rightarrow abP = R_1 = s_1Q_2 \tag{8}$$

This obviously contradicts the hardness of the CDHP. □

TABLE II: Comparison of Computational Complexity

Algorithm	Sign			Verify		
	P	E	M	P	E	M
AP03 [31]	1	1	2	4	1	1
CZK03 [32]	0	0	3	4	0	2
LCS05 [33]	0	0	2	4	0	2
GS05 [34]	0	0	2	3	0	1
ZWXF06 [35]	0	3	0	4	0	0
WLT09 [36]	0	1	1	3	0	1
Our scheme	1	1	2	2	1	0

Note: "P" – the number of pairing operations; "E" – the number of exponentiations in G_2;
"M" – the number of multiplications in G_1.

C. Computational Complexity Analysis

Our scheme has some pre-computations, making our scheme efficient. Before signing any message, the user can pre-compute $e(Q_2, Q_{PKG})$ for $r = e(Q_2, Q_{PKG})^k$ in step 1 and s_1Q_2 for $U = kS_2 - vs_1Q_2$ in step 3. Similarly, before verifying any signature, the verifier can pre-compute $e(Q_2, Q_1)$ for $r = e(U, P)e(Q_2, Q_1)^v$ in step 1 and $Q_2 = \mathsf{H}(id, Q_1)$. These pre-computations can be used in the future protocols design for a special purpose.

Generally, the pairing operation is several times more complex than the scalar multiplication in G_1. Thus, the number of pairing operations is a key performance metric. We then carefully examined the operational efficiency of our scheme and compared it to those of the existing schemes. Table II summarized the results, in which "P" denotes the number of pairing operations, "E" denotes the number of exponentiations in G_2, and "M" denotes the number of multiplications in G_1.

The other operations are omitted from the table due to their trivial computational cost. It is easily observed that our scheme does not perform better than [31] and even worse than [32], [33], [34], [35], [36] for solely signing operation. However, our verification algorithm is significantly simplified. Our scheme can obtain higher efficiency as a whole, since a signature scheme generally contains a single-time-sign and multi-time-verify.

IV. Our Authentication Protocols for WBANs

To meet the unique security demands of wireless body area networks, we use our new certificateless signature scheme to design remote anonymous authentication protocols, which can preserve the anonymity of remote WBAN clients and save computational overhead.

A. Design Objectives

In general, we assume that the authentication protocols are deployed in distributed WBAN application environments equipped with *public key cryptographic primitives*. This implies the existence of some authority mechanisms, such as the certification authority (CA) that can generate and certify cryptographic keys for different purposes. The patients, as well as healthcare service providers, must contact with a CA in advance for key distribution. Because the keys are individual-specific, it avoids *one body authentication problem*, i.e. ensuring that the body sensors in a WBAN collect data about one individual and not multiple individuals [40]. Moreover, we assume anonymity to be an *fundamental property* and *service on demand*, and there exist *active adversaries* who attempt to subvert the anonymous authentication system by recovering or misusing the real identities of WBAN clients. Because in these remote health-care application scenarios, the doctors and nurses only need to know the bio-information of the patient, rather than other private information such as name and ID number, while legitimate users should be allowed to preserve their sensitive information to the maximum extent. Remote anonymous authentication schemes in insecure channels are required to achieve this.

Based on the assumptions and taking into account the special characteristics of WBANs, we intend to design such an authentication scheme which can do the following,

- Achieve anonymity regardless of particular operational environments or WBAN network infrastructure;
- Provide services for a WBAN client more than once;
- Operate with high efficiency while incurring negligible computational cost.

B. Design Architecture

There are three types of participants involved in the authentication protocol, as shown in Figure 2: WBAN client, network manager (NM for short), and application provider (AP for short). In particular, WBAN clients refer to the users who use certain WBAN terminals or applications such as PDA, smart phone, biosensor or medical device to regularly access various medical services that are offered by AP, including patient monitoring, physician consult, and so on. APs can be hospital, clinic, physician and even weather forecast station. In addition, there is an NM which serves as key generator. It is not required to be a strong trusted third party (TTP), because it is only used to issue one half of the private key of a legitimate client, while this half of private key alone is not sufficient to impersonate legitimate clients. This is a desirable property in practice. For example, a commercial organization can be delegated as private key generator for managing an enrollment system.

C. Preliminary Version Authentication Protocol

In principle, our protocols take the new CLS scheme proposed in Section III-A as design basis, in which NM firstly generates an *account index* for each requesting WBAN client and uses it for signature generation and verification. A signature is generated using the account index together with the specified rights including prescriptive period and service type for the requesting client. To log in, a client needs to send its signature of the message issued by NM, along with the account index, to the corresponding AP, which then verifies the client's signature using account index and NM's signature by NM's public key. It is obvious that the role of AP is only to verify the generated signature, and the information in hand does not allow it to recover the real identity of the client. By assuming that the requested AP and requesting client are synchronous in time, our protocol can be formally described as follows:

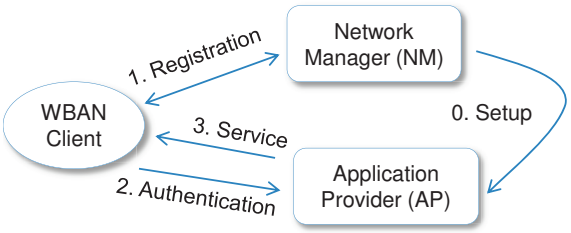

Fig. 2: Participants and working flow in anonymous authentication protocol

Initialization: System is setup by NM, generating keys and establishing an enrollment system. In this step, given security parameter l, NM determines its public/private key pair $\langle Q_{NM}, s_{NM}\rangle$, where $Q_{NM} = s_{NM}P$, and publicizes the system parameters $\{l, G_1, G_2, q, P, e, \mathsf{H}, \mathsf{h}, Q_{NM}\}$, as described in Section III-A. We suppose that each AP also has a long-term key pair $\langle Q_{AP}, s_{AP}\rangle$ where $Q_{AP} = s_{AP}P$.

Registration: A WBAN client with identifier C must perform this operation with NM in order to access an AP of interest. The following steps should be done in turn,

1) A legitimate client chooses one partial private key while obtain another partial private key using algorithm Partial-Private-Key-Extract described in Section III-A,
2) NM creates an account in the form $\langle C, ind_{C_v}, ind_{C_s}, right\rangle$ for client C, where $ind_{C_v} = e(Q_2, Q_1)$ is *verifying index*, $ind_{C_s} = e(Q_2, Q_{NM})$ is *signing index* for algorithm CL-Sign. Also, $right$ indicates auxiliary information such as service type and prescriptive period.
3) NM issues a $ticket = \langle m, \sigma\rangle$ to client C, where $m = right||ind_{C_v}$ and σ is the corresponding signature on m.

In the same way, client C can store a group of Q_{AP} at the mobile device for different APs. Two predetermined functions, $\mathsf{h}(\cdot)$ (defined in Section III-A) and message authentication code, denoted as $\mathsf{MAC}_{(\cdot)}(\cdot)$, are loaded simultaneously for access.

Authentication: the WBAN client performs the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.

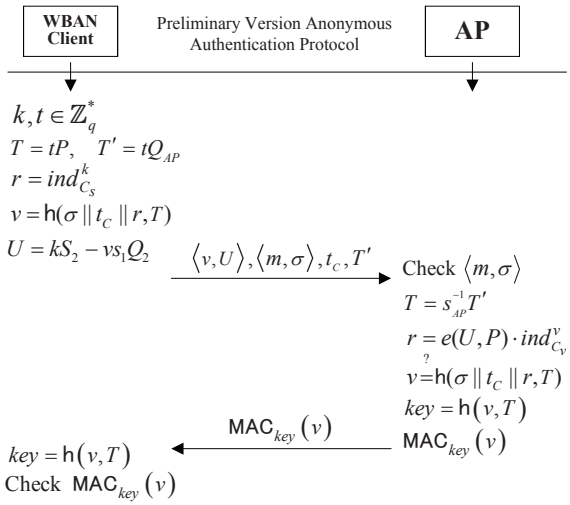

Fig. 3: Preliminary version authentication protocol

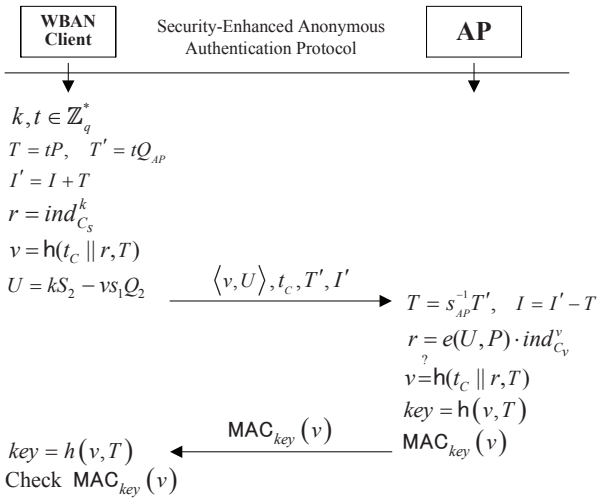

Fig. 4: Security-enhanced authentication protocol

following steps to anonymously authenticate him/herself to the AP of interest,

1) Select at random $k, t \in \mathbb{Z}_q^*$, and compute $T = tP$ and $T' = tQ_{AP}$.
2) Pick up the current time t_c of the requesting WBAN terminal. Then, compute $v = \mathsf{h}(\sigma||t_c||r, T)$.
3) Compute $U = kS_2 - vs_1Q_2$.
4) Compute the session key $key = \mathsf{h}(v, T)$.
5) Send a service request message $Req = (v, U, m, \sigma, t_c, T')$ to the AP.

When the AP receives $Req = (v, U, m, \sigma, t_c, T')$, it checks the validity of $\langle m, \sigma \rangle$ and t_c. The AP rejects the request if σ on m and t_c are not valid. Otherwise, the AP does the following:

1) Compute $r = e(U, P) \cdot ind_{C_v}^v$.
2) Compute $T = s_{AP}^{-1} T'$ with its private key s_{AP}.
3) Verify $v \stackrel{?}{=} \mathsf{h}(\sigma||t_c||r, T)$.
4) Compute the session key $key = \mathsf{h}(v, T)$.
5) Compute $\mathsf{MAC}_{key}(v)$ as the reply.
6) Reply to C's service request by sending back $\mathsf{MAC}_{key}(v)$.

On receiving the reply from the AP, C checks the integrity of $\mathsf{MAC}_{key}(v)$ with session key key. C will quit the current session if the check produces a negative result; otherwise, C authenticates the AP and uses key as the session key with the AP in future communications. The message flow of the anonymous authentication phase is described in Figure 3.

D. Security-Enhanced Authentication Protocol

In the preliminary version, all the requested authentication information, including the account index and the corresponding right of the client, are carried in the request massage. This may allow one sophisticated adversary to determine whether two different sessions are initiated by a same client, and may also allow NM to trace the client's real identity from the session information. To remedy this vulnerability, we propose a security-enhanced anonymous authentication protocol, which also consists of three phases: initialization, registration, and remote anonymous authentication. More formally,

Initialization: System setup (same as preliminary version).

Registration: This process is as same as preliminary version but NM issues $\langle I, ind_{C_v}, right \rangle$ to AP and client C, where $I = ind_{C_v} P$, instead of sending a $ticket = \langle m, \sigma \rangle$ to client C.

Authentication: The WBAN client performs the following steps to anonymously authenticate him/herself to the requested AP:

1) Select at random $k, t \in \mathbb{Z}_q^*$, and compute $T = tP$, $T' = tQ_{AP}$ and $I' = I + T$.
2) Pick up the current time t_c of the requesting WBAN terminal, and then, compute $v = \mathsf{h}(t_c||r, T)$.
3) Compute $U = kS_2 - vs_1Q_2$.
4) Compute the session key $key = \mathsf{h}(v, T)$.
5) Send a service request message $Req = (v, U, t_c, T', I')$ to the AP.

When the AP receives $Req = (v, U, t_c, T', I')$, it checks the validity of t_c. The AP rejects the request if t_c is invalid. Otherwise, AP does the following:

1) Compute $T = s_{AP}^{-1} T'$ with its private key s_{AP} and $I = I' - T$.
2) Find ind_{C_v} with I in the database and compute $r = e(U, P) \cdot ind_{C_v}^v$.
3) Verify $v \stackrel{?}{=} \mathsf{h}(t_c||r, T)$.
4) Compute the session key $key = \mathsf{h}(v, T)$.
5) Compute $\mathsf{MAC}_{key}(v)$ as the reply.
6) Reply to C's service request by sending back $\mathsf{MAC}_{key}(v)$.

On receiving the reply from the AP, C checks the integrity of $\mathsf{MAC}_{key}(v)$ with session key key. C will quit the current session if the check produces a negative result; otherwise, C authenticates the AP

and uses key as the session key with the AP in future communications. Figure 4 describes the message flow of the anonymous authentication phase.

V. Security Analysis

This section presents the security analysis of our authentication protocols. Our protocols ensure that NM can only generate partial private keys, avoiding it impersonating as legitimate client. This property makes NM more applicable in real WBAN network application scenarios. In what follows, we examine the proposed authentication protocols in terms of six security properties of particularly concern.

Anonymity means that an adversary $\mathcal{A}_I$ cannot obtain the real identity of any WBAN client based on the existing communication. Now we formalize a game: when an oracle $\mathcal{O}_\Pi(id)$ outputs a session message Π with the real identity id of a legitimate client, $\mathcal{A}_I$ outputs id' with the help of AP.

Definition 1. *An authentication scheme achieves anonymity, if for any probabilistic polynomial time adversary $\mathcal{A}_I$, $\mathbf{Pr}[\Pi \leftarrow \mathcal{O}_\Pi(id), id' \leftarrow \mathcal{A}_I : id' = id]$ is negligible.*

Theorem 2. (Anonymity) *The proposed two authentication protocols meet anonymity, assuming the hardness of PIP described in Section II-C.*

Proof. Here we only give detailed proof of anonymity for the security-enhanced version due to space limitations. The anonymity of the preliminary version can be proved in the same way. Suppose adversary $\mathcal{A}_I$ is a probabilistic polynomial time Turing machine whose input consists of public data. It can find the true id and Q_1 corresponding to any existing session massage with non-negligible probability after getting enough experience. Simulator $\mathcal{C}$ has strong ability to imitate any state of whole communication environment and share all information with AP, who maybe a malice AP. When $\mathcal{C}$ receives a PIP instance $ind_{C_v} = e(Q_2, Q_1)$. Its goal is to compute $Q_2 \in G_1$ and $Q_1 \in G_1$. $\mathcal{C}$ gives the parameters $\{l, G_1, G_2, q, P, e, \mathsf{H}, \mathsf{h}, Q_{PKG}\}$ and ind_{C_v} to $\mathcal{A}_I$. It attempts to simulate the challenger by simulating all the oracles to obtain $\langle id, Q_1\rangle$ of client C. In particular, $\mathcal{A}_I$ can query as follows:

– h-Queries: $\mathcal{A}_I$ can query the random oracle h at any time. $\mathcal{C}$ simulates the random oracle by keeping a list of couples $\langle \perp_i, v_i\rangle$ that is called $\mathsf{L_h}$, where $\perp_i$ is a couple of $\langle x_i, Y_i\rangle$, where $x_i \in \{0,1\}^*$ and $Y_i \in G_1$. When the oracle is queried with an input $\perp$, $\mathcal{C}$ responds as follows:

1) If the query $\perp$ is already in the item of $\langle \perp, v_i\rangle$ in $\mathsf{L_h}$, $\mathcal{C}$ outputs v_i.
2) Otherwise $\mathcal{C}$ selects a random $v \in \mathbb{Z}_q^*$, outputs v and adds $\langle \perp, v\rangle$ to $\mathsf{L_h}$.

– Extract-Queries:$\mathcal{A}_I$ can query ind_{C_v} of any (T', I'). $\mathcal{C}$ computes $T = s_{AP}^{-1}T'$ and $I = I' - T$. If I can be found in the database, $\mathcal{C}$ outputs ind_{C_v}. Otherwise, it outputs "error".

– Initial-Queries: $\mathcal{C}$ simulates the initial massage sent by any WBAN client C_i with $\langle Q_{(1,i)}, Q_{(2,i)}\rangle$ and t_c. $\mathcal{C}$ answers the query as follows:

1) $\mathcal{C}$ picks up a random $t \in \mathbb{Z}_q^*$, $U \in G_1$ and $v \in \mathbb{Z}_q^*$ where v is not equal to any existing output of h oracle.
2) $\mathcal{C}$ computes $r = e(U, P) \cdot e(Q_{(2,i)}, Q_{(1,i)})^v$ and $T = tP$. If $\perp = \langle t_c \| r, T\rangle$ equals to any previous input of h oracle, then returns to step 1.
3) $\mathcal{C}$ adds $\langle \perp, v\rangle$ to $\mathsf{L_h}$.
4) $\mathcal{C}$ computes $T' = tQ_{AP}$, $I' = I + T$ and outputs $(\langle v, U\rangle, t_c, T', I')$ as the initial message sent from client C.

– Respond-Queries: $\mathcal{C}$ simulates the respond massage sent by AP with $(\langle v, U\rangle, t_c, T', I')$. $\mathcal{C}$ answers the query as follows:

1) $\mathcal{C}$ computes $T = s_{AP}^{-1}T'$ and $I = I' - T$. If $\mathcal{C}$ can find ind_{C_v} corresponding to I in the database and $\langle v, U\rangle$ is legal, go to step 2. Otherwise, $\mathcal{C}$ outputs "error".
2) $\mathcal{C}$ computes $key = \mathsf{h}(v, T)$.
3) $\mathcal{C}$ outputs $\mathsf{MAC}_{key}(v)$ as the respond message sent from AP.

Thus, the initial message can be generated without knowing the private key $\langle s_1, S_2\rangle$ of client C. All oracles, simulated by $\mathcal{C}$, has high quality; $\mathcal{A}_I$ is fully satisfied with the all queries' answers. It can fully exert its ability.

Eventually, given an input of $(\langle v, U\rangle, t_c, T', I')$, adversary $\mathcal{A}_I$,with non-negligible probability, outputs a legal pair of $\langle id, Q_1\rangle$ of client C. Here, $(\langle v, U\rangle, t_c, T', I')$ is not any output of Initial-Queries. $\mathcal{C}$ then computes $Q_2 = \mathsf{H}(id, Q_1)$, so that it successfully outputs $\langle id, Q_1\rangle$ with the equation $ind_{C_v} = e(Q_2, Q_1)$, which obviously contradicts the hardness of the PIP. □

Unlinkability [21], [22], [23], [25] means that an adversary $\mathcal{A}_{II}$ cannot distinguish WBAN clients based on their communication. This means that the all session messages generated by clients should not leak any information to $\mathcal{A}_{II}$ that allows $\mathcal{A}_{II}$ to trace them. Now , similar to [25], we formalize a **UL Game**: when an oracle $\mathcal{O}_\Pi(b)$ for $b \in (0,1)$ outputs two session messages $\langle \Pi_1, \Pi_2\rangle$ with two identical $(b = 0)$ or two different $(b = 1)$ legitimate clients, $\mathcal{A}_{II}$ guesses $b' \in (0,1)$ with the help of NM.

Definition 2. *An authentication scheme achieves unlinkability, if for any probabilistic polynomial time adversary $\mathcal{A}_{II}$ in above UL Game, $\mathbf{Adv}_{\mathcal{A}_{II}} = |\mathbf{Pr}[\langle \Pi_1, \Pi_2\rangle \leftarrow \mathcal{O}_\Pi(b), b' \leftarrow \mathcal{A}_{II} : b' = b] - \frac{1}{2}|$ is negligible.*

Theorem 3. (Unlinkability) *The security-enhanced anonymous authentication protocol achieves unlinkability, assuming the hardness of DDHP described in Section II-C.*

Proof. Suppose adversary $\mathcal{A}_{II}$ is a probabilistic polynomial time Turing machine whose input consists of public data. It can represent two identical or two different WBAN client from two given session massages with non-negligible probability after getting enough experience. Simulator $\mathcal{C}$ has strong ability to imitate any state of whole communication environment and share all information with NM, who maybe a malice NM. When $\mathcal{C}$ receives a DDHP instance (aP, bP, Q). Its goal is to decide if $Q = abP$. $\mathcal{C}$ gives the parameters $\{l, G_1, G_2, q, P, e, \mathsf{H}, \mathsf{h}, Q_{PKG}\}$ to $\mathcal{A}_{II}$. It attempts to simulate the challenger by simulating all the oracles. In particular, $\mathcal{A}_{II}$ can query as follows:

– h-Queries: Same as in Theorem 2.

– Extract-Queries:$\mathcal{A}_{II}$ can query any elements of $\langle id, Q_1, Q_2, ind_{C_v}, ind_{C_s}\rangle$ for having the others. If the

TABLE III: Comparison of security properties between different schemes

	HP[9]	YMW[10]	AME[11]	CHLS[12]	TWW[13]	YC[14]	CZKH[15]	LLZHS[16]	TFS[17]	Preliminary version	Enhanced version
P_1								$\surd$	$\surd$	$\surd$	$\surd$
P_2							$\surd$		$\surd$		$\surd$
P_3										$\surd$	$\surd$
P_4	$\rightleftarrows$	$\rightarrow$	$\rightleftarrows$	$\rightleftarrows$	$\rightleftarrows$	$\rightleftarrows$	$\rightleftarrows$	$(\rightleftarrows)$	$\rightarrow$	$\rightleftarrows$	$\rightleftarrows$
P_5	$\surd$			$\surd$	$\surd$	$\surd$	$\surd$	$\surd$		$\surd$	$\surd$
P_6	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$			$\surd$	$\surd$

Note P_x represents Theorem $(x+1)$, $\surd$ indicates that the property is satisfied, $\rightleftarrows$ and $\rightarrow$ denote that the protocol satisfies mutual authentication and one-way authentication respectively.

related information can be found in the database, $\mathcal{C}$ outputs it. Otherwise, $\mathcal{C}$ outputs "error".

– Initial-Queries: Same as in Theorem 2.
– Respond-Queries: Same as in Theorem 2.

Thus, the initial message can be generated without knowing the partial private key s_1 of client C. All oracles, simulated by $\mathcal{C}$, has high quality; $\mathcal{A}_{II}$ is fully satisfied with the all queries' answers. It can fully exert its ability.

Eventually, given two sessions of $(\langle v_1, U_1\rangle, t_{(c,1)}, T_1', I_1')$ and $(\langle v_2, U_2\rangle, t_{(c,2)}, T_2', I_2')$, adversary $\mathcal{A}_{II}$, with non-negligible probability, outputs "0" or "1" (*Note*: "0" means $I_1 = I_2$ and "1" means $I_1 \neq I_2$). Here, $(\langle v_1, U_1\rangle, t_{(c,1)}, T_1', I_1')$ and $(\langle v_2, U_2\rangle, t_{(c,2)}, T_2', I_2')$ are not any output of Initial-Queries. Without knowing $\langle a, b\rangle$, $\mathcal{C}$ then can solve a DDHP instance ($aP = s_{ap}P = Q_{ap}$, $bP = I_1' - I_2'$, $Q = T_1' - T_2'$) with the help of $\mathcal{A}_{II}$, because

$$\begin{aligned} & I_1 \stackrel{?}{=} I_2 \\ \Leftrightarrow \quad & I_1' - s_{ap}^{-1}T_1' \stackrel{?}{=} I_2' - s_{ap}^{-1}T_2' \\ \Leftrightarrow \quad & s_{ap}(I_1' - I_2') \stackrel{?}{=} T_1' - T_2' \\ \Leftrightarrow \quad & abP \stackrel{?}{=} Q \end{aligned} \tag{9}$$

This obviously contradicts the hardness of the DDHP. □

Theorem 4. (Immunity of key-escrow) *The two proposed protocols are constructed based on the new CLS scheme that can solve the inherent key-escrow problem in general ID-based signature schemes.*

Proof. This property can be obtained directly from Theorem 1. □

Theorem 5. (Mutual authentication) *The two proposed protocols achieve the property of mutual authentication.*

Proof. Only the requested AP can authenticate the accessing client by checking the client's signature $\langle v, U\rangle$, because $v = \mathsf{h}(\sigma||t_c||r, T)$ and $v = \mathsf{h}(t_c||r, T)$ in the two proposed authentications respectively are both based on T, which can only be recovered by AP. The client authenticates the AP by comparing the received $\mathsf{MAC}_{key}(v)$ to the result calculated by him/herself, because AP is the only one who can recover T from T' and then calculates the $key = \mathsf{h}(v, T)$ and $\mathsf{MAC}_{key}(v)$. If the client received a right $\mathsf{MAC}_{key}(v)$, the AP is the correct one the client wishes to access for service. Here this value is completely dependent on the time token t_c and random numbers k, t and can identity each authentication process uniquely. □

Theorem 6. (Session key establishment) *After successful access, both sides share the session key.*

Proof. Client C checks the $MAC_{key}(v)$ to authenticate the AP and agrees upon the session key. If the value is correct, the requested AP generates the correct $key = \mathsf{h}(v, T)$ with the recovered T. key is only shared by C and AP. The opponents cannot deduce key even if they eavesdrop all of the session information no matter in which protocol we proposed. □

Theorem 7. (Nonrepudiation) *After successful access, client C cannot deny that he/she has accessed the service provided by AP for the CLS signature $\langle v, U\rangle$.*

Proof. Client C is the unique signer who can generate a legal signature pair of $\langle v, U\rangle$. Even NM is unable to impersonate C to sign such a valid signature for Theorem 1. □

We carefully select nine existing schemes for comparative analysis and the results are summarized in Table III. We discuss the above six security properties in these schemes respectively, including two anonymities (P_1, P_2) and the other four security characters. In the first six schemes, the authentication protocols do not meet the anonymous property. The scheme in [15] only has the property P_2 in two anonymities. In [16], only anonymous property P_1 is satisfied, moreover the mutual authentication property can only be achieved under special conditions. The scheme in [17] meets both two anonymous properties, but it only provides one-way authentication and misses the properties P_3, P_5, P_6. From Table III, we can conclude that the new schemes achieve a higher security level with strict anonymity.

VI. Simulation-based Performance Validation

We are particularly concerned the computational complexity of our protocol in addition to the security properties. To validate that, we set up simulations and compare its run time with a number of typical schemes.

A. Simulation Setup

In this subsection, to evaluate the computation overhead of the proposed schemes, we first setup simulation hardware environment and quantify the computation time of the cryptographic operations used in the selected schemes. The simulation environment of AP is Windows XP OS over an Inter(R) Pentium IV 3.0GHz processor and 512MB memory. The hardware environment of the mobile WBAN client, such as a PDA, has a low-power high-performance 32-bit Inter(R) PXA270 624MHz processor and 128MB memory running Windows CE 5.2 OS. In addition, we set the public modulator

used in RSA signature to be 1024 bits. The pair operation is defined over a supersingular elliptic curve $y^2 = x^3 + x$. The run time of cryptographic primitives on AP is obtained by experiment, and that on the client terminal is estimated using the method in [41]. The simulations were run several times, and the results were averaged to compensate for the randomness. Table IV lists the run time of several cryptographic operations. In these schemes, the computation overhead is mainly due to the cryptographic operations of exponentiation in $\mathbb{Z}_q^*$, multiplication in $\mathbb{G}_1$ and pairing.

TABLE IV: Operating time on server and client

Operations	Server (*ms*)	Client (*ms*)
RSA sign	3.84	18.46
RSA verification	0.20	0.96
Exponentiation in $\mathbb{Z}_q^*$	13.21	63.51
Multiplication in $\mathbb{G}_1$	6.38	30.67
Hash in $\mathbb{G}_1$	3.04	14.62
Pairing	20.04	96.35

B. Results and Analysis

Table V and Figure 5 compare the run time of AP and the WBAN client between eleven authentication schemes. We separate the selected authentication schemes into two groups for convenience: a.) *without anonymity*; b.) *with anonymity*. Compared with the first group, our scheme does not clearly show better performance, but it achieves the certificateless and anonymous properties that consume computational resource. Within the second group, the run time of our scheme obviously outperforms schemes LLZHS [16] and TFS [17]. In CZKH [15], the scheme seems run a shorter time, but it costs more storage space and the anonymity property is weaker.

The results demonstrate that our designed protocol generally outperforms the others, offering a better tradeoff between the security properties of concern and the run time of APs and WBAN clients. These make it more suitable to wireless body area networks.

TABLE V: A comparison of running time between different schemes

Protocols	AP (*ms*)	Mobile Client (*ms*)	Round
HP[9]	13.61	146.44	3
YMW[10]	85.79	121.25	1
AME[11]	25.52	61.34	4
CHLS[12]	59.67	155.52	2
TWW[13]	55.88	122.68	2
YC[14]	25.52	122.68	2
CZKH[15]	32.80	92.02	2
LLZHS[16]	62.71	410.3	2
TFS[17]	79.26	190.53	3
Preliminary version	39.83	186.19	2
Enhanced version	39.63	186.19	2

VII. Conclusion and Future Work

In this paper, we presented two certificateless remote authentication protocols to preserve the privacy of potential WBAN users when they access network medical service through WBANs terminals. To design the protocols, we developed a novel certificateless signature scheme as a cryptographic primitive by carefully exploring the special characteristics of WBANs. We formally proved that our certificateless signature scheme has potential to achieve more desirable security properties with less computational cost than the existing schemes. One salient feature of our protocols is that medical application or service providers do not have privilege to reveal the true identity of users even given all the session information. Also, network manager cannot impersonate any legitimate users although it serves as PKG. Sound theoretic analysis, comparative studies and simulations were conducted to evaluate our proposed protocols, which outperformed most of the existing authentication schemes in terms of better tradeoff between security properties, computational overhead, as well as implementation and running time.

As what we have clearly analyzed in the paper, the run round of mutual authentication protocols have been reduced to two. Thus we attempt to design signature schemes with better tradeoff between computational overhead and efficiency, so that the computational complexity of the authentication protocols can be decreased as a whole. In addition, we intend to develop a set of realistic experimental scenarios to test our protocols. As such benchmark scenarios are yet available, it would benefit to the WBAN research community.

Acknowledgment

This work is supported by National Natural Science Foundation of China (No. 61100232, No.61001131), the Fundamental Research Funds for the Central Universities (No. K5051301012), the 111 Project (B08038), National Science and Technology Major Project of the Ministry of Science and Technology of China (No. 2013ZX03005007) and the National Research Foundation of Korea (NRF) grant funded by the Korea government(MEST)(No.2010-0018116). The authors would like to thank the anonymous referees and the associate editor for their constructive comments and suggestions that helped to improve the manuscript. The author would also like to thank Dr. R. Sun for the inspiring discussions and valuable suggestions during this research.

References

[1] Zimmerman, T. G., "Personal Area Networks: Near-field intrabody communication," *IBM Systems Journal*, vol. 35, no. 3/4, pp.609-617, 1996.

[2] Huan-Bang Li, Ken-ichi Takizawa, Bin Zhen, and Ryuji Kohno, "Body Area Network and Its Standardization at IEEE 802.15.MBAN," *Mobile and Wireless Communications Summit, 16th IST*, pp.1-5, 2007.

[3] C. Otto, A. Milenkovic, C. Sanders, and E. Jovanov, "System Architecture of A Wireless Body Area Sensor Network for Ubiquitous Health Monitoring," *Journal of Mobile Multimedia*, vol. 1, no. 4, pp. 307-326, 2006.

[4] M. Seyedi, B. Kibret, D. T. H. Lai, M. Faulkner, "A Survey on Intrabody Communications for Body Area Network Applications," *IEEE Trans. Biomedical Engineering*, 2013.

[5] B. Latré, B. Braem, I. Moerman, C. Blondia, and P. Demeester, "A survey on wireless body area networks," *Journal of Wireless Networks*, vol. 17, Issue 4, pp. 1-18, 2011.

[6] K. S. Kwak, U. Sana, U. Niamat, "An Overview of IEEE 802.15.6 Standard," in *Proc. ISABEL 2010*, pp.1-6, 2010.

[7] M. Chen, S. Gonzalez, A. Vasilakos, et al., "Body Area Networks: A Survey," *Mobile Networks and Applications*, vol. 16, pp. 171-193, 2011.

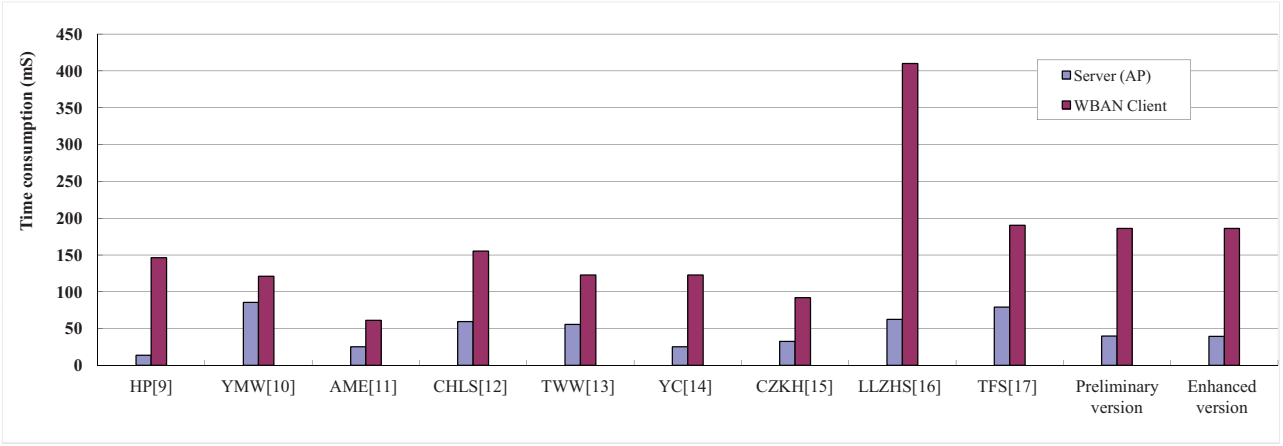

Fig. 5: A comparison of running time between different schemes

[8] J. Zhu and J. Ma, "A New Authentication Scheme with Anonymity for Wireless Environments," *IEEE Trans. Consumer Electronics*, vol. 50, no. 1, pp. 231-235, Feb. 2004.

[9] G. Horn and B. Preneel, "Authentication and payment in future mobile systems," in *Proc. 5th Eur. Symp. Res. Comput. Security*, pp. 277-293, 1998.

[10] C. Yang, W. Ma, and X. Wang, "Novel remote user authentication scheme using bilinear pairings," in *Proc. ATC'07*, LNCS vol. 4610, pp. 306-312, 2007.

[11] PE. Abichar, A. Mhamed, B. Elhassan, "A fast and secure elliptic curve based authenticated key agreement protocol for low power mobile communications," in *Proc. the 2007 international conference on next generation mobile applications, services and technologies*, pp. 235-240, 2007.

[12] K. Y. Choi, J. Y. Hwang, D. H. Lee, and I. S. Seo, "ID-based Authenticated Key Agreement for Low-Power Mobile Devices," in *Proc. ACISP 2005*, LNCS vol. 3574, pp. 494-505, 2005.

[13] Y. M. Tseng, T. Y. Wu, and J. D. Wu, "A mutual authentication and key exchange scheme from bilinear pairings for low power computing devices," in *Proc. COMPAC*, vol. 2, pp. 700-710, 2007.

[14] J. Yang, C. Chang, "An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem," *computers & security*, 28(2009), pp. 138-143, 2009.

[15] X. Cao, X. Zeng, W. Kou and L. Hu, "Identity-Based Anonymous Remote Authentication for Value-Added Services in Mobile Networks," *IEEE Trans. Vehicular Technology*, vol. 58, no. 7, pp. 3508-3517, Sep. 2009.

[16] R. Lu, X. Lin, H. Zhu, P. Ho, and X. Shen, "A Novel Anonymous Mutual Authentication Protocol With Provable Link-Layer Location Privacy," *IEEE Trans. Vehicular Technology*, vol. 58, no. 3, pp. 1454-1466, Mar. 2009.

[17] I. Teranishi, J. Furukawa, K. Sako, "k-Times Anonymous Authentication," *IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E92-A, no. 1, pp. 147-165, 2009.

[18] D. Hankerson, A. Menezes, S. Vanstone, "*Guide to Elliptic Curve Cryptography*," New York, Springer-Verlag, 2003.

[19] A. Juels, "RFID Security and Privacy: A Research Survey," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 381-394, Feb. 2006.

[20] S. Piramuthu, "Lightweight Cryptographic Authentication in Passive RFID-Tagged Systems," *IEEE Trans. System, Man, and Cybernetics-Pact C: Applications and Reviews*, vol. 38, no. 3, pp. 360-376, May. 2008.

[21] T. van Deursen, S. Mauw, and S. Radomirović, "Untraceability of RFID Protocols," in *Proc. WISTP 2008*, LNCS vol. 5019, Springer-Verlag, pp. 1-15, 2008.

[22] E. Cesena, H. Löhr, G. a Ramunno, A. Sadeghi, and D. Vernizzi, "Anonymous Authentication with TLS and DAA," in *Proc. TRUST 2010*, LNCS vol. 6101, Springer-Verlag, pp. 47-62, 2010.

[23] M. Burmester, T. Van Le, B. De Medeiros, and G. Tsudik, "Universally composable RFID identification and authentication protocols," *ACM Transactions on Information and System Security*, vol. 12, no. 4, artical 21, April 2009.

[24] P. Bichsel, J. Camenisch, T. Groβ, V. Shoup, "Anonymous credentials on a standard Java Card," in *Proc. of the 11th ACM Conference on Computer and Communications Security*, pp. 600-610, 2009.

[25] F. Armknecht, L. Chen, and A. Sadeghi, "Anonymous Authentication for RFID Systems," in *Proc. RFIDSec 2010*, LNCS vol. 6370, Springer-Verlag, pp. 158-175, 2010.

[26] Jian Ren, and Lein Harn, "An Efficient Threshold Anonymous Authentication Scheme for Privacy-Preserving Communications," *IEEE Trans. Wireless Commun.*, vol. 12, no. 3, pp. 1018-1025, March 2013.

[27] A. Shamir, "Identity-based Cryptosystems and Signature Schemes", in *Advances in Cryptology-Crypto'84*, LNCS vol. 196, Springer-Verlag, pp. 47-53, 1984.

[28] K. G. Paterson, "Id-based signatures from pairings on elliptic curves," *Electronics Letters*, 38(18), pp. 1025-1026, 2002.

[29] F. Hess, "Efficient Identity Based Signature Schemes Based on Pairings," in *Selected Areas in Cryptography-SAC'02*, LNCS vol. 2595, Springer-Verlag, pp. 310-324, 2003.

[30] J. C. Cha and J. H. Cheon, "An Identity-Based Signature from Gap Diffie-Hellman Groups," in *Public Key Cryptography-PKC'03*, LNCS vol. 2567, Springer-Verlag, pp. 18-30, 2003.

[31] S. S. Al-Riyami and K. G. Paterson, "Certificateless Public Key Cryptography," in *Advances in Cryptology-Asiacrypt'03*, LNCS vol. 2894, Springer-Verlag, pp. 452-473, 2003.

[32] X. Chen, F. Zhang, and K. Kim, "A New ID-based Group Signature Scheme from Bilinear Pairings," in *Proc. WISA'03*, LNCS vol. 2908, Springer-Verlag, pp. 585-592, 2003.

[33] X. Li, K. Chen, and L. Sun, "Certificateless Signature and Proxy Signature Schemes from Bilinear Pairings," *Lithuanian Mathematical Journal*, vol. 45, Springer-Verlag, pp. 76-83, 2005.

[34] M. C. Gorantla and A. Saxena, "An Efficient Certificateless Signature Scheme," in *Proc. CIS 2005, Part II*, LNAI vol. 3802, pp. 110-116, 2005.

[35] Z. Zhang, D. Wong, J. Xu, and D. Feng, "Certificateless Public-Key Signature: Security Model and Efficient Construction," in *Proc. ACNS 2006*, LNCS vol. 3989, Springer-Verlag, pp. 293-308, 2006.

[36] C. J. Wang, D. Y. Long, and Y Tang, "An Efficient Certificateless Signature from Pairings," *International Journal of Network Security*, vol. 8(1), pp. 96-100, 2009.

[37] S. Galbraith, F. Hess, and F. Vercauteren, "Aspects of Pairing Inversion," *IEEE Trans. Information Theory*, vol. 54, no. 12, pp. 5719-5728, 2008.

[38] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of Cryptology*, 13(2000), pp. 361-396, 2000.

[39] X. Huang, W. Susilo, Y. Mu, and F. Zhang, "On the security of certificateless signature schemes from asiacrypt 2003," in *Proc. CANS 2005*, LNCS vol. 3810, Springer-Verlag, pp. 13-25, 2005.

[40] C. Cornelius, and D. Kotz, "On Usable Authentication for Wireless Body Area Networks," in *Proc. 1st USENIX Workshop on Health Security and Privacy (HealthSec '10)*, 2010.

[41] K. Ren, W. Lou, K. Zeng, and P. J. Moran, "On broadcast authentication in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 6, no. 11, pp. 4136-4144, Nov. 2007.

PLACE PHOTO HERE

Jingwei Liu received a B.S. (majoring in Applied Mathematics) from Xidian University, Xi'an, China in 2001, and a M.S. (majoring in communication and information systems) from Xidian University in 2004 and a Ph.D. (majoring in communication and information systems) from Xidian University in 2007. He has published more than 20 papers in journals and conference proceedings. His research interests include information security, network security, and cryptography.

He is a member of IEEE and the Chinese Association for Cryptologic Research . He is now with the School of Telecommunications Engineering, Xidian University.

PLACE PHOTO HERE

Zonghua Zhang Zonghua Zhang is an Associate Professor of Institut Mines-Telecom of France. Previously, he worked as an expert researcher at the Information Security Research Center of National Institute of Information and Communications Technology (NICT), Japan, from April, 2008 to April, 2010. Even earlier, he spent two years for post-doc research at the University of Waterloo, Canada and INRIA, France after earning his Ph.D. degree in information science from Japan Advanced Institute of Science and Technology (JAIST) in 2006. Zonghua also obtained a M.Sc. degree in computer science and a B.Sc. degree in information science from Xidian University, China in 2003 and 2000 respectively. His research is centered on improving the quality of security services in various computer and communication networks, with current focus on cost-effective security management, privacy-preserving network forensics and reputation systems.

PLACE PHOTO HERE

Xiaofeng Chen received a B.E. in Mathematics from Northwest University, and a M.E. in Mathematics from Northwest University, and a Ph.D. in Cryptography from Xidian University, Xian, China, in 1997, 1999, and 2003, respectively.

He is a member of IEEE and IEICE. He is now with the School of Telecommunications Engineering, Xidian University. His research interests include information security, network security, and cryptography.

PLACE PHOTO HERE

Kyung Sup Kwak received a B.S. from Inha University, Inchon, Korea in 1977, and a M.S. from the University of Southern California in 1981 and a Ph.D. from the University of California at San Diego in 1988, under the Inha University Fellowship and the Korea Electric Association Abroad Scholarship Grants, respectively. From 1988 to 1989, he was a Member of Technical Staff at Hughes Network Systems, San Diego, California. From 1989 to 1990, he was with the IBM Network Analysis Center at Research Triangle Park, North Carolina. He has been with the School of Information and Communication, Inha University, Korea as a professor. He was Dean of the Graduate School of IT and Telecommunications from 2001 to 2002 at Inha University, Inchon, Korea. He is the current director of the UWB Wireless Communications Research Center, a key national IT research center in Korea. He has published 60 SCI journal papers, more than 200 conference and domestic papers, obtained 11 registered patents and had 35 patents pending. He has proposed 9 technical proposals on IEEE 802.15(WPAN) PHY/MAC. His research interests include multiple access communication systems, UWB radio systems and WPAN/WBAN, sensor networks. Mr. Kwak is a member of IEEE, IEICE, KICS and KIEE.