Hindawi
Security and Communication Networks
Volume 2018, Article ID 9146297, 15 pages
https://doi.org/10.1155/2018/9146297

Research Article

An Efficient Three-Party Authentication Scheme for Data Exchange in Medical Environment

Shin-Yan Chiou [1,2,3] **and Ching-Hsuan Lin** [1]

[1] *Department of Electrical Engineering, College of Engineering, Chang Gung University, 259 Wen-Hwa 1st Road, Kwei-Shan, Tao-Yuan, Taiwan*
[2] *Department of Nuclear Medicine, Linkou Chang Gung Memorial Hospital, Tao-Yuan, Taiwan*
[3] *Center for Biomedical Engineering, Chang Gung University, Tao-Yuan, Taiwan*

Correspondence should be addressed to Shin-Yan Chiou; ansel@mail.cgu.edu.tw

Received 6 July 2017; Revised 17 October 2017; Accepted 10 December 2017; Published 2 January 2018

Academic Editor: Emanuele Maiorana

Compared with traditional paper medical records, electronic medical records have many advantages such as easy transmission, high efficiency, better accuracy, and easier storage. The further development and penetration of electronic medical records will raise increasingly critical transmitted-data accuracy and security issues. Previous studies have proposed a verifier-based three-party authentication scheme and to provide high efficiency and security, with low computation and transmission costs. However, this protocol fails to achieve anonymity, is vulnerable to tracking attacks, and is inefficient. In this paper, we propose a new authentication scheme which provides patient anonymity and resistance to tracking attacks, while reducing computation and communication costs. The proposed system is easier to implement and is more suitable for use in remote electronic medical record exchange systems.

1. Introduction

Aging societies experience increasing rates of chronic disease (e.g., heart disease, diabetes, cardiovascular diseases, and mental health issues) which must be frequently observed and monitored. Patients with such illnesses require periodic hospital- or clinic-based checkups, which can be inconvenient and stressful for elderly people. The digitization of medical measurement equipment (e.g., blood pressure monitors, blood glucose meters) allows for diagnostic information to be stored electronically and transmitted to remote locations for analysis and monitoring, enabling patients to avoid hospital visits while enabling their health care to closely monitor their status. Such electronic medical records (EMR) [1–3] has many advantages over conventional paper medical records, such as easy transmission, high efficiency, better accuracy, and ease of storage. However, their increased convenience raises significant security issues such as patient privacy and data integrity.

Telecare medicine information systems (TMIS) [4–6] involve the transmission of remote digital medical information or health reports through the combination of computers, communication systems to provide patients, and medical institutions with a secure data transmission platform and allow them to obtain medical record or health reports securely and conveniently. However, there are many security issues such as patient privacy and data integrity. Many identification and authentication protocols have been proposed to protect patient privacy and information. TMIS with three-party authentication is a secure data transmission platform that allows an authentication server and two participants (a medical institution or doctor and a patient) to generate a session key and a secure channel to verify their identities and then exchange data securely.

Lin and Lee [7] proposed a verifier-based three-party authentication scheme to provide high efficiency and security, along with low computation and transmission costs. However, this protocol fails to achieve anonymity and is vulnerable to tracking attacks. In addition, when authenticating a participant, it takes considerable time for the server to locate the verifiers, making the system difficult to implement. We thus propose a new authentication scheme which provides

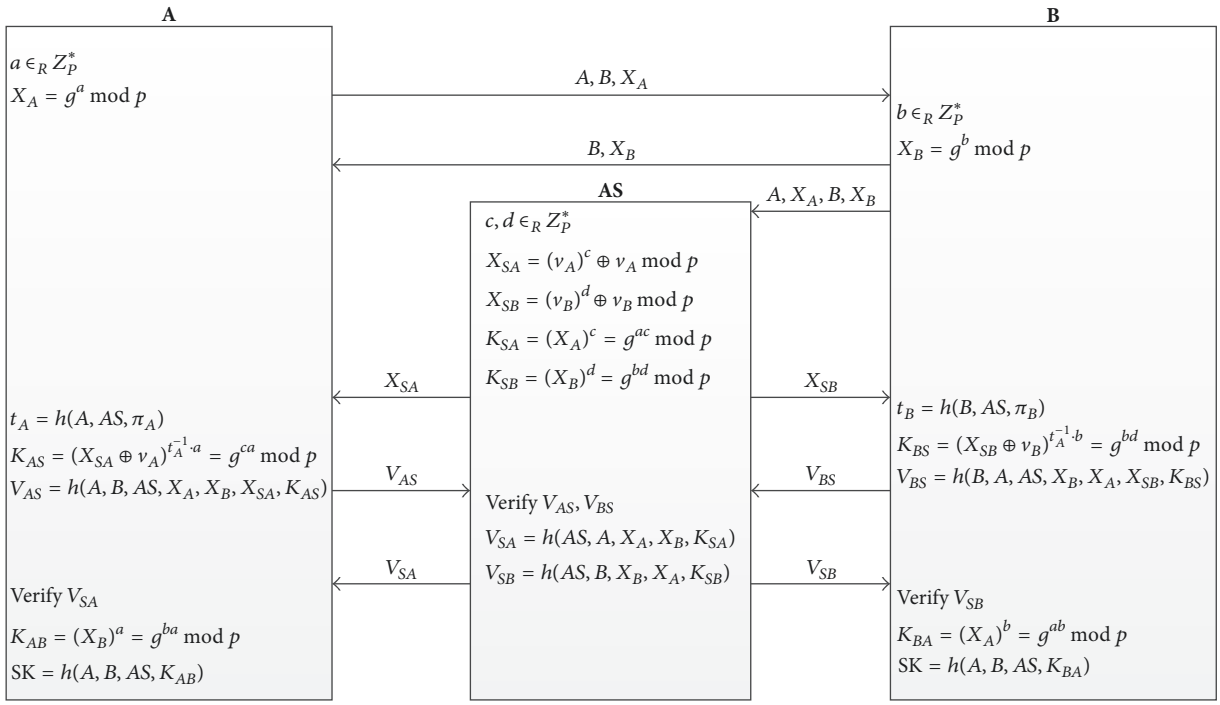


Figure 1: The procedure of Lee et al.'s scheme.

anonymity and resistance to tracking attacks, while reducing computation and communication costs. The proposed system is easier to implement and is more suitable for use in remote electronic medical record exchange systems.

The remainder of this paper is organized as follows. Section 2 reviews and analyzes verifier-based three-party authentication schemes without server public key including Lee et al.'s [8], Wang-Mo's [9], Kwon et al.'s [10], and Lin-Lee's [7] schemes. Section 3 introduces notations and security requirements for our scheme. Section 4 presents our proposed protocol, and the security analysis is given in Section 5. Section 6 provides a comparison of the proposed protocol and other related works. Finally, an implementation is described in Section 7 and a conclusion is drawn in Section 8.

2. Related Works

This section reviews four verifier-based three-party authentication schemes without server public key including Lee et al.'s [8], Wang-Mo's [9], Kwon et al.'s [10], and Lin-Lee's [7] schemes and analyzes the weaknesses of their schemes.

2.1. Review of Lee et al.'s Scheme. Lee et al. [8] proposed a verifier-based authentication scheme without server's public key based on the Diffie-Hellman key exchange. Their scheme enables each client to only remember a memorable password. The normal procedure of their scheme is shown in Figure 1.

2.1.1. Initialization Phase. A client A and a trusted authentication server AS share a verifier $v_A = g^{t_A} \bmod p$ for a password π_A, and a client B and AS share a verifiers $v_B = g^{t_B} \bmod p$ for a password π_B, where $t_A = h(A, AS, \pi_A)$ and $t_B = h(A, AS, \pi_B)$.

2.1.2. Verification Phase. This phase allows A and B to share a secret key confidentially via AS. The details of the execution steps are described as follows (Figure 1).

(1) $A \rightarrow B : A, B, X_A$: A chooses a random number $a \in_R Z_P^*$, computes $X_A = g^a \bmod p$, and sends A, B, X_A to B.

(2) $B \rightarrow A : B, X_B$ and $B \rightarrow AS : A, X_A, B, X_B$: B chooses a random number $b \in_R Z_P^*$, computes $X_B = g^b \bmod p$, and sends (B, X_B) and (A, X_A, B, X_B) to A and AS, respectively.

(3) $AS \rightarrow A : X_{SA}$ and $AS \rightarrow B : X_{SB}$: after receiving v_a and v_b, AS chooses two random numbers $c, d \in_R Z_P^*$, computes $X_{SA} = (v_A)^c \oplus v_A \bmod p$, $X_{SB} = (v_B)^d \oplus v_B \bmod p$, $K_{SA} = (X_A)^c = g^{ac} \bmod p$, and $K_{SB} = (X_B)^d = g^{bd} \bmod p$, and sends X_{SA} and X_{SB} to A and B, respectively.

(4) $A \rightarrow AS : V_{AS}$ and $B \rightarrow AS : V_{BS}$: A computes $K_{AS} = (X_{SA} \oplus v_A)^{t_A^{-1} \cdot a} = g^{ca} \bmod p$ and $V_{AS} = h(A, B, AS, X_A, X_B, X_{SA}, K_{AS})$, sends V_{AS} to AS, where $t_A = h(A, AS, \pi_A)$. B computes $K_{BS} = (X_{SB} \oplus v_B)^{t_B^{-1} \cdot b} = g^{bd} \bmod p$ and $V_{BS} = h(B, A, AS, X_B, X_A, X_{SB}, K_{BS})$, and sends V_{BS} to AS, where $t_B = h(B, AS, \pi_B)$.

(5) $AS \rightarrow A : V_{SA}$ and $AS \rightarrow B : V_{SB}$: AS verifies whether V_{AS} and V_{BS} are valid. If they do, AS

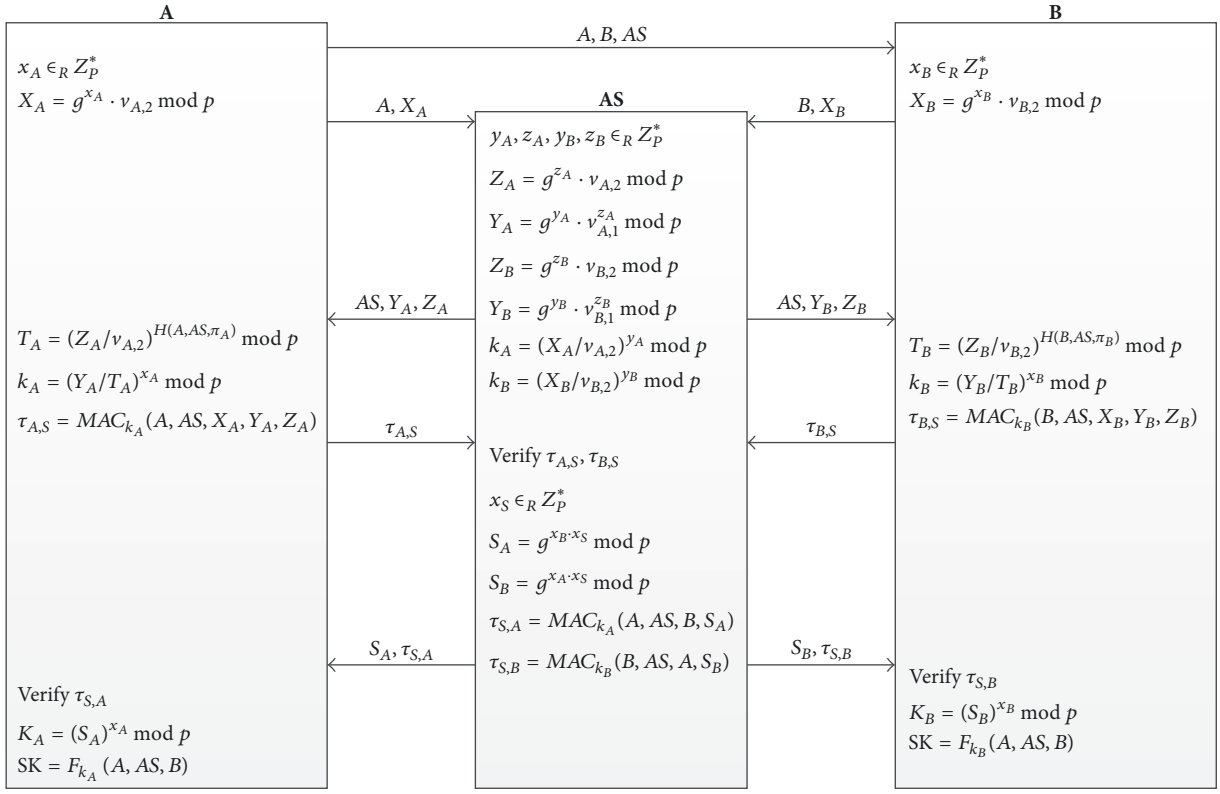


Figure 2: The procedure of Kwon et al.'s scheme.

computes $V_{SA} = h(AS, A, X_A, X_B, K_{SA})$ and $V_{SB} = h(AS, B, X_B, X_A, K_{SB})$ and sends V_{SA} and V_{SB} to A and B, respectively.

(6) A verifies V_{SA} and B verifies V_{SB}.

Finally, A possesses a session key $K_{AB} = (X_B)^a = g^{ba} \bmod p$ and B possesses a session key $K_{BA} = (X_A)^b = g^{ab} \bmod p$.

2.1.3. Weaknesses of Lee et al.'s Scheme. Wang and Mo [9] showed that the Lee et al.'s scheme [8] is not resistant to an impersonation attack if an attacker once has stolen A's verifier v_A.

2.2. Review of Wang-Mo's Scheme. In order to withstand an impersonation attack of the Lee et al.'s scheme [8] under verifier-stolen situation, Wang and Mo [9] modified V_{AS} as $h(A, B, AS, X_A, X_B, (X_{SA} \oplus v_A)^{t_A^{-1}} = g^c, K_{AS})$ and V_{BS} as $h(B, A, AS, X_B, X_A, (X_{SB} \oplus v_B)^{t_B^{-1}} = g^d, K_{BS})$, respectively. Therefore, if both verifiers V_{AS} and V_{BS} are stole, an impersonation attack does not work without t_A and t_B.

However, Lin and Lee [7] showed that the Wang and Mo's scheme [9] do not realize key confirmation. If the transmitted EMRs or EHRs are encrypted by using an unconfirmed key, their integrity and confidentiality are unsure.

2.3. Review of Kwon et al.'s Scheme. This section reviews Kwon et al.'s scheme [10]. The normal procedure of their scheme is shown in Figure 2.

2.3.1. Initialization Phase. A and AS share a verifier $v_{A,1} = g^{t_A} \bmod p$ and $v_{A,2} = g_2^{t_A} \bmod p$ for a password π_A, and B and AS share a verifiers $v_{B,1} = g^{t_B} \bmod p$ and $v_{B,2} = g_2^{t_B} \bmod p$ for a password π_B, where $t_A = h(A, AS, \pi_A)$ and $t_B = h(A, AS, \pi_B)$.

2.3.2. Verification Phase. This phase allows A and B to share a secret key confidentially via AS. The details of the execution steps are described as follows (Figure 2):

(1) $A \to B : A, B, AS$: A broadcasts (A, B, AS).

(2) $A \to AS : A, X_A$ and $B \to AS : B, X_B$: A chooses a random number $x_A \in_R Z_P^*$, computes $X_A = g^{x_A} \cdot v_{A,2} \bmod p$, and sends (A, X_A) to AS. B chooses a random number $x_B \in_R Z_P^*$, computes $X_B = g^{x_B} \cdot v_{B,2} \bmod p$, and sends (B, X_B) to AS.

(3) $AS \to A : AS, Y_A, Z_A$ and $AS \to B : AS, Y_B, Z_B$: AS chooses random numbers $y_A, z_A, y_B, z_B \in_R Z_P^*$, computes $Z_A = g^{z_A} \cdot v_{A,2} \bmod p$, $Y_A = g^{y_A} \cdot v_{A,1}^{z_A} \bmod p$, $Z_B = g^{z_B} \cdot v_{B,2} \bmod p$ and $Y_B = g^{y_B} \cdot v_{B,1}^{z_B} \bmod p$, and sends (AS, Y_A, Z_A) and (AS, Y_B, Z_B) to A and B, respectively. Moreover, AS computes $k_A = (X_A/v_{A,2})^{y_A} \bmod p$ and $k_B = (X_B/v_{B,2})^{y_B} \bmod p$.

(4) $A \to AS : \tau_{A,S}$ and $B \to AS : \tau_{B,S}$: after receiving (AS, Y_A, Z_A), A computes $T_A = (Z_A/v_{A,2})^{H(A,AS,\pi_A)} \bmod p$, $k_A = (Y_A/T_A)^{x_A} \bmod p$, and $\tau_{A,S} = MAC_{k_A}(A, AS, X_A, Y_A, Z_A)$ and sends $\tau_{A,S}$ to

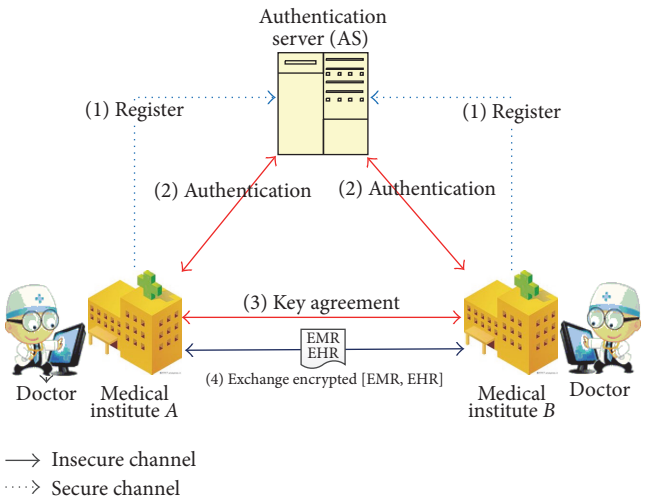


FIGURE 3: The normal procedure of Lin-Lee's scheme.

AS. After receiving (AS, Y_B, Z_B), B computes $T_B = (Z_B/v_{B,2})^{H(B,AS,\pi_B)} \bmod p$, $k_B = (Y_B/T_B)^{x_B} \bmod p$, and $\tau_{B,S} = MAC_{k_B}(B, AS, X_B, Y_B, Z_B)$ and sends $\tau_{B,S}$ to *AS*.

(5) $AS \to A : S_A, \tau_{S,A}$ and $AS \to B : S_B, \tau_{S,B}$: *AS* verifies whether $\tau_{A,S}$ and $\tau_{B,S}$ are correct. If so, *AS* chooses a random number $x_S \in_R Z_P^*$, computes $S_A = g^{x_B \cdot x_S} \bmod p$, $S_B = g^{x_A \cdot x_S} \bmod p$, $\tau_{S,A} = MAC_{k_A}(A, AS, B, S_A)$, and $\tau_{S,B} = MAC_{k_B}(B, AS, A, S_B)$, and sends $(S_A, \tau_{S,A})$ and $(S_B, \tau_{S,B})$ to A and B, respectively.

(6) A verifies $\tau_{S,A}$ and B verifies $\tau_{S,B}$.

Finally, A possesses a session key $K_A = (S_A)^{x_A} \bmod p$ and B possesses a session key $K_B = (S_B)^{x_B} \bmod p$.

2.3.3. Weaknesses of Kwon et al.'s Scheme. Lin and Lee [7] showed that the Kwon et al.'s scheme [10] do not realize key confirmation. If the transmitted EMRs or EHRs are encrypted by using an unconfirmed key, their integrity and confidentiality are unsure.

2.4. Review of Lin-Lee's Scheme. This section reviews Lin-Lee's scheme [7] (including the initialization and verification phases). The normal procedure of their scheme is shown in Figures 3 and 4.

A and B represent two medical institutions, and *AS* stands for a trusted authentication server.

2.4.1. Initialization Phase. As shown in steps (1) in Figure 3, A and B send their verifiers to *AS* via a secure and verified channel to register their verifiers. The details of the steps are as follows: A sends verifier $v_A = g^{t_A} \bmod p$ to *AS*, and B sends verifier $v_B = g^{t_B} \bmod p$ to *AS*, where $t_A = H(\mathrm{ID}_A, \mathrm{ID}_{AS}, \pi_A)$ and $t_B = H(\mathrm{ID}_B, \mathrm{ID}_{AS}, \pi_B)$.

2.4.2. Verification Phase. Assume A and B need to exchange EMR or EHR confidentially via authentication server *AS*. As shown in steps (2), (3), and (4) in Figure 3, A and B process a mutual authentication with *AS* and each other, perform a key agreement to obtain a session key, and exchange encrypted EMR or EHR encrypted by the session key. The details of the execution steps are described as follows:

(1) $A \to AS : \mathrm{ID}_A, \mathrm{ID}_B, X_A$: A chooses a random number $a \in_R Z_P^*$, computes $X_A = g^a \bmod p$, and sends ID_A, ID_B, X_A to *AS*.

(2) $A \to B : \mathrm{ID}_A, X_A$: A sends ID_A and X_A to B.

(3) $AS \to A : X_{SA}, AS \to B : X_{SB}$: *AS* chooses two random numbers $c, d \in_R Z_P^*$, computes $X_{SA} = (v_A)^c \oplus v_A \bmod p$ and $X_{SB} = (v_B)^d \oplus v_B \bmod p$, sends X_{SA} to A, and sends X_{SB} to B.

(4) $B \to AS : \mathrm{ID}_A, \mathrm{ID}_B, X_B$: B chooses a random number $b \in_R Z_P^*$, computes $X_B = g^b \bmod p$, and sends ID_A, ID_B, and X_B to *AS*.

(5) *AS*: *AS* computes g^c, g^d, $K_{SA} = (X_A)^c = g^{ac} \bmod p$, and $K_{SB} = (X_B)^d = g^{bd} \bmod p$.

(6) $B \to A : \mathrm{ID}_B, X_B$: B sends ID_B, X_B to A.

(7) $A \to AS : V_{AS}$: A computes $g^c = (X_{SA} \oplus v_A)^{t_A^{-1}} \bmod p$, uses g^c and a to evaluate $K_{AS} = (g^c)^a = g^{ca} \bmod p$, $V_{AS} = h(\mathrm{ID}_A, \mathrm{ID}_B, \mathrm{ID}_{AS}, X_A, X_B, g^c, K_{AS})$, $K_{AB} = (X_B)^a = g^{ba} \bmod p$, and $\mu_{AB} = h(\mathrm{ID}_A, \mathrm{ID}_B, X_A, X_B, K_{AB})$, and sends V_{AS} to *AS*.

(8) $B \to AS : V_{BS}$: B computes $g^d = (X_{SB} \oplus v_B)^{t_B^{-1}} \bmod p$, uses g^d and b to evaluate $K_{BS} = (g^d)^b = g^{db} \bmod p$, $V_{BS} = h(\mathrm{ID}_A, \mathrm{ID}_B, \mathrm{ID}_{AS}, X_A, X_B, g^d, K_{BS})$, $K_{BA} = (X_A)^b = g^{ab} \bmod p$, and $\mu_{AB} = h(\mathrm{ID}_A, \mathrm{ID}_B, X_A, X_B, K_{AB})$, and sends V_{BS} to *AS*.

(9) $A \to B : \mu_{AB}$: A sends $\mu_{AB} = h(\mathrm{ID}_A, \mathrm{ID}_B, X_A, X_B, K_{AB})$ to B.

(10) B authenticates A: B verifiers whether the values $\mathrm{ID}_A, \mathrm{ID}_B, X_A, X_B, K_{AB}$ in μ_{AB} are correct. If so, the identity of A is valid.

(11) $B \to A : \mu_{BA}$: B sends $\mu_{BA} = h(\mathrm{ID}_A, \mathrm{ID}_B, X_A, X_B, K_{BA})$ to A.

(12) A authenticates B: A verifiers whether the values $\mathrm{ID}_A, \mathrm{ID}_B, X_A, X_B, K_{BA}$ in μ_{BA} are correct. If so, the identity of B is valid.

(13) *AS* authenticates A, B: *AS* verifiers whether the equations $V_{AS} = h(\mathrm{ID}_A, \mathrm{ID}_B, \mathrm{ID}_{AS}, X_A, X_B, g^c, K_{AS})$ and $V_{BS} = h(\mathrm{ID}_A, \mathrm{ID}_B, \mathrm{ID}_{AS}, X_A, X_B, g^d, K_{BS})$ are hold. If so, the identities of A and B are valid.

(14) $AS \to A : V_{SA}$; $AS \to B : V_{SB}$: *AS* computes $V_{SA} = h(\mathrm{ID}_{AS}, \mathrm{ID}_A, X_A, X_B, K_{SA})$ and $V_{SB} = h(\mathrm{ID}_{AS}, \mathrm{ID}_B, X_B, X_A, K_{SB})$, sends V_{SA} to A, and sends V_{SB} to B.

(15) A authenticates *AS*: A verifiers whether V_{SA} is correct. If so, the identity of *AS* is valid.

(16) B authenticates *AS*: B verifiers whether V_{SB} is correct. If so, the identity of *AS* is valid.

Finally, A possesses a session key $\mathrm{SK}_{AB} = h(\mathrm{ID}_A, \mathrm{ID}_B, \mathrm{ID}_{AS}, K_{AB})$ and B possesses a session key $\mathrm{SK}_{BA} = h(\mathrm{ID}_A, \mathrm{ID}_B, \mathrm{ID}_{AS}, K_{BA})$.

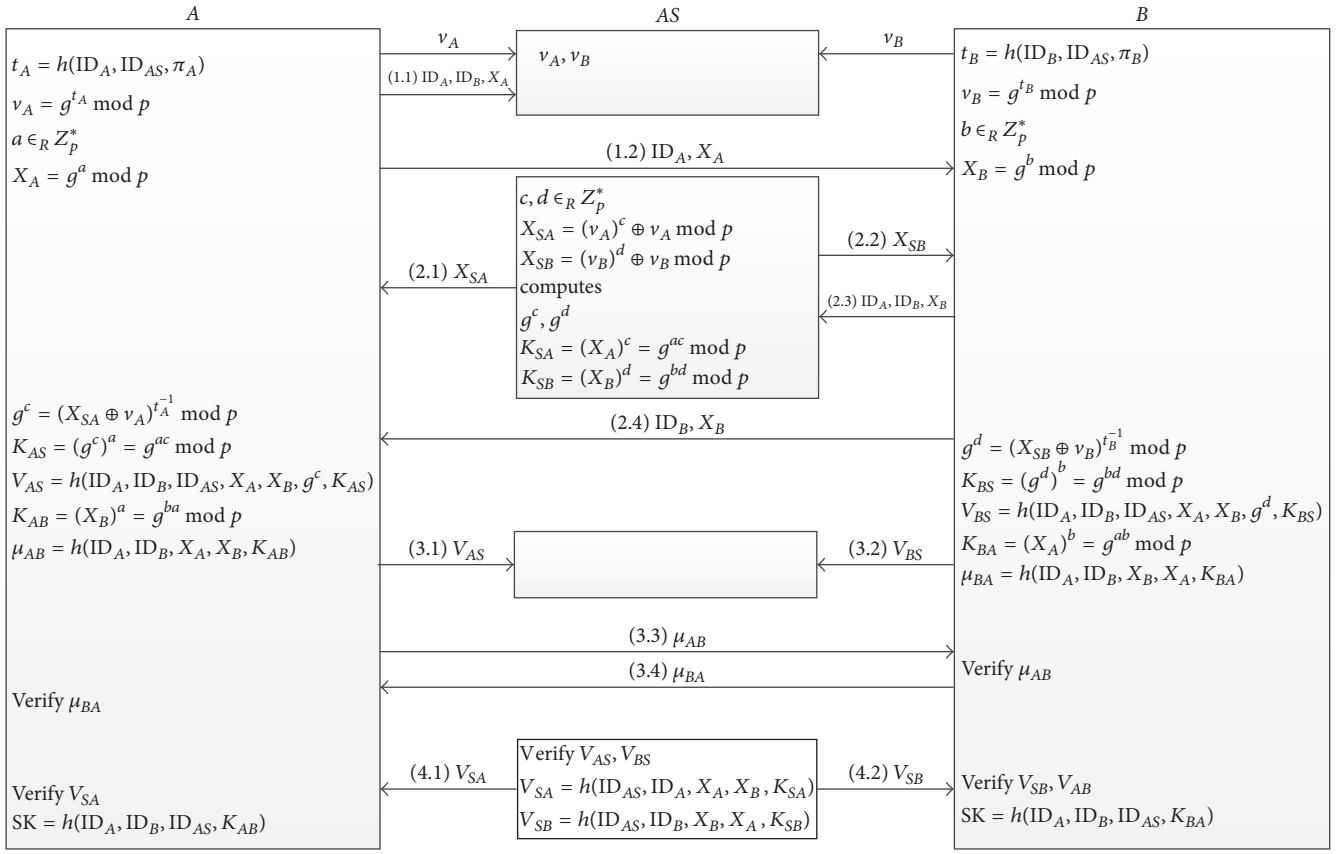


Figure 4: The procedure of Lin-Lee's scheme.

2.4.3. Weaknesses of Lin-Lee's Scheme. We find Lin-Lee's scheme [7] has three drawbacks: (1) does not provide anonymity, (2) vulnerable to tracking attack, and (3) inefficiency.

(1) Does Not Provide Anonymity. Medical institution A transmits data ID_A and ID_B to AS in the step (1) of verification phase, while medical institution B transmits the same data (ID_A and ID_B) to AS in the step (4) of verification phase. An attacker can obtain the identity (ID_A and ID_B) of both A and B by eavesdropping on the transmission; thus the scheme does not provide anonymity.

(2) Vulnerable to Tracking Attack. The data ID_A and ID_B are transmitted in both step (1) and step (4) of verification phase. An adversary can track institutions A and B easily from the identity (ID_A and ID_B); thus the scheme is vulnerable to tracking attack.

(3) Inefficiency. The scheme needs 16 exponentiations; therefore the computation cost of Lin-Lee's scheme is inefficiency.

3. Preliminary

3.1. Notations. Notations section shows the notations used in our protocol, where $\mathrm{SID}_X = h(\mathrm{ID}_X, \pi_X, T_X)$ is the pseudo ID of X, D_{UV} is a data encrypted by V using symmetric key encryption algorithm and sent to U from V, and X, U, and V represent medical institutions A, B, or server S.

3.2. Attacker Model. In our scheme, we assume that the channels between A and S, B and S, and A and B are insecure. Any identity communicates with each other via an insecure public channel, offering adversaries opportunities to intercept. In the following, we present the assumptions of the attacker model [18–21].

(1) An adversary may eavesdrop on all communications between protocol actors over the public channel.

(2) An attacker can modify, delete, resend, and reroute the eavesdropped message.

(3) An attacker cannot be a legitimate server.

(4) The attacker knows the protocol description, which means the protocol is public.

3.3. Security Requirements. The security requirements of our proposed scheme are listed as follows:

(1) Data integrity: an adversary cannot alter the transmitted data without being detected.

(2) Anonymity: an adversary cannot know the identities of medical institutions through the eavesdropped data.

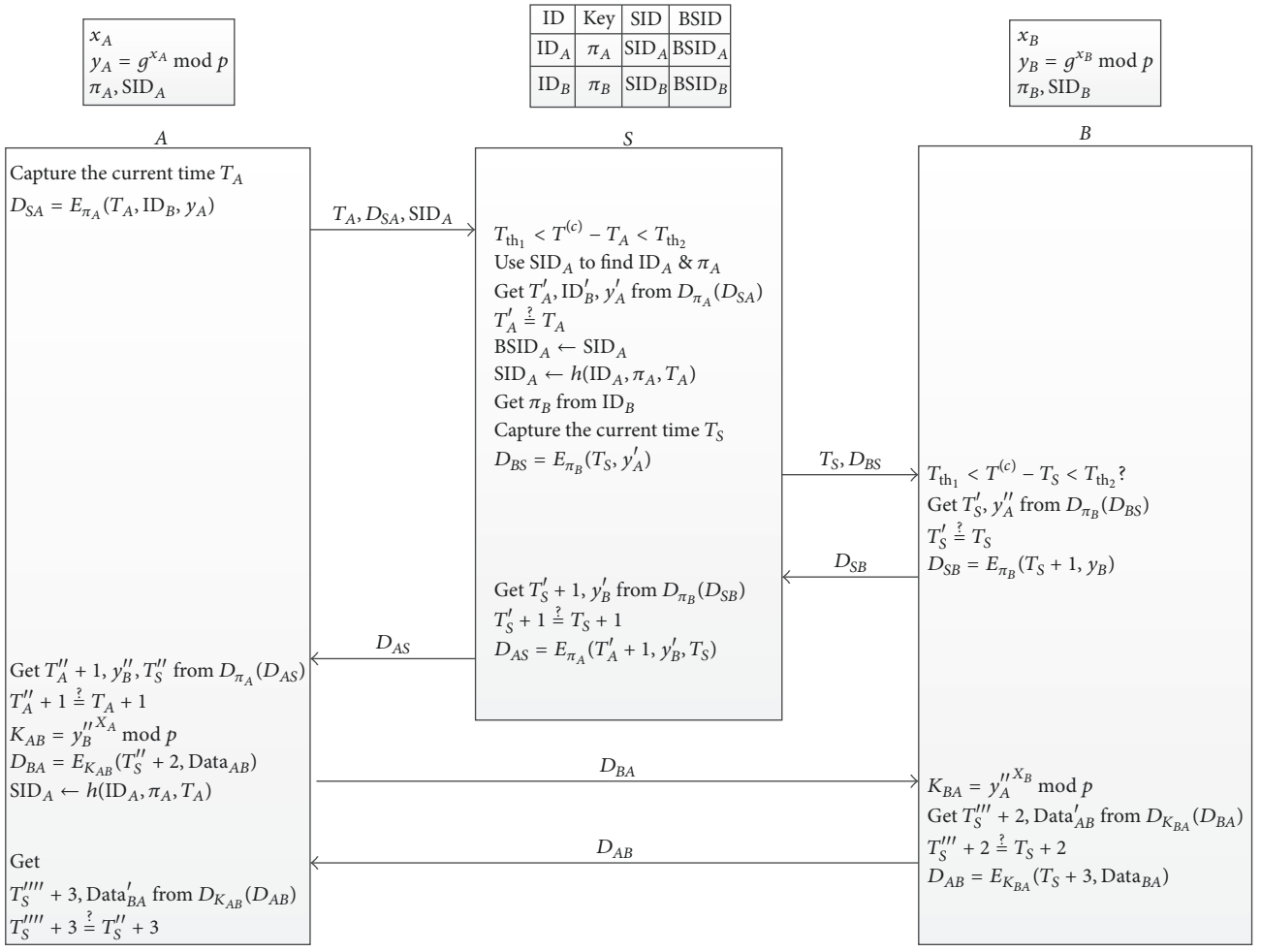


Figure 5: Procedure of the proposed scheme.

(3) Authenticity: any participant can authenticate other participants including the server.

(4) Medical record confidentiality: an adversary (including the server) cannot disclose any medical records.

(5) Medical record nonforgeability: an adversary cannot successfully forge electronic medical records.

(6) Resistance to asynchronous attacks: the system can process a successful authentication even if the data stored in participants' database may be asynchronous when a session cannot be normally completed.

(7) Resistance to tracking attack: an adversary cannot trace the medical institution A or B through the eavesdropped data.

4. Proposed Scheme

In this section, we propose a new three-party authentication scheme to achieve the functional requirements outlined in Definition 1 and the security goals outlined in Definition 2. The procedure of the proposed scheme is shown in Figure 5.

Definition 1 (functional requirements of our scheme). Our scheme features three roles: medical institution A, medical institution B, and authentication server S. Our scheme is functional if it provides that (1) A, B, and S can authenticate each other; (2) A and B can obtain a common session key; (3) A and B can exchange electronic medical records; (4) S is not required to have a public key; and (5) it is efficient to implement.

Definition 2 (security requirements of our scheme). Our scheme is secure if it achieves the following: (1) data integrity, (2) anonymity, (3) authenticity, (4) medical record confidentiality, (5) medical record nonforgeability, (6) resistance to asynchronous attacks, and (7) resistance to tracking attacks.

4.1. Initialization Phase. This phase establishes the required parameters.

(1) The system chooses one large prime number p.

(2) The system chooses one primitive root g modulo p.

(3) A and B each chooses a random number, respectively, x_A and $x_B \in_R Z^*_{p-1}$ and, respectively, computes $y_A = g^{x_A} \bmod p$, $y_B = g^{x_B} \bmod p$.

(4) A and B, respectively, generate symmetric keys π_A and π_B and use them to register with S.

(5) A and B, respectively, compute $\mathrm{SID}_A = h(\mathrm{ID}_A, \pi_A, 0)$ and $\mathrm{SID}_B = h(\mathrm{ID}_B, \pi_B, 0)$.

(6) S stores ID_X, π_X, and $\mathrm{SID}_X = h(\mathrm{ID}_X, \pi_X, 0)$, where $X = A$ or B.

4.2. Verification Phase. This phase presents the process of mutual authentication, key exchange, and data transmission among A, B, and S.

(1) $A \rightarrow S : T_A, D_{SA}, \mathrm{SID}_A$: A obtains the current time T_A, computes $D_{SA} = E_{\pi_A}(T_A, \mathrm{ID}_B, y_A)$, and sends T_A, D_{SA}, and SID_A to S.

(2) S authenticates A: S verifies whether $T_{\mathrm{th}_1} < T^{(c)} - T_A < T_{\mathrm{th}_2}$ holds, uses SID_A to find ID_A, decrypts D_{SA} via key π_A to obtain T'_A, ID'_B, and y'_A, and evaluates whether T'_A equals T_A. If it is, the identity of A is authenticated.

(3) S updates BSID_A: S updates $\mathrm{BSID}_A \leftarrow \mathrm{SID}_A$.

(4) S updates SID_A: S updates $\mathrm{SID}_A \leftarrow h(\mathrm{ID}_A, \pi_A, T_A)$.

(5) $S \rightarrow B : T_S, D_{BS}$: S obtains the current time T_S, uses ID'_B to find π_B, computes $D_{BS} = E_{\pi_B}(T_S, y'_A)$, and sends T_S and D_{BS} to B.

(6) B authenticates S: B verifies whether $T_{\mathrm{th}_1} < T^{(c)} - T_S < T_{\mathrm{th}_2}$ holds, decrypts D_{BS} via key π_B to obtain T'_S and y''_A, and evaluates whether T_S equals T'_S. If so, the identity of S is authenticated.

(7) $B \rightarrow S : D_{SB}$: B computes $D_{SB} = E_{\pi_B}(T_S + 1, y_B)$ and sends D_{SB} to S.

(8) S authenticates B: S decrypts D_{SB} via key π_B to obtain T'_S+1 and y'_B and evaluates whether T'_S+1 equals T_S+1. If so, the identity of B is authenticated.

(9) $S \rightarrow A : D_{AS}$: S computes $D_{AS} = E_{\pi_A}(T'_A + 1, y'_B, T_S)$ and sends D_{AS} to A.

(10) A authenticates S: A decrypts D_{AS} via key π_A to obtain T''_A+1, y''_B, and T''_S and evaluates whether T''_A+1 equals $T_A + 1$. If so, the identity of S is authenticated. A then computes $K_{AB} = y''^{X_A}_B \bmod p$.

(11) $A \rightarrow B : D_{BA}$: A computes $D_{BA} = E_{K_{AB}}(T''_S + 2, \mathrm{Data}_{AB})$ and sends D_{BA} to B.

(12) A updates SID_A: A updates $\mathrm{SID}_A \leftarrow h(\mathrm{ID}_A, \pi_A, T_A)$.

(13) B authenticates A: B computes $K_{BA} = y''^{X_B}_A \bmod p$, decrypts D_{BA} via key K_{BA} to obtain $T'''_S + 2$ and Data'_{AB}, and evaluates whether $T'''_S + 2$ equals $T_S + 2$. If so, the identity of A is authenticated, while the data Data'_{AB} is also obtained.

(14) $B \rightarrow A : D_{AB}$: B computes $D_{AB} = E_{K_{BA}}(T_S + 3, \mathrm{Data}_{BA})$ and sends D_{AB} to A.

(15) A authenticates B: A decrypts D_{AB} via key K_{AB} to obtain $T''''_S + 3$ and Data'_{BA} and evaluates whether $T''''_S + 3$ equals $T''_S + 3$. If so, the identity of B is authenticated, while the data Data'_{BA} is also obtained.

5. Security Analysis

In this section, we analyze our protocol according to the security requirements defined in Section 3.3. The proof uses security reduction similar to that used in the random oracle model [22]. In other words, based on the security goal and attacker model, we prove that "if one claimed security property of our scheme is broken then one *atomic primitive* is broken," where the atomic primitive means some basic cryptographic algorithm or hard mathematical problem. Therefore, our scheme provides this claimed security property since the atomic primitive is assumed to be secure.

5.1. Data Integrity. If the transmitted data D_{UV} is altered, postdecryption verification will fail, thus ensuring data integrity. Theorem 4 proves the property of data integrity from Definition 3.

Definition 3 (modified symmetric encryption problem). Let $x, y, y' \in Z$, $c = E_k(x, y)$, and $c' = E_k(x, y')$, where $y \neq y'$. If c' and y' can be evaluated from given x and c, then we say the modified symmetric encryption problem is solved (the probability of solving this problem is denoted as $\Pr(c', y' \mid x, c) = \varepsilon_1$).

Theorem 4 (data integrity). *In our scheme, if an adversary can change* $(Data_{AB}, D_{BA})$ *to* $(Data'_{AB}, D'_{BA})$ *successfully, then the modified symmetric encryption problem can be solved.*

Proof. In our scheme, assume an adversary tries to change $(\mathrm{Data}_{AB}, D_{BA})$ to $(\mathrm{Data}'_{AB}, D'_{BA})$ from eavesdropped T_S and D_{BA}. Let RO_1 be a random oracle: input T_S and D_{BA} to output Data'_{AB} and D'_{BA} such that $D_{K_{AB}}(D'_{BA}) = (T_S + 2, \mathrm{Data}'_{AB})$, where $D'_{BA} \neq D_{BA}$ (i.e., $\mathrm{RO}_1(T_S, D_{BA}) \Rightarrow \mathrm{Data}'_{AB}, D'_{BA} : D_{K_{AB}}(D'_{BA}) = (T_S + 2, \mathrm{Data}'_{AB})$). In Definition 3, let $k_{AB} \leftarrow k$ and $\mathrm{Data}_{AB} \leftarrow y$, and let $T_S \leftarrow x - 2$, $D_{BA} \leftarrow c$ be input parameters of RO_1 and obtain output Data'_{AB} and D'_{BA}. Let $y' \leftarrow \mathrm{Data}'_{AB}$ and $c' \leftarrow D'_{BA}$; then y' is evaluated. Therefore, $\Pr(\mathrm{Data}'_{AB}, D'_{BA} \mid T_S, D_{BA}) \leq \Pr(c', y' \mid x, c) = \varepsilon_1$, which means the modified symmetric encryption problem can be solved if RO_1 exists. □

5.2. Anonymity. If the attacker wants to obtain ID_A or ID_B, he has to use SID_A or D_{SA} to evaluate them. However, ID_A cannot be evaluated from $\mathrm{SID}_A \leftarrow h(\mathrm{ID}_A, \pi_A, T_A)$ because of the nonreversible one-way hash function. Moreover, evaluating ID_B requires decrypting $D_{SA} = E_{\pi_A}(T_A, \mathrm{ID}_B, y_A)$ using the key π_X, which is not obtained or evaluated through the eavesdropped data, therefore ensuring anonymity. Theorem 6 proves the property of data integrity from Definition 5.

Definition 5 (modified hash problem). Let $a, b, c \in Z$, and $d = h(a, b, c)$. If a can be evaluated from given d and c, then we say the modified hash problem is solved (the probability of solving this problem is denoted as $\Pr(a \mid d, c) = \varepsilon_2$).

Theorem 6 (anonymity). *In our scheme, if an administrator can obtain* ID_A *from* SID_A *and* T_A*, then the modified hash problem can be solved.*

Proof. In our scheme, assume an adversary tries to evaluate ID_A from eavesdropped SID_A and T_S. Let RO_2 be a random oracle: input T_S and SID_A to output ID_A (i.e., $\mathrm{RO}_2(T_S, \mathrm{SID}_A) \Rightarrow \mathrm{ID}_A$). In Definition 5, let $\pi_A \leftarrow b$, and let $T_S \leftarrow c$ and $\mathrm{SID}_A \leftarrow d$ be input parameters of RO_2 and obtain output ID_A. Let $a \leftarrow \mathrm{ID}_A$; then a is evaluated. Therefore, $\Pr(\mathrm{ID}_A \mid \mathrm{SID}_A, T_S) \leq \Pr(a \mid d, c) = \varepsilon_2$, which means the modified hash problem can be solved if RO_2 exists. □

5.3. Authenticity. Authenticating a participant requires evaluating whether T_X is equal to T_X'. Although an adversary can create a new T_X or obtain T_X through the eavesdropped data, he cannot obtain π_X or K_{UV} to decrypt T_X to achieve successful authentication, therefore ensuring authenticity. Theorem 8 proves the property of data integrity from Definition 7.

Definition 7 (joint modified symmetric encryption problem). Let $a_i, b, c, d_i \in Z$ and $d_i = E_k(a_i, b, c)$, where $i = 1, 2, \ldots, n+1$. If (a_{n+1}, d_{n+1}) can be evaluated from given c and (a_j, d_j), then we say the joint modified symmetric encryption problem is solved, where $j = 1, 2, \ldots, n$ (the probability of solving this problem is denoted as $\Pr(a_{n+1}, d_{n+1} \mid c, a_j, d_j) = \varepsilon_3$).

Theorem 8 (authenticity). *In our scheme, if D_{SA} and T_A can be forged, then the joint modified symmetric encryption problem can be solved.*

Proof. In our scheme, assume an adversary tries to evaluate ${T_A}^{(n+1)}, {D_{SA}}^{(n+1)}$ to forge the identity of A from y_A and eavesdropped $({T_A}^{(i)}, {D_{SA}}^{(i)})$, $i = 1, 2, \ldots, n$. Let RO_3 be a random oracle: input ${T_A}^{(i)}, {D_{SA}}^{(i)}, y_A$ to output ${D_{SA}}^{(n+1)}, {T_A}^{(n+1)}$, $i = 1, 2, \ldots, n$ (i.e., $\mathrm{RO}_3(({T_A}^{(i)}, {D_{SA}}^{(i)}), y_A) \Rightarrow {T_A}^{(n+1)}, {D_{SA}}^{(n+1)}$). In Definition 7, let ${T_A}^{(i)} \leftarrow a_i$, ${D_{SA}}^{(i)} \leftarrow d_i$, and $y_A \leftarrow c$ be input parameters of RO_3 and obtain output ${D_{SA}}^{(n+1)}, {T_A}^{(n+1)}$, $i = 1, 2, \ldots, n$. Let $d_{n+1} \leftarrow {D_{SA}}^{(n+1)}$ and $a_{n+1} \leftarrow {T_A}^{(n+1)}$, and then (a_{n+1}, d_{n+1}) are evaluated. Therefore, $\Pr({D_{SA}}^{(n+1)}, {T_A}^{(n+1)} \mid {D_{SA}}^{(i)}, {T_A}^{(i)}, y_A) \leq \Pr(a_{n+1}, d_{n+1} \mid c, a_j, d_j) = \varepsilon_3$, which means the joint modified symmetric encryption problem can be solved if RO_3 exists. □

5.4. Medical Record Confidentiality. Obtaining medical records requires using the session key K_{AB} (or K_{BA}) to decrypt D_{BA} (or D_{AB}), where the session key is generated from one's own private key x_A (or x_B) and the public key y_B (or y_A) of the opposite side. An attacker can neither evaluate the private keys x_A or x_B, nor obtain the public keys y_B or y_A due to anonymity. Therefore, the scheme ensures medical record confidentiality. Theorem 10 proves the property of data integrity from Definition 9.

Definition 9 (second modified symmetric problem). Let $x, y \in Z$, and $c = E_k(x, y)$. If y can be evaluated from given x and c, then we say the second modified symmetric problem is solved (the probability of solving this problem is denoted as $\Pr(y \mid x, c) = \varepsilon_4$).

Theorem 10 (medical record confidentiality). *In our scheme, if attacker can obtain Data_{AB}, then the second modified symmetric problem can be solved.*

Proof. In our scheme, assume an adversary tries to obtain Data_{AB} from eavesdropped T_S and D_{BA}. Let RO_4 be a random oracle: input T_S and D_{BA} to output Data_{AB} (i.e., $\mathrm{RO}_4(T_S, D_{BA}) \Rightarrow \mathrm{Data}_{AB}$). In Definition 9, let $T_S \leftarrow x$ and $D_{BA} \leftarrow c$ be input parameters of RO_4 and obtain output Data_{AB}. Let $y \leftarrow \mathrm{Data}_{AB}$, then y is evaluated. Therefore, $\Pr(\mathrm{Data}_{AB} \mid T_S, D_{BA}) \leq \Pr(y \mid x, c) = \varepsilon_4$, which means the second modified symmetric problem can be solved if RO_4 exists. □

5.5. Medical Record Nonforgeability. After decrypting D_{AB} (or D_{BA}), A (or B) have to authenticate each other via checking $T_S'''' + 3 \stackrel{?}{=} T_S'' + 3$ (or $T_S''' + 2 \stackrel{?}{=} T_S + 2$). If an attacker wants to forge a medical record Data_{BA} (or Data_{AB}), he/she has to evaluate the session key K_{AB} (or K_{BA}) to encrypt both Data_{BA} and $T_S + 3$ (or both Data_{AB} and $T_S'' + 2$). Since the attacker cannot evaluate the session key, our scheme provides medical record nonforgeability. Theorem 12 proves the property of data integrity from Definition 11.

Definition 11 (second joint modified symmetric encryption problem). Let $x_i, y_i \in Z$ and $c_i = E_k(x_i, y_i)$, $i = 1, 2, \ldots, n+1$. If c_{n+1} can be evaluated from given x_{n+1} and (x_j, c_j), $j = 1, 2, \ldots, n$, then we say the second joint modified symmetric encryption problem is solved (the probability of solving this problem is denoted as $\Pr(c_{n+1} \mid (x_j, c_j), x_{n+1}) = \varepsilon_5$).

Theorem 12 (medical record nonforgeability). *In our scheme, if D_{BA} can be modified successfully, then the second joint modified symmetric encryption problem can be solved.*

Proof. In our scheme, assume an adversary tries to forge $D_{BA}^{(n+1)}$ from $T_S^{(n+1)}$ and eavesdropped $(T_S^{(i)}, D_{BA}^{(i)})$, $i = 1, 2, \ldots, n$. Let RO_5 be a random oracle: input $T_S^{(n+1)}$ and $(T_S^{(i)}, D_{BA}^{(i)})$ to output $D_{BA}^{(n+1)}$ (i.e., $\mathrm{RO}_5((T_S^{(i)}, D_{BA}^{(i)}), T_S^{(n+1)}) \Rightarrow D_{BA}^{(n+1)}$). In Definition 11, let $T_S^{(i)} \leftarrow x_i - 2$, $D_{BA}^{(i)} \leftarrow c_i$ and $T_S^{(n+1)} \leftarrow x_{n+1} - 2$ be input parameters of RO_5 and obtain output $D_{BA}^{(n+1)}$. Let $c_{n+1} \leftarrow D_{BA}^{(n+1)}$, then c_{n+1} is evaluated. Therefore, $\Pr(D_{BA}^{(n+1)} \mid (T_S^{(i)}, D_{BA}^{(i)}), T_S^{(n+1)}) \leq \Pr(c_{n+1} \mid (x_i, c_i), x_{n+1}) = \varepsilon_5$, which means the second joint modified symmetric encryption problem can be solved if RO_5 exists. □

5.6. Resistance to Asynchronous Attacks. If an attacker wants to block a communication to make an asynchronous attack, he/she can use the following methods to cause A and S to update SID_A asynchronously, causing the system fail in the future.

(A) Blocking $A \rightarrow S : T_A, D_{SA}, \mathrm{SID}_A$: if S does not receive the data sent from A, S does not update SID_A and BSID_A, nor does A update SID_A. Therefore, an asynchronous attack based on this blocking method will fail.

(B) Blocking $S \rightarrow A : D_{AS}$: if A does not receive the data sent from S, A will not update SID_A. In the next authentication session, S will use BSID_A to determine the information of ID_A. Therefore, this blocking method is resisted.

Table 1: Comparison of computation and communication costs with verifier-based 3PAKA schemes without server public keys.

	Lee et al.'s scheme [8]			Wang-Mo's scheme [9]			Kwon et al.'s scheme [10]			Lin-Lee's scheme [7]			Our scheme		
	A	B	S	A	B	S	A	B	S	A	B	S	A	B	S
Exponentiation	3	4	4	4	4	6	4	4	10	4	4	6	1	1	0
X-or	1	1	2	1	1	2	0	0	0	1	1	2	0	0	0
Multip./division	0	0	0	0	0	0	3	3	4	0	0	0	0	0	0
Random number	1	1	2	1	1	2	1	1	4	1	1	2	0	0	0
Hash	3	3	4	3	3	4	3	3	4	4	4	4	1	0	1
Encryption/decryption	0	0	0	0	0	0	0	0	0	0	0	0	4	4	2
Transmission messages	3	6	4	3	6	4	3	10	3	6	7	4	4	2	3
Transmission rounds	2	3	4	2	3	4	2	4	2	4	4	4	2	2	2

Table 2: Security comparison with verifier-based 3PAKA schemes w/o server public keys.

Property	Lee et al.'s scheme [8]	Wang-Mo's scheme [9]	Kwon et al. 's scheme [10]	Lin-Lee's scheme [7]	Our scheme
Resistance to password guessing attacks	√	√	√	√	√
Resistance to verifier stolen attacks		√	√	√	√
Key confirmation				√	√
Resistance to impersonation attacks				√	√
Anonymity					√
Resistance to tracking attacks					√
Efficiency of implementation					√

(C) Blocking $S \rightarrow B$ or $B \rightarrow S$: blocking $S \rightarrow B$ or $B \rightarrow S$ has the same result as blocking $S \rightarrow A : D_{AS}$ which prevents asynchronous attacks.

(D) Blocking $A \rightarrow B$ or $B \rightarrow A$: blocking $A \rightarrow B$ or $B \rightarrow A$ does not affect any update of SID_A.

5.7. Resistance to Tracking Attack. Since $\mathrm{SID}_X \leftarrow h(\mathrm{ID}_X, \pi_X, T_X)$ changes in each round and the relationship between the previous and current SID_X and T_X cannot be found, where $X = A$ or B, the scheme is resistant to tracking attacks. Theorem 14 proves the property of data integrity from Definition 13.

Definition 13 (modified hash problem). Let $a_i, b_i, c_i \in Z$, $d_i = h(a_i, b_i, c_i)$, $i = 1, 2$. If $\mathrm{Equal}(a_1, a_2)$ can be evaluated from given d_1, d_2, c_1, and c_2, then we say the modified hash problem is solved, where $\mathrm{Equal}(x, y) = \{1, \text{if } x = y;\ 0, \text{otherwise}\}$ (the probability of solving this problem is denoted as $\Pr(\mathrm{Equal}(a_1, a_2) \mid d_1, d_2, c_1, c_2) = \varepsilon_6$).

Theorem 14 (resistance to tracking attack). *In our scheme, if attacker can evaluate Equal($ID_A^{(i)}, ID_A^{(j)}$), then the modified hash problem can be solved.*

Proof. In our scheme, assume an adversary tries to evaluate $\mathrm{Equal}(\mathrm{ID}_A^{(i)}, \mathrm{ID}_A^{(j)})$ to track user A from eavesdropped $\mathrm{SID}_A^{(i)}$, $\mathrm{SID}_A^{(j)}$, $T_A^{(i)}$, and $T_A^{(j)}$. Let RO_6 be a random oracle: input $\mathrm{SID}_A^{(i)}$, $\mathrm{SID}_A^{(j)}$, $T_A^{(i)}$, and $T_A^{(j)}$ to output $\mathrm{Equal}(\mathrm{ID}_A^{(i)}, \mathrm{ID}_A^{(j)})$ (i.e., $\mathrm{RO}_6(\mathrm{SID}_A^{(i)}, \mathrm{SID}_A^{(j)}, T_A^{(i)}, T_A^{(j)}) \Rightarrow \mathrm{Equal}(\mathrm{ID}_A^{(i)}, \mathrm{ID}_A^{(j)})$). In Definition 13, let $\mathrm{SID}_A^{(i)} \leftarrow d_i$, $\mathrm{SID}_A^{(j)} \leftarrow d_j$, $T_A^{(i)} \leftarrow c_i$, and $T_A^{(j)} \leftarrow c_j$ be input parameters of RO_6 and obtain output $\mathrm{Equal}(\mathrm{ID}_A^{(i)}, \mathrm{ID}_A^{(j)})$. Let $\mathrm{Equal}(a_1, a_2) \leftarrow \mathrm{Equal}(\mathrm{ID}_A^{(i)}, \mathrm{ID}_A^{(j)})$, then $\mathrm{Equal}(a_1, a_2)$ is evaluated. Therefore, $\Pr(\mathrm{Equal}(\mathrm{ID}_A^{(i)}, \mathrm{ID}_A^{(j)}) \mid \mathrm{SID}_A^{(i)}, \mathrm{SID}_A^{(j)}, T_A^{(i)}, T_A^{(j)}) \leq \Pr(\mathrm{Equal}(a_1, a_2) \mid d_1, d_2, c_1, c_2) = \varepsilon_6$, which means the modified hash problem can be solved if RO_6 exists. □

6. Comparison

This section compares the performance of our proposed method with previous verifier-based three-party authentication and key agreement (3PAKA) protocols without server public keys in terms of two aspects: computation and communication loadings (as shown in Table 1) and system properties (as shown in Table 2). From Table 1, our scheme is superior to previous schemes in terms of computation and communication performance. Table 2 shows that, unlike other schemes, our proposed scheme provides anonymity and resistance to tracking attacks. Therefore, our scheme is superior to previous schemes in terms of security.

Moreover, in Tables 3 and 4, we compare our proposed method with previous RSA-based 3PAKA schemes in terms of computation and communication loadings and system properties. Our protocol is a secure scheme providing 3PAKA and data exchange in medical environment, and the computation and communication loadings for providing only 3PAKA (without data exchange) in our scheme are different (lesser). In Table 4, Chang et al.'s [11] and Tso's [12] schemes do not support mutual authentication, and Deebak et al.'s scheme

Table 3: Comparison of computation and communication costs with RSA-based 3PAKA schemes.

	Chang et al.'s scheme [11]			Tso's scheme [12]			Farash and Attari's scheme [13]			Deebak et al.'s scheme [14]			Our scheme		
	A	*B*	*S*	*A*	*B*	*S*	*A*	*B*	*S*	*A*	*B*	*S*	*A*	*B*	*S*
Exponentiation	3	2	3	3	3	4	3	2	2	1	1	2	1	1	0
X-or	1	1	2	0	0	4	0	0	0	2	2	2	0	0	0
Multip./division	0	0	0	0	0	0	2	2	0	0	0	0	0	0	0
Random number	1	1	2	1	1	2	1	1	2	0	0	0	0	0	0
Hash	4	2	4	4	2	4	4	3	5	6	6	4	0	0	1
Encryption/decryption	0	0	0	0	0	0	0	0	0	0	0	0	2	2	2
Transmission messages	8	5	5	8	5	6	5	3	9	3	6	10	3	1	3
Transmission rounds	3	1	2	3	1	2	2	1	3	1	1	2	1	1	2

Table 4: Security comparison with RSA-based 3PAKA schemes.

Property	Chang et al.'s scheme [11]	Tso's scheme [12]	Farash and Attari's scheme [13]	Deebak et al.'s scheme [14]	Our scheme
Resistance to password guessing attacks	√	√	√	√	√
Resistance to verifier stolen attacks	N/A	N/A	N/A	√	√
Key confirmation	√	√	√	√	√
Resistance to impersonation attacks	√	√	√	√	√
Anonymity					√
Resistance to tracking attacks					√
Efficiency of implementation					√

Table 5: Comparison of computation and communication costs with other 3PAKA schemes.

	Chen et at.'s scheme [15]			Wang et al.'s scheme [16]			Farash et al.'s scheme [17]			Our scheme		
	A	*B*	*S*	*A*	*B*	*S*	*A*	*B*	*S*	*A*	*B*	*S*
Exponentiation	3	3	2	4	4	6	2	3	2	1	1	0
X-or	0	0	0	1	1	2	1	2	3	0	0	0
Multip./division	0	0	0	0	0	0	0	0	0	0	0	0
Random number	1	1	0	1	1	1	1	1	0	0	0	0
Hash	2	2	2	3	3	4	1	2	2	0	0	1
Encryption/decryption	0	0	0	2	2	3	0	0	0	2	2	2
Transmission messages	5	11	2	3	8	1	4	10	5	3	1	3
Transmission rounds	2	2	1	2	1	4	1	2	1	1	1	2

Table 6: Security comparison with other 3PAKA schemes.

Property	Chen et at.'s scheme [15]	Wang et al.'s scheme [16]	Farash et at.'s scheme [17]	Our scheme
Resistance to password guessing attacks	√	√	√	√
Resistance to verifier stolen attacks	√	√	N/A	√
Key confirmation	√	√	√	√
Resistance to impersonation attacks	√		√	√
Anonymity			√	√
Resistance to tracking attacks			√	√
Efficiency of implementation				√

[14] requires clients to logon the system successfully before starting the 3PAKA protocol in each time. In the logon phase of Deebak et al.'s scheme [14], each IP multimedia system (IMS) client enters his/her credentials into the registration form to avail the multimedia services, like video, voice, and data, and subsequently, the IMS server executes some steps to verify whether the client authorization is success or not. Moreover, each client has to perform two hash and two XOR functions in the logon phase, and the server has to perform four inverse computations in the authentication phase. Furthermore, we also compare our proposed method with other recently published 3PAKA schemes in terms of computation and communication loadings (Table 5) and system properties (Table 6). The schemes [15, 16] are smart card based schemes and some of their security and efficiency are based on smart cards. The properties "resistance to verifier-stolen attacks" of the schemes [11–13, 17] are all "N/A" because they are password-based schemes without verifiers. From Tables 3–6, our scheme is superior to previous RSA-based and other recently published 3PAKA schemes in terms of security and computation and communication performance.

7. Implementation

This section presents the implementation of our scheme in mobile phones (Android 4.1) and PCs (Windows 7). The mobile system is implemented on Google Nexus S with a 1 GHz processor and 512 MB RAM. The PC implementation used Windows 7 Professional with an Intel (R) core (TM) CPU i5-650 @3.2 Hz and 4 GB RAM. The server *S* (Server 1) and the user *B* (Server 2) are implemented on Windows 7, while the user *A* (Telecare) is implemented on Android. The hash function used is SHA-256 [23] and the symmetric encryption algorithm is AES [24]. Figure 6 shows the scheme flow in terms of data transmission and Figure 7 shows the data transfer renderings.

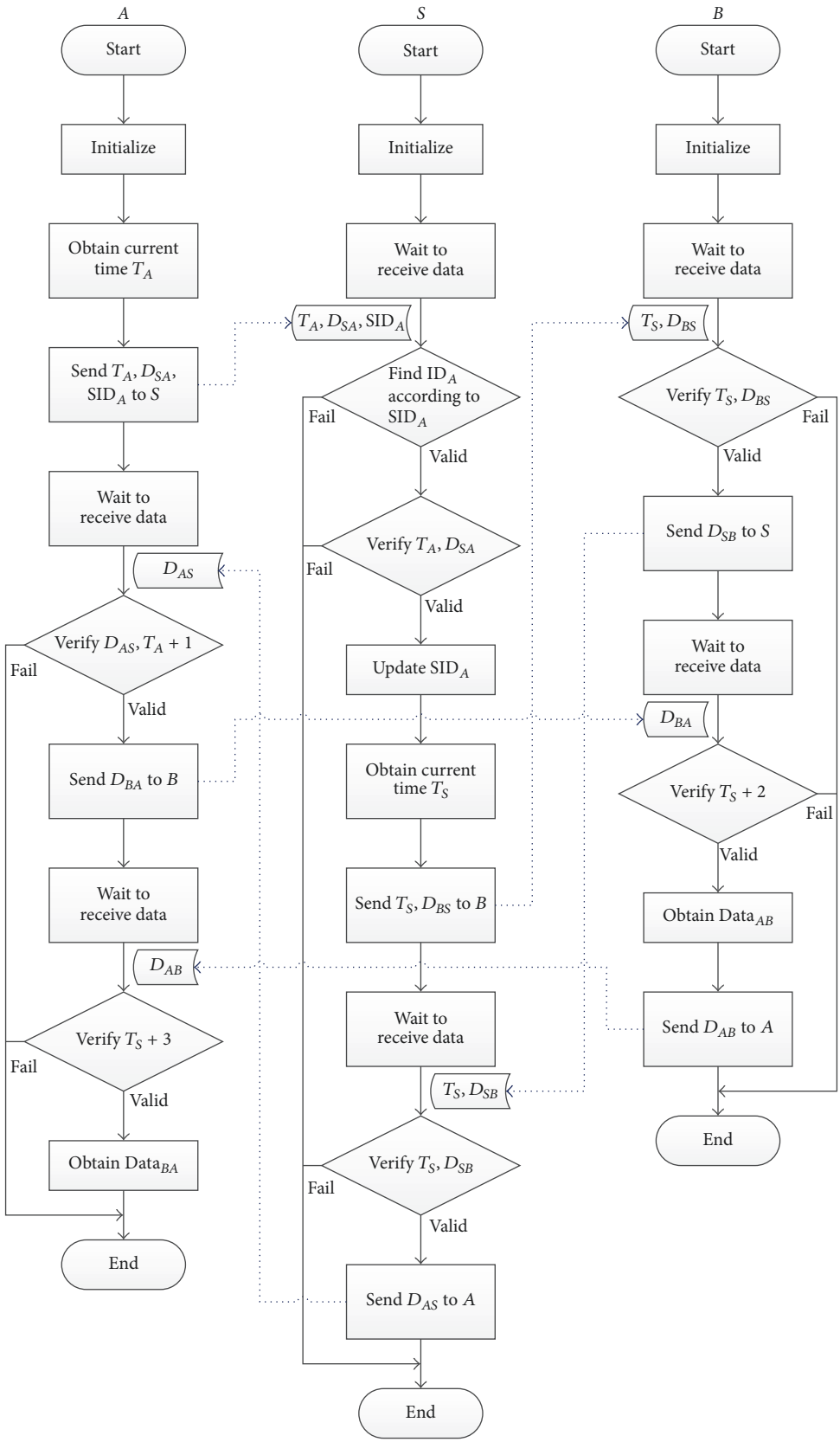
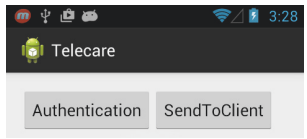
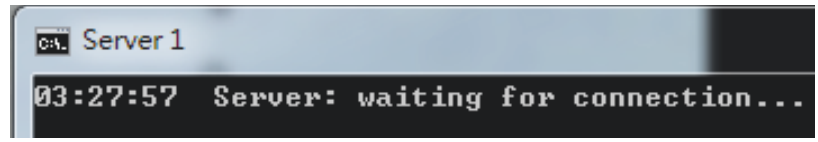


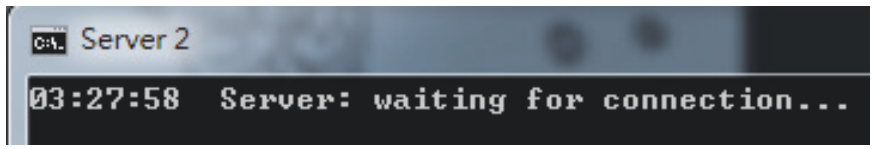
Figure 6: Application flowchart.



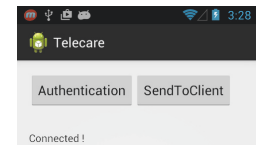
(a) Initial (on the end *A*)



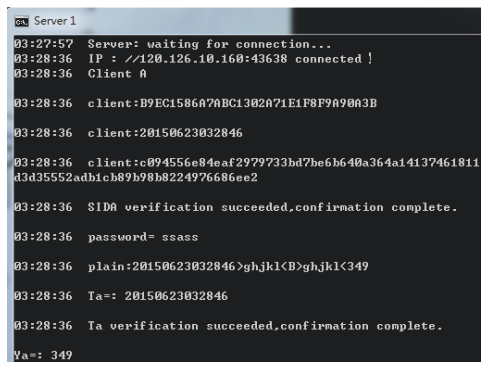
(b) Initial (on the end *S*)



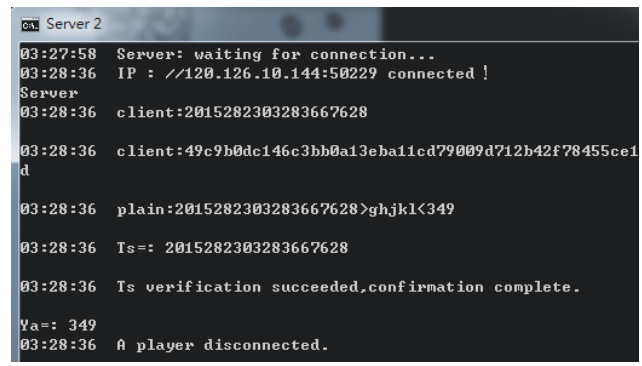
(c) Initial (on the end *B*)



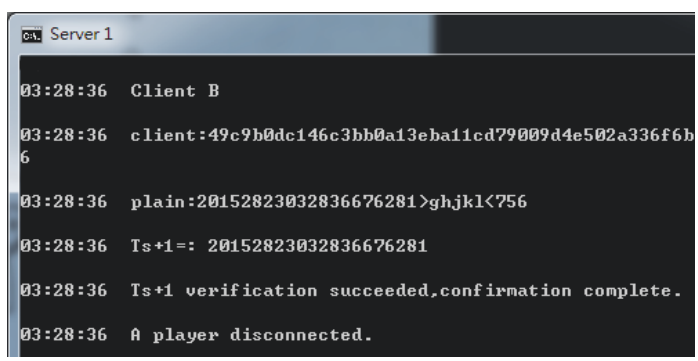
(d) Connected with *S* (on the end *A*)



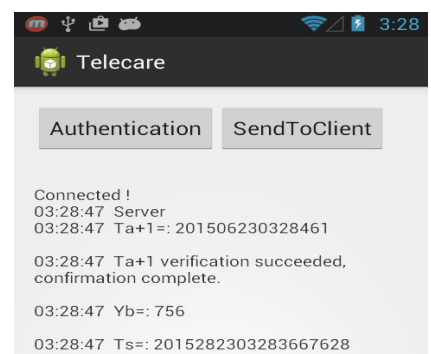
(e) Verification data received from *A* (on the end *S*)



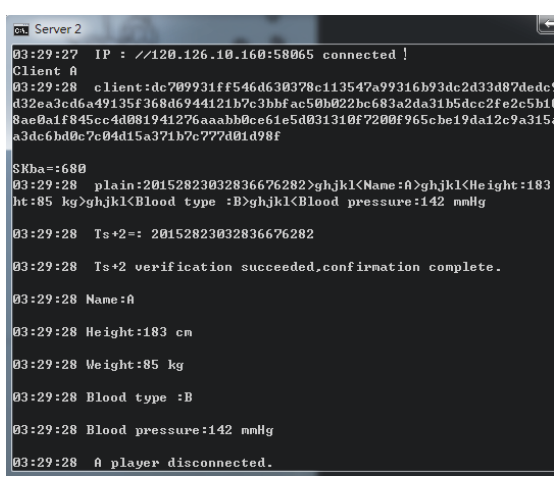
(f) Verification data received from *S* (on the end *B*)



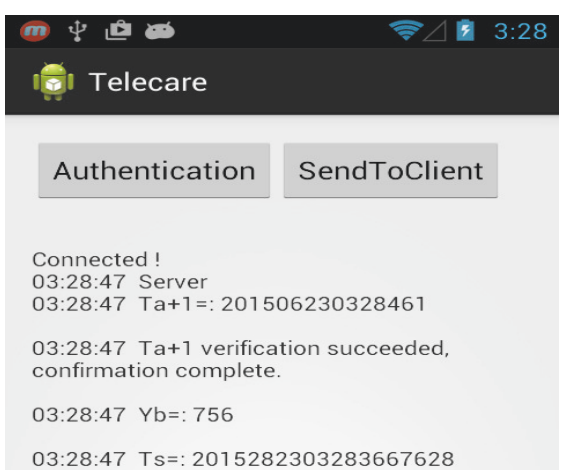
(g) Verification data received from *B* (on the end *S*)



(h) Verification data received from *S* (on the end *A*)



(i) (Verification) data received from *A* (on the end *B*)



(j) (Verification) data received from *B* (on the end *A*)

Figure 7: Data transfer renderings.

In our implementation, we assume that the system times of the server S and the users A and B are synchronized. However, their system times are difficult to be synchronized. Fortunately, the experience in implementation shows that the system time difference between the server and the users is within miniseconds. By assuming the maximum system time difference between the clients and the server is 1000 miniseconds and the values $T^{(c)} - T_A$ and $T^{(c)} - T_S$ are between 10 ms and 30 ms, we suggest to set T_{th_1} and T_{th_2} to −990 ms and 1030 ms, respectively (in real situation, the values $T^{(c)} - T_A$ and $T^{(c)} - T_S$ are suggested to be measured again for much accuracy).

8. Conclusion

In this paper, we review Lin-Lee's protocol and demonstrate its lack of anonymity and resistance to tracking attacks. We propose an enhanced three-party authentication scheme for use in telecare medicine information systems, which provides high standards of security issues and performance. The proposed scheme does not need server public keys, reduces computation costs, and resolves two significant security issues (anonymity and resistance to tracking attacks). Comparisons with other approaches show the proposed scheme provides improved security while incurring computational, communication, and transaction costs comparable to other methods.

Notations

A, B:	Medical institutions
S:	Server
p:	A large prime
g:	Primitive root modulo p
ID_X:	ID of X
SID_X:	Pseudo ID of X
BSID_X:	The last pseudo ID of X
T_X:	The time of X
$T^{(c)}$:	The current time
T_{th_i}:	The ith time threshold
x_A, x_B:	Private keys of A and B
y_A, y_B:	Public keys of A and B
π_X:	A symmetric key of X
K_{AB}, K_{BA}:	Section keys between A and B
D_{UV}:	Encrypted data from V to U
$h(\cdot)$:	A one-way hash function
$E_K(\cdot)$:	A symmetric encryption using key K
$D_K(\cdot)$:	A symmetric decryption using key K.

Disclosure

This article does not contain any studies with human participants or animals performed by any of the authors.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is partially supported by the Ministry of Science and Technology under Grant MOST 104-2221-E-182-012 and by the CGMH project under Grant BMRPB46.

References

[1] Y.-C. Chen, G. Horng, Y.-J. Lin, and K.-C. Chen, "Privacy preserving index for encrypted electronic medical records," *Journal of Medical Systems*, vol. 37, no. 6, article no. 9992, 2013.

[2] A. AlJarullah and S. El-Masri, "A Novel System Architecture for the National Integration of Electronic Health Records: A Semi-Centralized Approach," *Journal of Medical Systems*, vol. 37, no. 4, 2013.

[3] L. Liu, J. Lai, R. H. Deng, and Y. Li, "Ciphertext-policy attribute-based encryption with partially hidden access structure and its application to privacy-preserving electronic medical record system in cloud environment," *Security and Communication Networks*, vol. 9, no. 18, pp. 4897–4913, 2016.

[4] M. Wazid, A. K. Das, S. Kumari, X. Li, and F. Wu, "Design of an efficient and provably secure anonymity preserving three-factor user authentication and key agreement scheme for TMIS," *Security and Communication Networks*, vol. 9, no. 13, pp. 1983–2001, 2016.

[5] J. Noh, S. Lee, J. Park, S. Shin, and B. B. Kang, "Vulnerabilities of network OS and mitigation with state-based permission system," *Security and Communication Networks*, vol. 9, no. 13, pp. 1971–1982, 2016.

[6] M. Benssalah, M. Djeddou, and K. Drouiche, "Dual cooperative RFID-telecare medicine information system authentication protocol for healthcare environments," *Security and Communication Networks*, vol. 9, no. 18, pp. 4924–4948, 2016.

[7] T.-H. Lin and T.-F. Lee, "Secure verifier-based three-party authentication schemes without server public keys for data exchange in telecare medicine information systems," *Journal of Medical Systems*, vol. 38, no. 5, 2014.

[8] S.-W. Lee, H.-S. Kim, and K.-Y. Yoo, "Efficient verifier-based key agreement protocol for three parties without server's public key," *Applied Mathematics and Computation*, vol. 167, no. 2, pp. 996–1003, 2005.

[9] R.-C. Wang and K.-R. Mo, "Security enhancement on efficient verifier-based key agreement protocol for three parties without server's public key," *International Mathematical Forum. Journal for Theory and Applications*, vol. 1, no. 17-20, pp. 965–971, 2006.

[10] J. O. Kwon, I. R. Jeong, K. Sakurai, and D. H. Lee, "Efficient verifier-based password-authenticated key exchange in the three-party setting," *Computer Standards & Interfaces*, vol. 29, no. 5, pp. 513–520, 2007.

[11] T.-Y. Chang, M.-S. Hwang, and W.-P. Yang, "A communication-efficient three-party password authenticated key exchange protocol," *Information Sciences*, vol. 181, no. 1, pp. 217–226, 2011.

[12] R. Tso, "Security analysis and improvements of a communication-efficient three-party password authenticated key exchange protocol," *The Journal of Supercomputing*, vol. 66, no. 2, pp. 863–874, 2013.

[13] M. S. Farash and M. A. Attari, "An efficient and provably secure three-party password-based authenticated key exchange protocol based on Chebyshev chaotic maps," *Nonlinear Dynamics*, vol. 77, no. 1-2, pp. 399–411, 2014.

[14] B. D. Deebak, R. Muthaiah, K. Thenmozhi, and P. I. Swaminathan, "Analyzing three-party authentication and key agreement protocol for real time IP multimedia server–client systems," *Multimedia Tools and Applications*, vol. 75, no. 10, pp. 5795–5817, 2016.

[15] C. Chen, L. Xu, W. Fang, and T. Wu, "A Three-Party Password Authenticated Key Exchange Protocol Resistant to Stolen Smart Card Attacks," in *Proceedings of the 12th International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, vol. 1 of *Advances in Intelligent Information Hiding and Multimedia Signal Processing*, pp. 331–336.

[16] Q. Wang, O. Ruan, and Z. Wang, "Security Analysis and Improvements of Three-Party Password-Based Authenticated Key Exchange Protocol," in *Proceedings of the International Conference on Emerging Internetworking, Data and Web Technologies*, pp. 497–508, 2017.

[17] M. S. Farash, M. A. Attari, and S. Kumari, "Cryptanalysis and improvement of a three-party password-based authenticated key exchange protocol with user anonymity using extended chaotic maps," *International Journal of Communication Systems*, vol. 30, no. 1, 2017.

[18] R. Amin and G. P. Biswas, "A Novel User Authentication and Key Agreement Protocol for Accessing Multi-Medical Server Usable in TMIS," *Journal of Medical Systems*, vol. 39, no. 3, 2015.

[19] D. Mishra, A. K. Das, A. Chaturvedi, and S. Mukhopadhyay, "A secure password-based authentication and key agreement scheme using smart cards," *Journal of Information Security and Applications*, vol. 23, pp. 28–43, 2015.

[20] S.-Y. Chiou, Z. Ying, and J. Liu, "Improvement of a Privacy Authentication Scheme Based on Cloud for Medical Environment," *Journal of Medical Systems*, vol. 40, no. 4, article no. 101, pp. 1–15, 2016.

[21] S.-Y. Chiou, "Common friends discovery for multiple parties with friendship ownership and replay-attack resistance in mobile social networks," *Wireless Networks*, pp. 1–15, 2016.

[22] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *Proceedings of the 1st ACM conference on Computer and communications security*, pp. 62–73, 1993.

[23] SHA-256, http://www.cnblogs.com/elaron/archive/2013/04/09/3010375.html.

[24] AES, http://blog.csdn.net/hbcui1984/article/details/5201247.