Hindawi Publishing Corporation
The Scientific World Journal
Volume 2013, Article ID 761240, 7 pages
http://dx.doi.org/10.1155/2013/761240

Research Article

An Efficient and Secure Certificateless Authentication Protocol for Healthcare System on Wireless Medical Sensor Networks

Rui Guo, Qiaoyan Wen, Zhengping Jin, and Hua Zhang

State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

Correspondence should be addressed to Rui Guo; grbupt@gmail.com

Received 21 February 2013; Accepted 2 April 2013

Academic Editors: Z. Cao, R. Lu, Q. Shi, and Q. Wu

Sensor networks have opened up new opportunities in healthcare systems, which can transmit patient's condition to health professional's hand-held devices in time. The patient's physiological signals are very sensitive and the networks are extremely vulnerable to many attacks. It must be ensured that patient's privacy is not exposed to unauthorized entities. Therefore, the control of access to healthcare systems has become a crucial challenge. An efficient and secure authentication protocol will thus be needed in wireless medical sensor networks. In this paper, we propose a certificateless authentication scheme without bilinear pairing while providing patient anonymity. Compared with other related protocols, the proposed scheme needs less computation and communication cost and preserves stronger security. Our performance evaluations show that this protocol is more practical for healthcare system in wireless medical sensor networks.

1. Introduction

Wireless medical sensor networks (WMSNs) have a capability of connecting patient with doctor by using of lightweight devices with limited memory, small and low power [1]. All these medical sensors collaborate together to collecting patient's physiological signals (e.g., blood pressure, blood sugar, and pulse oximeter) and send the collected data to health professional's hand-held devices (i.e., PDA, iPhone, iPad, etc.) via a wireless channel. The doctor uses these hand-held devices to observe the patient's real-time health condition.

However, the healthcare system on WMSN has many challenges, such as reliable data transmission, timely delivery of data, and power management [2]. Patient's privacy, a big concern for healthcare system, must be ensured at all sections on WMSN. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 established rules for healthcare provider that it is necessary to control who is accessing to medical server's (MS's) resources and whether they are authorized to do so. Therefore, a secure authentication scheme among patient, MS, and doctor is needed to protect the patient's privacy. So far many schemes that use cryptography have been proposed for this goal.

Most recently, Pu et al. [3] proposed a generic construction of smart card-based password authentication protocol for Telecare Medicine Information Systems (TMIS) and proved its security. Wu et al. [4] proposed a concrete efficient authentication scheme for TMIS. In their scheme, Wu et al. introduced a precomputing phase to compute costly and time-consuming exponential operations that are stored in a smart card. He et al. [5] pointed out that Wu et al.'s scheme could not resist impersonation attack and insider attack. Then, they proposed a more secure authentication scheme for TMIS. However, Wei et al. [6] demonstrated that both of Wu et al.'s scheme and He et al.'s scheme could not achieve a two-factor authentication. To overcome the weakness, Wei et al. proposed an improved authentication scheme for TMIS. Zhu [7] showed that Wei et al.'s scheme is vulnerable to an offline password guessing attack and also proposed a new authentication scheme for TMIS.

A common property of the above schemes is that the patient's identity ID is transmitted in plaintext on the public channel, which leads to impersonating attack and divulging

the patient's privacy. To avoid these risks, based on the identity-based public key cryptography (ID-PKC) [8], Das et al. [9] proposed a dynamic ID-based remote client authentication scheme without any verifier table. However, Chien and Chen [10] pointed out that it fails to protect the anonymity of a user, and Ku and Chang [11] demonstrated that it is vulnerable to impersonation attack.

To address the key escrow problem [8] in ID-based authentication scheme, Xiong et al. [12] and Zhang et al. [13] proposed two certificateless authentication schemes, respectively. Unfortunately, their schemes are based on the bilinear pairing. Chen et al. [14] pointed out that the relative computation cost of the bilinear pairing is approximately twenty times higher than that of the scalar multiplication over a cyclic additive group, which is unsuitable for healthcare system on WMSN with lower computation power. Therefore, it is vitally important to present a certificateless authentication without bilinear pairing in the healthcare system.

In this paper, based on certificateless public key cryptography (CL-PKC) [15], we propose a certificateless authentication scheme without bilinear pairing in healthcare system on WMSN. Our protocol can establish a secure channel in Patient-to-MS and Doctor-to-MS with high efficiency. The proposed scheme has the following advantages: (1) it limits the power of MS to resist the malicious MS attack. (2) It ensures that the serial numbers of patient's wearable medical sensor and doctor's hand-held device can be updated in time. (3) It avoids the management of digital certificate and releases the key escrow problem by MS. (4) It achieves the Girault trust level 3 [16] as in traditional public key infrastructure (PKI). (5) It provides patient anonymity. (6) It preserves the perfect forward secrecy. (7) It can resist replay attack and impersonation attack. (8) It does not need to operate the bilinear pairing.

The remainder of this paper is organized as follows. Section 2 addresses some preliminaries such as the computational assumptions, security model, Girault's trust level, and the model of certificateless authentication. Section 3 proposes a certificateless authentication scheme and analyzes its security. Section 4 compares the proposed scheme with some other related schemes. Finally, we conclude the paper in Section 5.

2. Preliminaries

In this section, we review some fundamental backgrounds required in this paper, namely, computational assumptions, security model, Girault's trust level, and the model of certificateless authentication.

2.1. Computational Assumptions. The security of our protocol is based on the following computational assumptions:

Discrete Logarithm (DL) problem: let G be a cyclic additive group of prime order p; P is a generator of G. Given $Q \in G$, find an integer $x \in Z_p^*$ such that $Q = xP$.

The DL assumption is that there is no polynomial time algorithm that can solve the DL problem with nonnegligible probability.

Computational Diffie-Hellman (CDH) problem: let G be a cyclic additive group of prime order p; P is a generator of G. Given $Q, R \in G$ and $Q = xP$, $R = yP$ for any $x, y \in Z_p^*$, compute xyP.

The CDH assumption is that there is no polynomial time algorithm that can solve CDH problem with nonnegligible probability.

2.2. Security Model. In WMSN, we assume that attackers are "internal adversary" and "external adversary." Internal adversary is a legitimate member of WMSN, such as the malicious MS who has the ability of obtaining the private key and eavesdropping the privacy information of patient. We also assume that the external adversary is divided into four kinds. Type I adversary may capture the transmitted information between patient and doctor. By this information, Type I adversary can get the specific identity of patient. Type II adversary has a capability of extracting the secret key from the transmitted information; it may derivate the secret key in previous session by using this extracted key. Type III adversary may eavesdrop the transmitted information in public channel. Then, it transmits this information again to deceive patient (or doctor) that is provided from the legitimate doctor (or patient). Type IV adversary may capture the transmitted information and extract some important data from it. After that, it may impersonate the patient (or doctor) to communicate with the legitimate doctor (or patient).

2.3. Girault's Trust Level. Girault's trust level provides the trust hierarchy for public key cryptography, which can be used to judge the creditability of the authority (e.g., the MS in the healthcare system on WMSN).

> Level 1: the authority knows (or can easily compute) users' secret keys. Therefore, the authority can impersonate any user at any time without being detected.
>
> Level 2: the authority does not knows (or cannot easily compute) users' secret keys. Nevertheless, it can still impersonate user by generating false guarantees (e.g., false public keys).
>
> Level 3: the authority cannot compute users' secret keys, and it can be proven that it generates false guarantees of users' if it does so.

According to these definitions, we can easily find that the conventional certificateless cryptography can reach Level 2, and a traditional PKI can achieve Level 3 while the ID-PKC falls into Level 1.

2.4. Model of Certificateless Authentication. A certificateless authentication scheme consists of six probabilistic, polynomial time algorithms: *Setup*, *User-Key-Generation*, *Partial-Key-Extract*, *Set-Private-Key*, *Set-Public-Key,* and *Authentication*. These algorithms are defined as follows.

Setup. Taking security parameter k as input, the authority returns a list of public parameters param and a randomly

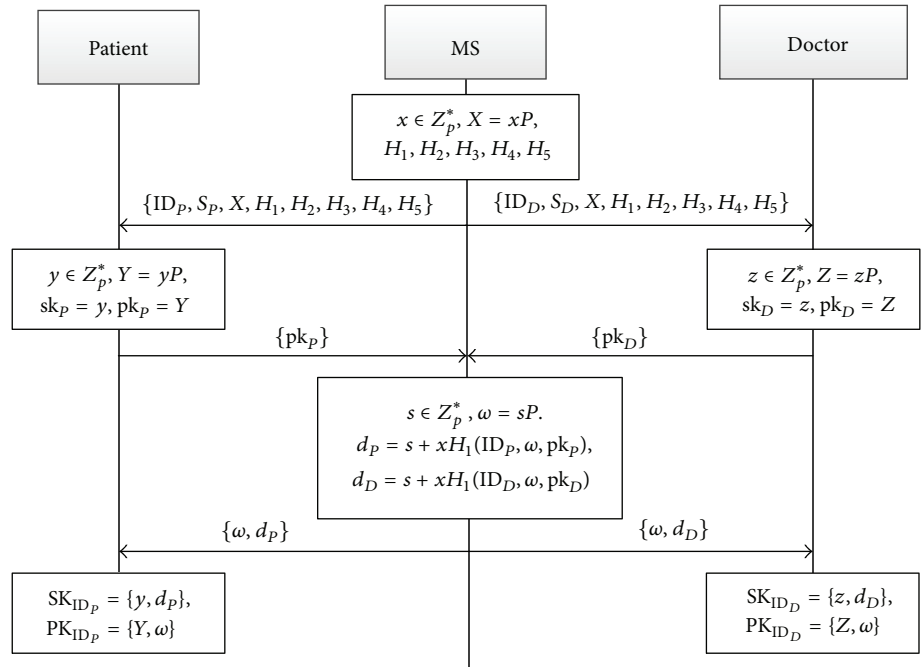

Figure 1: Initialization phase.

chosen master secret key msk.

User-Key-Generation. Taking a list of public parameters param as input, the user returns a secret key sk and a public key pk.

Partial-Key-Extract. Taking param, msk, user's identity ID, and pk received from the user as inputs, the authority returns a partial private key D_{ID} and a partial public key P_{ID}.

Set-Private-Key. Taking param, D_{ID}, and sk as inputs, the user returns a private key SK_{ID}.

Set-Public-Key. Taking param, P_{ID}, and pk as inputs, the user returns a public key PK_{ID}.

Authentication. Taking identity, private key of the sender, and a list of parameters param as inputs, the receiver verifies the legality of the sender by its public key.

This model is similar to that of [15] but with a crucial difference that *User-Key-Generation* algorithm must be run prior to the *Partial-Key-Extract* algorithm, which makes the scheme achieve Girault's trust level 3.

3. Our Protocol

In this section, we propose a certificateless authentication scheme without bilinear pairing to ensure the legality of Patient and Doctor by the MS.

3.1. Construction. The proposed scheme involves three entities: Patient, Doctor, and MS. Before Patient obtains the wearable medical sensor at the first time, MS presets the $\{\mathrm{ID}_P, S_P\} \in \{0,1\}^m$ and $\{\mathrm{ID}_D, S_D\} \in \{0,1\}^m$ into Patient's sensor and his/her doctor's health professional hand-held device through the secure channel as their identities and the serial numbers of equipments, respectively. Besides, these two serial numbers will be preserved secretly by themselves. The details of our certificateless authentication scheme are as follows.

We show the initialization phase of this protocol in Figure 1.

Setup. The MS generates a large prime p, which makes the DL and CDH problems in the cyclic additive group G with generator P of order p be intractable. Then, the MS picks $x \in Z_p^*$ uniformly at random, computes $X = xP$, and chooses hash functions

$$\begin{gathered} H_1 : \{0,1\}^m \times G^* \times G^* \longrightarrow Z_p^*, \\ H_2 : \{0,1\}^m \times \{0,1\}^m \times \{0,1\}^m \longrightarrow Z_p^*, \\ H_3 : G^* \longrightarrow \{0,1\}^m, \qquad H_4 : \{0,1\}^m \longrightarrow \{0,1\}^m, \\ H_5 : \{0,1\}^m \longrightarrow \{0,1\}^*, \end{gathered} \tag{1}$$

which can be achieved easily by collision-resistant hash function. Return $\{p, P, G, X, H_1, H_2, H_3, H_4, H_5\}$ as scheme parameters and the master secret key msk = $\{x\}$.

Patient/Doctor-Key-Generation. The Patient and the Doctor pick $y, z \in Z_p^*$ at random, compute $Y = yP$, $Z = zP$, and return $(\mathrm{sk}_P, \mathrm{pk}_P) = (y, Y)$ and $(\mathrm{sk}_D, \mathrm{pk}_D) = (z, Z)$, respectively.

Partial-Key-Extract. The MS picks $s \in Z_p^*$ at random and computes

$$\begin{aligned} \omega &= sP, \\ d_P &= s + xH_1\left(\mathrm{ID}_P, \omega, \mathrm{pk}_P\right), \\ d_D &= s + xH_1\left(\mathrm{ID}_D, \omega, \mathrm{pk}_D\right). \end{aligned} \tag{2}$$

Return $(P, D_{\mathrm{ID}_P}) = (\omega, d_P)$, $(P, D_{\mathrm{ID}_D}) = (\omega, d_D)$ as partial keys to be placed into Patient's sensor and the Doctor's hand-held device, respectively.

Set-Private-Key. The Patient sets $\mathrm{SK}_{\mathrm{ID}_P} = (\mathrm{sk}_P, D_{\mathrm{ID}_P}) = (y, d_P)$ as his/her private key, and the Doctor sets $\mathrm{SK}_{\mathrm{ID}_D} = (\mathrm{sk}_D, D_{\mathrm{ID}_D}) = (z, d_D)$ as his/her private key as well.

Set-Public-Key. Set $\mathrm{PK}_{\mathrm{ID}_P} = (\mathrm{pk}_P, \omega)$ and $\mathrm{PK}_{\mathrm{ID}_D} = (\mathrm{pk}_D, \omega)$ as the public keys of Patient and Doctor, respectively.

Now, we show the authentication phase in Figure 2.

Authentication

Step 1. The Patient picks the current time stamp t_P and computes

$$\begin{aligned} h_1 &= H_1\left(\mathrm{ID}_P, \omega, \mathrm{pk}_P\right), \qquad r_P = H_2\left(\mathrm{ID}_P, S_P, t_P\right), \\ \alpha_P &= \left(y + r_P\right) \cdot \left(h_1 X + \omega\right), \\ M_P &= H_5\left(H_3\left(\alpha_P\right) \oplus H_4\left(\mathrm{ID}_P \oplus S_P\right)\right). \end{aligned} \tag{3}$$

Send $\{M_P, t_P\}$ to the MS.

Step 2. The Doctor picks the current time stamp t_D and computes

$$\begin{aligned} h_1' &= H_1\left(\mathrm{ID}_D, \omega, \mathrm{pk}_D\right), \qquad r_D = H_2\left(\mathrm{ID}_D, S_D, t_D\right), \\ \alpha_D &= \left(z + r_D\right) \cdot \left(h_1' X + \omega\right), \\ M_D &= H_5\left(H_3\left(\alpha_D\right) \oplus H_4\left(\mathrm{ID}_D \oplus S_D\right)\right). \end{aligned} \tag{4}$$

Send $\{M_D, t_D\}$ to the MS.

Step 3. If $(t^* - t_P) < \Delta t_P$ and $(t^* - t_D) < \Delta t_D$, where Δt_P and Δt_D denote the expected valid time interval for time delay of Patient and Doctor, the MS proceeds to the next step. Otherwise, return "*Reject*."

Step 4. The MS computes

$$\begin{aligned} M_P' = H_5 &\left(H_3\left(d_P \cdot \left(Y + H_2\left(\mathrm{ID}_P, S_P, t_P\right) \cdot P\right)\right)\right. \\ &\left.\oplus H_4\left(\mathrm{ID}_P \oplus S_P\right)\right), \\ M_D' = H_5 &\left(H_3\left(d_D \cdot \left(Z + H_2\left(\mathrm{ID}_D, S_D, t_D\right) \cdot P\right)\right)\right. \\ &\left.\oplus H_4\left(\mathrm{ID}_D \oplus S_D\right)\right). \end{aligned} \tag{5}$$

If M_P' is equal to M_P, Patient is a legal one. Otherwise, return "*Reject*." In addition, if M_D' is equal to M_D, Doctor is a legal one. Otherwise, return "*Reject*."

Step 5. The MS picks $N_M \in \{0, 1\}^m$ uniformly at random and updates the serial numbers of Patient and Doctor as follows:

$$\begin{aligned} S_{P,\mathrm{new}} &= H_4\left(S_P \oplus N_M \oplus \mathrm{ID}_P\right), \\ S_{D,\mathrm{new}} &= H_4\left(S_D \oplus N_M \oplus \mathrm{ID}_D\right). \end{aligned} \tag{6}$$

Send $\{N_M\}$ to Patient and Doctor.

Step 6. By using of $\{N_M\}$, Patient computes

$$S_{P,\,\mathrm{new}} = H_4\left(S_P \oplus N_M \oplus \mathrm{ID}_P\right) \tag{7}$$

for updating the serial number of his/her wearable medical sensor.

Step 7. After obtaining $\{N_M\}$, Doctor computes

$$S_{D,\,\mathrm{new}} = H_4\left(S_D \oplus N_M \oplus \mathrm{ID}_D\right) \tag{8}$$

for updating the serial number of his/her hand-held device.

3.2. Security Analysis

Theorem 1. *This certificateless authentication scheme is secure in the following possible attacks, provided that H_1 is a collision-resistance hash function and DL and CDH problems are intractable.*

Proof

Anonymity. In the proposed scheme, the partial key $d_P = s + xH_1(\mathrm{ID}_P, \omega, \mathrm{pk}_P)$ is used instead of ID_P to ensure the Patient's anonymity. Since ID_P is never transmitted as plaintext form in the public channel, Type I adversary cannot find the real identity ID_P of Patient. That is, when Patient transmits his/her health information, their real identity ID_P can only be computed as $d_P = s + xH_1(\mathrm{ID}_P, \omega, \mathrm{pk}_P)$ to be transmitted, where s is a random value, H_1 is a collision-resistant hash function, and x is the master secret key which is preserved by MS. Therefore, Type I adversary cannot trace Patient.

Perfect Forward Secrecy. To extract $\{M_P, M_D\}$ without the knowledge of the values $\{r_P, y, d_P, r_D, z, d_D\}$, Type II adversary should solve the DL problem and the CDH problem from public parameters. Moreover, $r_P = H_2(\mathrm{ID}_P, S_P, t_P)$ and

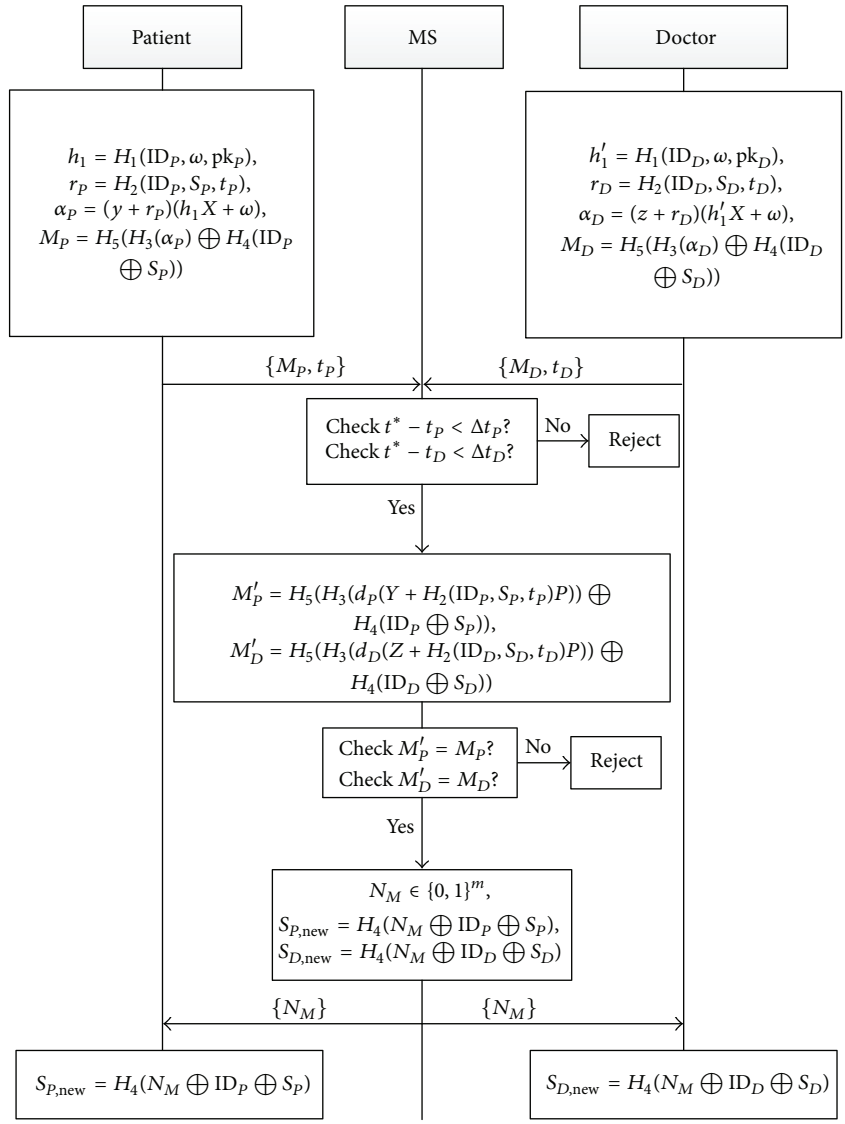

Figure 2: Authentication phase.

$r_D = H_2(\mathrm{ID}_D, S_D, t_D)$ will be different in every session for the reason of time stamps $\{t_P, t_D\}$ and the updated serial numbers $\{S_P, S_D\}$. Therefore, Type II adversary cannot receive the previous value $\{r_P, y, d_P, r_D, z, d_D\}$ and the protocol enjoys the perfect forward security.

Replay Attack. During the data transmission, Type III adversary may eavesdrop $\{M_P, M_D\}$ and impersonate the legitimate Patient and Doctor to transmit $\{M_P, M_D\}$ to MS. After each session is over, the serial numbers of the Patient's sensor and Doctor's hand-held device have been updated to be the new serial numbers $\{S_{P,\mathrm{new}}, S_{D,\mathrm{new}}\}$, which can be used to generate the new messages $\{M_{P,\mathrm{new}}, M_{D,\mathrm{new}}\}$. Hence, Type III adversary cannot pass the verification by retransmitting $\{M_P, M_D\}$ in the new session. Moreover, there are time stamps $\{t_P, t_D\}$ in this scheme, which ensures the freshness of $\{M_P, M_D\}$.

Impersonation Attack. The impersonation attack fails due to the secret serial number. Provided that Type IV adversary wants to impersonate the legitimate Patient and Doctor, it must produce the relative $\{M_P, M_D\}$ for passing the verification of MS. However, in order to generate the exactly $\{M_P, M_D\}$, Type IV adversary needs to obtain the current serial numbers $\{S_P, S_D\}$ first of all, which are preserved secretly by Patient and Doctor and updated in time in the end of *Authentication* phase. Therefore, Type IV adversary has no capability to impersonate the legitimate Patient and Doctor to generate the correct $\{M_P, M_D\}$.

Malicious MS Attack. The malicious MS cannot obtain the private keys to eavesdrop the privacy information of patient.

Table 1: Functionality comparisons.

Properties	[7]	[12]	[13]	Ours
User anonymity	No	No	No	Yes
Perfect forward secrecy	No	Yes	Yes	Yes
Replay attack resistance	Yes	No	No	Yes
Impersonation attack resistance	Yes	Yes	Yes	Yes
Malicious server attack resistance	Yes	Yes	Yes	Yes
No certificate management	No	Yes	Yes	Yes
Trust level	1	2	3	3

This authentication scheme is proposed on the base of CL-PKC, and the private keys (SK_{ID_P}, SK_{ID_D}) generated by Patient and Doctor consist of partial private keys (d_P, d_D) and the secret values (y, z). The malicious MS cannot obtain (y, z) from public parameters for the intractable of DL and CDH problems. Therefore, our scheme can resist the malicious MS attack.

Achieve Girault's Trust Level 3. The *Patient/Doctor-Key-Generation* must be run prior to *Partial-Key-Extract*. In this way, the *Partial-Key-Extract* algorithm includes (pk_P, pk_D) generated by Patient and Doctor as input. Therefore, provided that the MS replaces (pk_P, pk_D), there will exist two working keys (pk_P, pk'_P) and (pk_D, pk'_D) for Patient and Doctor, respectively. Furthermore, two working public keys (PK_{ID_P}, PK'_{ID_P}) binding only one identity ID_P can result from two partial private keys (the same to Doctor), and only the MS could generate these two working partial private keys. Hence, it can be proven that MS generates false guarantees of Patient and Doctor, which means that our scheme achieves Girault's trust level 3 (the same level as is enjoyed in a traditional PKI).

Thus, to sum up the analysis above, we complete the proof of Theorem 1.

4. Comparisons

In this section, we evaluate some performance issues of our protocol with related works in functionality and efficiency.

4.1. Functionality Comparisons. Table 1 demonstrates the functionality comparisons between the proposed scheme and others [7, 12, 13]. Zhu's, Xiong et al.'s, and Zhang et al.'s protocols do not provide user anonymity. Moreover, the schemes in [12, 13] are insecure against the replay attack. However, as shown in Table 1, our scheme not only provides user anonymity but also achieves all security requirements. Furthermore, our scheme does not need an additional certificate to bind the user to its public key.

4.2. Efficiency Comparisons. In this subsection, we compare the proposed scheme with others on the computation complexity of authentication (Authen), bandwidth of the largest message (Bandwidth), and operation time in authentication (Time). Without considering the addition of two points, hash function and exclusive-OR operations, each scheme has three types of operations, that is, pairing (P), exponentiation (E), and scalar multiplication (S).

Table 2: Cryptographic operation time.

Fast-Tate-Pairing	Exponential	Scalar multiplication
2.66 ms	3.75 ms	0.94 ms

Table 3: Efficiency comparisons.

Scheme	Authen	Bandwidth	Time
[7]	4E	48 bytes	15 ms
[12]	6P + 6E + 21S	96 bytes	58.2 ms
[13]	2P + 10S	72 bytes	14.72 ms
Ours	8S	28 bytes	7.52 ms

We evaluate the cryptographic operations by using of MIRACL (version 5.6.1, [17]), a standard cryptographic library, on a laptop using the Intel Core i5-2400 at a frequency of 3.10 GHz with 3 GB memory, and then obtain the average running time in Table 2. For pairing-based schemes, we use the Fast-Tate-Pairing in MIRACL, which is defined over the MNT curve E/F_q [18] with embedding degree 4, and q is a 160-bit prime. For ECC-based scheme, we employed the parameter secp192r1 [19], where $p = 2^{192} - 2^{64} - 1$. Moreover, the length of an element in multiplication group is set to be 1024 bits.

We compare the computation cost of different protocols with the method in [20]. For example, to finish the authentication in [12], six pairing operations, six exponentiations in Z_p^*, and twenty-one scalar multiplications are needed; thus, the operation time is $2.66 \times 6 + 3.75 \times 6 + 0.94 \times 21 = 58.2$ ms. Assuming the bit size of the identity, the point in additional group and the output of one-way hash function are all 192 bits. We also assume that the size of timestamp is 32 bits. In [12], the largest message contains three points in additional group and one identification; thus, the bandwidth of it is $(192 \times 3 + 192)/8 = 96$ bytes. The detailed comparison results are demonstrated in Table 3.

From Table 3, we know that the largest bandwidth of our scheme is only 28 bytes and the whole operation time in authentication is only 7.52 ms, which shows that our protocol is suitable for the lightweight devices (with limited memory, small and low power) in the healthcare system on WMSN.

5. Conclusions

In this paper, we propose a secure certificateless authentication scheme to ensure the legality of Patient and Doctor in healthcare system on WMSN. Meanwhile, this protocol also provides patient anonymity and resists the malicious MS attack to meet the privacy requirements in HIPAA. Our certificateless authentication protocol achieves a lower communication and computational overhead and stronger security than others. By the performance evaluation, the results show that our protocol is suitable for healthcare system on WMSN.

Acknowledgments

This work is supported by NSFC (Grants nos. 61272057, 61202434, 61170270, 61100203, 61003286, and 61121061), the Fundamental Research Funds for the Central Universities (Grants nos. 2012RC0612, 2011YB01).

References

[1] R. S. H. Istepanian, E. Jovanov, and Y. T. Zhang, "Introduction to the special section on m-Health: beyond seamless mobility and global wireless health-care connectivity," *IEEE Transactions on Information Technology in Biomedicine*, vol. 8, no. 4, pp. 405–414, 2004.

[2] F. Bellifemine, G. Fortino, R. Giannantonio, R. Gravina, A. Guerrieri, and M. Sgroi, "SPINE: a domain-specific framework for rapid prototyping of WBSN applications," *Software, Practice and Experience*, vol. 41, no. 3, pp. 237–265, 2011.

[3] Q. Pu, J. Wang, and R. Y. Zhao, "Strong authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 36, no. 4, pp. 2609–2619, 2012.

[4] Z.-Y. Wu, Y.-C. Lee, F. Lai, H.-C. Lee, and Y. Chung, "A secure authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 36, no. 3, pp. 1529–1535, 2012.

[5] D. B. He, J. H. Chen, and R. Zhang, "A more secure authentication scheme for telecaremedicine information systems," *Journal of Medical Systems*, vol. 36, no. 3, pp. 1989–1995, 2012.

[6] J. H. Wei, X. X. Hu, and W. F. Liu, "An improved authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 36, no. 6, pp. 3597–3604, 2012.

[7] Z. A. Zhu, "An efficient authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 36, no. 6, pp. 3833–3838, 2012.

[8] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proceedings of the Advances in Cryptology (CRYPTO '85)*, pp. 47–53, 1985.

[9] M. L. Das, A. Saxena, and V. P. Gulati, "A dynamic ID-based remote user authentication scheme," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 629–631, 2004.

[10] H. Y. Chien and C. H. Chen, "A remote authentication scheme preserving user anonymity," in *Proceedings of the International Conference on AINA*, vol. 2, 2005.

[11] W. C. Ku and S. T. Chang, "Impersonation attack on a dynamic ID-based remote user authentication scheme using smart cards," *IEICE Transactions on Communications*, vol. E88-B, no. 5, pp. 2165–2167, 2005.

[12] H. Xiong, Z. Chen, and F. G. Li, "Provably secure and efficient certificateless authenticated tripartite key agreement protocol," *Mathematical and Computer Modelling*, vol. 55, no. 3-4, pp. 1213–1221, 2012.

[13] L. Zhang, F. Zhang, Q. Wu, and J. Domingo-Ferrer, "Simulatable certificateless two-party authenticated key agreement protocol," *Information Sciences*, vol. 180, no. 6, pp. 1020–1030, 2010.

[14] L. Chen, Z. Cheng, and N. P. Smart, "Identity-based key agreement protocols from pairings," *International Journal of Information Security*, vol. 6, no. 4, pp. 213–241, 2007.

[15] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Proceedings of the Advances in Cryptology (ASIACRYRT '03)*, pp. 452–473, 2003.

[16] M. Girualt, "Self-certified public keys," in *Proceedings of the Advances in Cryptology (EUROCRYPTO '91)*, pp. 490–497.

[17] M. Scott, "Miracl library," http://certivox.com/.

[18] A. Miyaji, M. Nakabayashi, and S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 84, no. 5, pp. 1234–1243, 2001.

[19] The Certicom Corporation, SEC2: Recommended elliptic curve domain parameters, 2000.

[20] K. Ren, W. Lou, K. Zeng, and P. J. Moran, "On broadcast authentication in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 6, no. 11, pp. 4136–4144, 2007.