Cryptanalysis and Improvement of an Improved Two Factor Authentication Scheme for Telecare Medicine Information Systems

Gaopeng Jian · Rongquan Feng

Abstract. Telecare medical information systems (TMIS) aim to provide healthcare services remotely. Efficient and secure mechanism for authentication and key agreement is required in order to guarantee the security and privacy of patients in TMIS. Recently Amin et al. proposed an improved RSA based user authentication and session key agreement protocol for TMIS after demonstrating some security pitfalls in Giri et al.’s scheme. They claimed that their improved protocol overcomes the weakness of Giri et al.’s scheme and resists all known attacks. However, our analyses show that Amin et al.’s protocol is vulnerable to offline identity-password guessing attacks once the victim’s card is compromised and does not provide perfect forward secrecy. Furthermore we propose a new ECC based anonymous authentication and key agreement scheme which is efficient and provides all security requirements.

Keywords Authentication · Telecare Medicine Information Systems · ECC · Smart card · User anonymity

1 Introduction

With the recent development in information science and communication technology, telecare medical information systems (TMIS) are widely used to provide remote healthcare services. By using TIMS, not only can patients receive desired treatments directly at home as they can establish communication with doctors over public Internet, which reduces their economic burdens, but also the hospitals can save precious resources such as beds and medical devices for other patients [28]. It may be noted that the only communication link between...
patients and doctors is the public Internet, which is insecure against various attacks such as eavesdropping, replaying and impersonating. What’s more, the message exchanged between TIMS server and patients (e.g. blood pressure, heart rate, etc.) as well as the information stored in TMIS server (e.g. health records) should not be modified by the adversary since these data are crucial for doctors to make decisions. Any modification of them may cause a substantial injury or even risk the patient’s life [17,22]. In addition to traditional security requirements, user anonymity has become an important issue in TMIS, which enables a remote patient to get proper healthcare services without revealing his name or identity to the doctor. To maintain the confidentiality, integrity and authenticity of data along with user anonymity, a secure authentication and key agreement scheme is usually employed for TIMS [2,10,5].

Since Lamport [20] introduced the first password based authentication scheme in 1981, lots of password only authentication schemes have been proposed to offer various levels of security for two-party setting [15], three-party setting [14], etc. Though such password only authentication schemes are relatively easy to implement, they suffer from two main threats: password stealing and password-table leakage [23]. In 1991, Chang et al. [4] proposed the first two factor authentication scheme combining the use of smart cards and passwords. Later on, there have been many two factor authentication schemes developed [13,8,19], whose security largely relies on the tamper-proof property of the smart cards. Unfortunately, the recent developments in side-channel attacks (e.g., monitoring the power consumption [15,21]) make it possible to extract the smart card information stored in its memory. Thus the smart card can no longer be regarded as fully tamper-proof devices and it’s desirable to design two factor authentication schemes based on the new assumption that smart cards are conditionally not tamper-proof [25], which means that their physical security can be breached at the hands of attackers for a sufficiently long time (e.g., a few hours) for performing side-channel attacks.

In 2012, Wu et al. [27] proposed a DLP based authentication and key agreement scheme for TMIS. However, He et al. [9] demonstrated that Wu et al.’s scheme was vulnerable to impersonation and privileged insider attacks, and also proposed an enhanced DLP based scheme for the same system requiring fewer exponentiation operations than Wu et al.’s scheme. Nevertheless, Wei et al. [26] pointed out that both Wu et al.’s scheme and He et al.’s scheme suffered from offline password guessing attacks. Furthermore, Wei et al. proposed an improved authentication scheme for TMIS against offline password guessing attacks. Unfortunately, it was proved by Zhu [29] that Wei et al.’s scheme was similar to the previous schemes and was still vulnerable to offline guessing attacks. In addition, Zhu proposed a new RSA based authentication scheme. But several security weaknesses such as vulnerable to parallel attacks and denial-of-service attacks were showed by Khan et al. [16] on Zhu’s scheme in 2013. And Khan et al. also proposed an improved scheme.

Recently, Giri et al. [7] illustrated that the Khan et al.’s scheme was insecure against offline password guessing attacks and also didn’t provide user
anonymity. They proposed an improved scheme to overcome the mentioned weaknesses. But their goals were not achieved, which was pointed out by Amin et al. [1] that their scheme was still vulnerable to offline guessing attacks as well as not providing user anonymity. After that, Amin et al. proposed an improved scheme over Giri et al.’s. However, our analyses in this paper reveal that Amin et al.’s scheme is also vulnerable to offline identity-password guessing attacks once the victim’s card is compromised, and does not provide perfect forward secrecy, which is an important security requirement for protocols. Then we propose a new ECC based two factor anonymous authentication and key agreement scheme. The proposed scheme not only achieves all security requirements, but also has better performance than previous schemes.

The rest of the paper is organized as follows. In Section 2 we briefly review Amin et al.’s scheme; In Section 3 we present the security weaknesses of Amin et al.’s scheme; In Section 4 we propose our ECC based anonymous authentication and key agreement scheme; In Section 5 and Section 6 we summarize the comparative security and performance analysis; We conclude the paper in Section 7.

2 Review of Amin et al.’s scheme

In this section, we will briefly review Amin et al.’s RSA based two factor scheme for TMIS [1]. The definition of notations used in Amin et al.’s scheme is summarized in Table 1 and the scheme is illustrated in Fig. 1 which consists of the following phases:

2.1 Initialization phase

To initialize, TIMS server \( S \) chooses two large primes \( p, q \) and computes \( n = pq \). Then \( S \) chooses a secure one way hash function \( h(\cdot) : \{0, 1\}^* \rightarrow \{0, 1\}^l \) as well as two integers \( c \) and \( d \) such that \( cd \equiv 1 \mod (p - 1)(q - 1) \). Finally, \( S \) publishes \((c, n)\) as its public key and keeps \( d \) secretly.

### Table 1 List of notations used in Amin et al.’s scheme

| Symbol | Definition |
|--------|------------|
| \( U_i \) | The \( i \)th patient/user |
| \( S \) | TIMS server |
| \( ID_i \) | Identity of user \( U_i \) |
| \( pw_i \) | Password of user \( U_i \) |
| \( \| \) | String concatenation operation |
| \( \oplus \) | Bitwise XOR operation |
| \( (e, n) \) | Public key of \( S \) |
| \( d \) | Secret key of \( S \) |
| \( h(\cdot) \) | A secure one way hash function |
| \( A \rightarrow B : C \) | message \( C \) is transferred over a public channel from \( A \) to \( B \) |
| \( A \Rightarrow B : C \) | message \( C \) is transferred over a secure channel from \( A \) to \( B \) |
Fig. 1 Amin et al.’s scheme

**User**

**Registration phase**

- Chooses ID\(_i\), pw\(_i\), a random number b\(_i\)
- Computes pwb\(_i\) = h(pw\(_i\)∥b\(_i\))

**TIMS Server**

- Computes R\(_i\) = h(ID\(_i\)∥d)
- Computes A\(_i\) = R\(_i\) ⊕ h(pwb\(_i\)∥ID\(_i\))
- Computes L\(_i\) = h(pwb\(_i\) ⊕ ID\(_i\))
- Stores \{A\(_i\), L\(_i\)\} into a smart card

**Smart card**

- Computes DP = b\(_i\) ⊕ h(ID\(_i\)∥pw\(_i\))
- Stores DP in the smart card

---

**User**

**Log & Authentication phase**

- Inputs ID\(_i\), pw\(_i\)
- Computes b\(_i\)' = DP ⊕ h(ID\(_i\)∥pw\(_i\))
- Computes pwb\(_i\)' = h(pw\(_i\)∥b\(_i\)')
- Computes L\(_i\)' = h(ID\(_i\) ⊕ pwb\(_i\)')
- Checks L\(_i\)' ⊆ L\(_i\)
- Computes a random number N\(_i\)
  - Computes R\(_i\)' = h(pwb\(_i\)∥ID\(_i\)) ⊕ A\(_i\)
  - Computes C\(_i\) = h(pwb\(_i\)∥N\(_i\)∥R\(_i\)')
  - Computes D\(_i\) = h(ID\(_i\)∥pwb\(_i\)') ⊕ N\(_i\)
  - Computes B\(_i\) = (ID\(_i\)∥pwb\(_i\)∥N\(_i\))^n mod n

**TIMS Server**

- Computes B\(_i\)' mod n = (ID\(_i\)∥pwb\(_i\)∥N\(_i\))
- Computes R\(_i\) = h(ID\(_i\)∥d)
- Computes N\(_i\)' = h(pwb\(_i\)∥ID\(_i\)) ⊕ D\(_i\)
- Checks N\(_i\)' ⊆ N\(_i\)
- Computes C\(_i\)' = h(pwb\(_i\)∥N\(_i\)∥R\(_i\))
- Checks C\(_i\)' ⊆ C\(_i\)
- Computes a random number N\(_2\)
  - Computes N\(_3\) = N\(_2\) ⊕ N\(_1\)
  - Computes K\(_i\) = h(R\(_i\)∥N\(_2\))
  - Computes SK = h(ID\(_i\)∥pwb\(_i\)∥N\(_i\)∥N\(_i\)'),
  - Computes SKV = h(SK∥ID\(_i\)"
- Computes SK = h(ID\(_i\)∥pwb\(_i\)∥N\(_i\)∥N\(_2\))
- Computes SKV' = h(SK∥ID\(_i\))
- Checks SKV' ⊆ SKV
2.2 Registration phase

The steps of the registration phase in Amin et al.’s scheme are presented below:

Step R1: $U_i$ chooses his identity $ID_i$, password $pw_i$;

Step R2: $U_i$ chooses a random number $b_i$ and computes $pwb_i = h(pw_i || b_i)$;

Step R3: $U_i \Rightarrow S$: $\{ID_i, pwb_i\}$;

Step R4: Upon receiving the registration message $\{ID_i, pwb_i\}$, $S$ computes $R_i = h(ID_i || d)$, $L_i = h(ID_i \oplus pwb_i)$ and $A_i = h(pwb_i || ID_i) \oplus R_i$;

Step R5: $S \Rightarrow U_i$: A smart card containing security parameters $\{A_i, L_i, n, e, h(\cdot)\}$;

Step R6: Upon receiving the smart card, $U_i$ computes $DP = h(ID_i || pwb_i) \oplus b_i$ and stores $DP$ in the memory of the smart card.

2.3 Login phase

In this phase, $U_i$ inserts his smart card to the card reader and keys in $ID_i$ and $pw_i$. The smart card executes the following operations:

Step L1: The smart card retrieves $b_i' = h(ID_i || pwb_i) \oplus DP$ and computes $pwb_i' = h(pw_i || b_i')$, $L_i' = h(ID_i \oplus pwb_i')$. Then the smart card checks whether $L_i'$ is equal to the stored $L_i$ or not. If they are unequal, the smart card rejects the session, otherwise chooses a random number $N_1$ and computes $R_i' = h(pwb_i' || ID_i) \oplus A_i$, $C_i = h(pwb_i' || N_1 || R_i')$, $D_i = h(ID_i || pwb_i') \oplus N_1$ and $B_i = (ID_i || pwb_i')^e \mod n$;

Step L2: $U_i \rightarrow S$: $\{C_i, B_i, D_i\}$.

2.4 Authentication and session key agreement phase

After receiving the login request from $U_i$, the following operations are performed between $S$ and $U_i$ to achieve mutual authentication and session key agreement:

Step A1: $S$ decrypts $B_i$ using the private key $d$ as $B_i^d \mod n = (ID_i || pwb_i' || N_1)$ and then computes $R_i = h(ID_i || d)$, $N_i' = h(ID_i || pwb_i') \oplus D_i$. Then $S$ compares $N_i'$ with $N_1$ and rejects if they are not equal; Otherwise, $S$ computes $C_i' = h(pwb_i' || N_1 || R_i)$ and checks whether $C_i'$ matches with the received $C_i$ or not. If the condition does not hold, $S$ aborts the connection. Then $S$ generates a random number $N_2$ and computes $N_3 = N_1 \oplus N_2$, $K_i = h(R_i || N_2)$;

Step A2: $S \rightarrow U_i$: $\{N_3, K_i\}$;

Step A3: On receiving the reply message $\{N_3, K_i\}$, $U_i$ computes $N_2' = N_3 \oplus N_1$, $K_i' = h(R_i' || N_2')$ and then matches $K_i'$ with the received $K_i$. If they are equal, $S$ and $U_i$ are mutually authenticated. After that, $U_i$ computes the session key $SK = h(ID_i || pwb_i' || N_1 || N_2')$ and $SKV = h(SK || ID_i)$;

Step A4: $U_i \rightarrow S$: $\{SKV\}$;

Step A5: $S$ computes $SK = h(ID_i || pwb_i' || N_1 || N_2)$, $SKV' = h(SK || ID_i)$ and checks whether $SKV' = SKV$ or not. If it holds, $S$ and $U_i$ agree upon a secret session key $SK$ for secure communication.
2.5 Password change phase

In this phase, $U_i$ changes his password $pw_i$ to a new one $pw^{\text{new}}_i$ without interacting with the server $S$ through the following steps:

Step P1: $U_i$ inserts his smart card into a card reader and enters his identity $ID_i$ and old password $pw_i$ and then submits a password change request.

Step P2: The smart card computes $b'_i = h(ID_i \parallel pw_i) \oplus DP$, $pw'_i = h(pw_i \parallel b'_i)$ and $L'_i = h(ID_i \oplus pw'_i)$. Then the smart card checks whether the computed $L'_i$ is equal to $L_i$ or not. If they are unequal, the smart card rejects $U_i$, otherwise asks $U_i$ to input a new password $pw^{\text{new}}_i$.

Step P3: On inputting $pw^{\text{new}}_i$, the smart card computes $R'_i = A_i \oplus h(pw^{\text{new}}_i \parallel ID_i)$, $pw^{\text{new}}_i = h(pw^{\text{new}}_i \parallel b'_i)$, $A^{\text{new}}_i = h(ID_i \parallel pw^{\text{new}}_i) \oplus R'_i$, $L^{\text{new}}_i = h(ID_i \oplus pw^{\text{new}}_i)$, $DP^{\text{new}} = DP \oplus h(ID_i \parallel pw_i) \oplus h(ID_i \parallel pw^{\text{new}}_i)$ and replaces $\{A_i, L_i, DP\}$ with $\{A^{\text{new}}_i, L^{\text{new}}_i, DP^{\text{new}}\}$.

2.6 Identity change phase

Since the phase has little relevance with our discussions, it is omitted here.

3 Security weaknesses of Amin et al.’s scheme

We make two widely accepted assumptions about the adversary’s capabilities:

1. The adversary is in total control of the public communication channel between the user and TIMS server. That means the adversary can eavesdrop, modify, delete and resend any messages transmitted in the public channel.
2. If the adversary gets access to a user’s smart card somehow, he gets all stored information of the smart card.

Under the above two assumptions, we show that Amin et al.’s scheme is insecure against offline identity-password guessing attacks and does not provide perfect forward secrecy in this section.

3.1 Offline identity-password guessing attacks

Suppose an adversary $A$ gets the smart card of a legal user $U_i$ by some means, he knows the parameters $\{DP, A_i, L_i\}$ stored in the smart card by assumption 2. Further according to assumption 1, $A$ has also intercepted the message $\{C_i, B_i, D_i\}$ exchanged in the login phase of one normal session. Then $A$ can guess $ID_i, pw_i$, by the following steps:

1. $A$ selects a pair $(ID^*_i, pw^*_i)$ from $D_{ID} \times D_{pw}$ where $D_{ID}$ and $D_{pw}$ denote the dictionary of the identity and the password respectively;
Table 2 List of notations used in the proposed scheme

| Symbol | Definition |
|--------|------------|
| $U_i$  | The $i$th patient/user |
| $S$    | TIMS server |
| $ID_i$ | Identity of user $U_i$ |
| $pw_i$ | Password of user $U_i$ |
| $\|$  | String concatenation operation |
| $\oplus$ | Bitwise XOR operation |
| $E/F_p$ | Elliptic Curve |
| $G$    | Base point over $E/F_p$ |
| $x$    | Master secret key of $S$ |
| $Y$    | Public key of $S$, where $Y = xG$ |
| $h(\cdot)$ | A secure one way hash function |
| $A \rightarrow B: C$ | message $C$ is transferred over a public channel from $A$ to $B$ |
| $A \Rightarrow B: C$ | message $C$ is transferred over a secure channel from $A$ to $B$ |

2. $A$ computes $b_i^* = DP \oplus h(ID_i^* || pw_i^*)$, $pw_i^* = h(pw_i^* || b_i^*)$, $R_i^* = h(ID_i^* || pw_i^*) \oplus A_i$, $N_1^* = D_i \oplus h(ID_i^* || pw_i^*)$, $C_i^* = h(pw_i^* || N_1^* || R_i^*)$ and checks whether $C_i^*$ is equal to $C_i$ or not. If they are equal, it implies that $A$ has selects the right pair $(ID_i^*, pw_i^*)$. Otherwise $A$ repeats the above steps until succeeding.

Since the identity and password of each user have low entropy, $A$ can enumerate all pairs $(ID_i^*, pw_i^*)$ within polynomial time. So Amin et al.’s scheme is vulnerable to offline identity-password guessing attacks.

3.2 Lack of perfect forward secrecy

An authentication and key agreement scheme is said to support perfect forward secrecy if the adversary $A$ having obtained TIMS server’s master secret key and the password $pw_i$ of a legal user $U_i$ is still not able to compute previously generated session keys. Amin et al.’s scheme does not provide perfect forward secrecy as $A$ can compute previous session keys if he knows the secret key $d$:

1. $A$ decrypts $B_i$ with $d$ as $B_i^d \mod n = (ID_i || pw_i || N_1)$;
2. $A$ computes $N_2 = N_3 \oplus N_1$;
3. $A$ computes the session key $SK = h(ID_i || pw_i || N_1 || N_2)$.

4 The proposed scheme

In this section we propose a new ECC based anonymous authentication and key agreement scheme. Our scheme is composed of four phases: initialization phase, registration phase, login & authentication phase and password change phase. For ease of presentation, the definition of notations used is listed in Table 2 and the phases are described in the following subsections. Fig 2 illustrates the registration and authentication phase.
Fig. 2 The proposed scheme

| User | TIMS Server |
|------|-------------|
| Registration phase | |
| Chooses $ID_i$ | ID$_i$ | Computes $A_i = h(ID_i || x)$
| | | Stores $A_i$ into a smart card |
| | Smart card | |
| Chooses $pw_i$ | | Computes $B_i = A_i \oplus h(pw_i)$
| | | Replaces $A_i$ with $B_i$ in the smart card |

| User | TIMS Server |
|------|-------------|
| Login & authentication phase | |
| Enters $ID_i$, $pw_i$ | | |
| Computes $A_i = B_i \oplus h(pw_i)$ | | |
| Chooses a random integer $a$ | | |
| Computes $Q_i = aG$ | | |
| Computes $K_i = aY$ | $\{Q_i, C_i, V_1, T_1\}$ | |
| Computes $C_i = ID_i \oplus h(K_i)$ | | Checks whether $T_2 - T_1 \leq \Delta T_i$
| Computes $V_1 = h(Q_i || K_i || A_i || T_1)$ | | Computes $K_i^* = xQ_i$
| | | Computes $ID_i^* = C_i \oplus h(K_i^*)$
| | | Checks $h(Q_i || K_i^* || h(ID_i^* || x) || T_1) \oplus V_1$
| | | Chooses a random integer $a_S$
| | | Computes $Q_S = a_SG$
| | | Computes $K_S = a_SQ_i$
| | | Computes $V_2 = h(Q_S || K_S || K_i^* || T_3)$
| | | $\{Q_S, V_2, T_3\}$ | |
| Checks whether $T_4 - T_3 \leq \Delta T_i$ | | Checks $h(K_S || V_2) \oplus V_3$
| | | Computes $K_S^* = a_SQ_S$
| | | Computes $V_3 = h(K_S^* || V_2)$
| | | Computes $SK = h(ID_i || K_2)$ | |
| | | | Checks $h(K_S || V_2) \oplus V_3$ |
4.1 Initialization phase

In this phase, TIMS server $S$ selects a prime number $p$ and chooses an elliptic curve $E/F_p$ as well as a base point $G$. Then $S$ selects a random integer $x \in \mathbb{Z}_p^*$ as its secret key and computes its public key $Y = xG$. Finally, $S$ selects a secure one way hash function $h(\cdot) : \{0,1\}^* \rightarrow \{0,1\}^l$ and publishes $(p, E/F_p, G, Y, h(\cdot))$ as system parameters and keeps $x$ secret.

4.2 Registration phase

This phase is meant to register a user $U_i$ with TIMS server $S$ for which the following steps are performed over a secure channel:

Step 1: $U_i$ chooses his identity $ID_i \in \{0,1\}^l$.
Step 2: $U_i \Rightarrow S : \{ID_i\}$.
Step 3: On receiving the registration request message from $U_i$, $S$ checks whether $ID_i$ exists in its database or not. If it already exists, $S$ asks $U_i$ for a different identity. Then $S$ computes the authenticator $A_i = h(ID_i \| x)$ and stores $ID_i$ in its database.
Step 4: $S \Rightarrow U_i :$ A smart card containing $(p, E/F_p, G, Y, h(\cdot), A_i)$ in its memory.
Step 5: On receiving the smart card, $U_i$ chooses a password $pw_i$ and replaces $A_i$ with $B_i = A_i \oplus h(pw_i)$ in the smart card.

4.3 Login & authentication phase

In this phase, the process of mutual authentication and key agreement are performed through the following steps over a public channel:

Step 1: $U_i$ inserts his smart card into a card reader and inputs $ID_i$ and $pw_i$.
Step 2: The smart card selects a random integer $a_i \in \mathbb{Z}_p^*$ and computes $A_i = B_i \oplus h(pw_i)$, $Q_i = a_iG$, $K_i = a_iY$, $C_i = ID_i \oplus h(K_i)$ and $V_i = h(Q_i \| K_i \| A_i \| T_1)$ where $T_1$ is the current timestamp.
Step 3: $U_i \rightarrow S : \{Q_i, C_i, V_i, T_1\}$.
Step 4: After receiving the message $\{Q_i, C_i, V_i, T_1\}$, $S$ checks whether $T_2 - T_1 \leq \Delta T_S$ where $T_2$ is the current timestamp and $\Delta T_S$ is the predetermined maximal time limit for transmission delay. If it doesn’t hold, $S$ terminates the session. Otherwise $S$ computes $K'_i = xQ_i$, $ID'_i = C_i \oplus h(K'_i)$ and checks the validity of the identity $ID'_i$ as well as if $h(Q_i \| K'_i \| h(ID'_i \| x) \| T_1)$ are equal to the received $V_i$. If either goes wrong, $S$ stops the process. Then $S$ selects a random integer $a_s \in \mathbb{Z}_p^*$ and computes $Q_S = a_sG$, $K_2 = a_sQ_i$, $V_2 = h(Q_S \| K_2 \| K'_i \| T_3)$ where $T_3$ is the current timestamp.
Step 5: $S \Rightarrow U_i : \{Q_S, V_2, T_3\}$.
Step 6: Upon receiving the message $\{Q_S, V_2, T_3\}$, $U_i$ checks whether $T_4 - T_3 \leq \Delta T_i$ where $T_4$ is the current timestamp and $\Delta T_i$ is the permitted time limit for transmission delay. If it doesn’t hold, $U_i$ terminates the session. Otherwise
Table 3 Security analysis

| Security Properties                                      | Khan et al. [16] | Giri et al. [7] | Amin et al. [1] | Proposed |
|----------------------------------------------------------|------------------|-----------------|-----------------|----------|
| Offline identity-password guessing attacks               | Insecure         | Insecure        | Insecure        | Secure   |
| Privileged insider attacks                               | Secure           | Secure          | Secure          | Secure   |
| Replay attacks                                           | Secure           | Secure          | Secure          | Secure   |
| Server impersonation attacks                             | Secure           | Secure          | Secure          | Secure   |
| User impersonation attacks                               | Secure           | Secure          | Secure          | Secure   |
| Man-in-the-middle attacks                                | Secure           | Secure          | Secure          | Secure   |
| User anonymity                                           | No               | No              | Yes             | Yes      |
| Perfect forward secrecy                                  | Yes              | No              | No              | Yes      |

\[ U_i \text{ computes } K_2^* = a_iQ_S \text{ and checks whether } h(Q_S||K_2^*||K_1||T_3) \text{ is equal to the received } V_2 \text{ or not. If they are not equal, } U_i \text{ stops the process. Then } U_i \text{ computes } V_3 = h(K_3^*||V_2) \text{ and the shared session key } SK = h(ID_i||K_2^*). \]

Step 7: \( U_i \rightarrow S : \{V_3\} \).

Step 8: \( S \) compares \( h(K_2^*||V_2) \) with the received \( V_3 \) and rejects if they are unequal.

Then \( S \) grants \( U_i \)'s login request and computes the shared session key \( SK = h(ID_i||K_2^*). \)

4.4 Password change phase

In this phase, \( U_i \) can change his password \( pw_i \) to a new one \( pw_{new,i} \) by the following way: He inserts his smart card into a card reader and keys in \( ID_i, pw_i, \) and \( pw_{new,i} \), then step 2, 3, 4, 5 in the authentication phase are performed successively. Upon receiving the reply message \( \{Q_S, V_2, T_3\} \), the smart card checks the validity of the timestamp \( T_3 \). If there is no problem, the smart card continues to compute \( K_2^* = a_iQ_S \text{ and compare } h(Q_S||K_2^*||K_1||T_3) \text{ with the received } V_2 \). If they are not equal, the smart card stops the process. Otherwise it computes \( B_{new,i} = h(pw_{new,i}^{new}) \oplus h(pw_i) \oplus B_i = A_i \oplus h(pw_{new,i}^{new}) \) and replaces \( B_i \) with \( B_{new,i} \).

5 Security analysis

In this section we informally analyse the security of the proposed scheme. It’s showed that the proposed scheme not only is immune from offline identity-password guessing attacks, privileged insider attacks, replay attacks, server impersonation attacks, user impersonation attacks and man-in-the-middle attacks, but also provides user anonymity and perfect forward secrecy. Table 3 illustrates the security comparison of the proposed scheme with some other schemes [16, 7, 1].
5.1 Offline identity-password guessing attacks

We have assumed that each user’s identity and password have low entropy, but an adversary can not successfully guess $ID_i$ or $pw_i$ offline if he steals $U_i$’s smart card and extracts parameters in the memory, as the only parameter related to $ID_i$ or $pw_i$ is $B_i = h(pw_i) \oplus h(ID_i \| x)$, but he doesn’t know $x$. The correct estimation of three values is infeasible in polynomial time \[3\]. Even if the adversary also eavesdrops all the previous message $\{Q_i, C_i, V_1, T_1, Q_S, V_2, T_3, V_3\}$ during protocol execution, he is still not able to extract the correct $ID_i$ or $pw_i$ as he doesn’t know $K_1$. According to the computational Diffie-Hellman assumption (CDH assumption [6]), it’s computationally intractable to compute $K_1 = a_i x G$ given $Y = x G$ and $Q_i = a_i G$. Therefore the proposed scheme prevents offline identity-password guessing attacks.

5.2 Privileged insider attacks

During the registration phase of the proposed scheme, $U_i$ only sends his identity $ID_i$ to TIMS server but doesn’t submit his password $pw_i$. Besides, the messages sent to TIMS server in the login & authentication phase, namely $\{Q_i, C_i, V_1, T_1\}$ and $\{V_3\}$, has nothing to do with $pw_i$. Therefore no privileged insider can obtain the user’s password. In other words, the proposed scheme could withstand privileged insider attacks.

5.3 Replay attacks

The proposed scheme is secure against replay attacks. First, the timestamps are generated and verified both at the user and server side to ensure freshness of every new session. Furthermore, even if an adversary may replay the eavesdropped message $\{Q_i, C_i, V_1, T_1\}$ within the permitted time limit for transmission delay, he cannot produce a valid response $\{V_3\}$ to the server’s challenge message $\{Q_S, V_2, T_3\}$ since he does not know $K_2 = a_i a_S G$, which can not be computed given $Q_S = a_S G$ and $Q_i = a_i G$. Therefore the proposed scheme resists replay attacks.

5.4 Server impersonation attacks

In the proposed scheme, an adversary can impersonate as legitimate TIMS server if he is able to produce a valid verification message $V_2$ to the users login request message $\{Q_i, C_i, V_1, T_1\}$. But the computation of $V_2$ involves $K_1 = a_i x G$, which is unknown given $Y = x G$ and $Q_i = a_i G$. Since the adversary does not know the server’s master secret key $x$, he fails to impersonate a legal TIMS server.
5.5 User impersonation attacks

In the proposed scheme, an adversary can impersonate as a legal user $U_i$ if he is able to forge the messages $\{Q_i, C_i, V_1, T_1\}$ and $\{V_3\}$. The problem comes from $C_i$ which involves $ID_i$ and $V_1$ which can be computed by $h(Q_i\|K_1\|(B_i \oplus h(pw_i))\|T_1)$ or $h(Q_i\|K_1\|h(ID_i\|x)\|T_1)$ while the adversary doesn’t know $ID_i$ and $pw_i$. Therefore the proposed scheme is secure against user impersonation attacks.

5.6 Man-in-the-middle attacks

It has been proven in the previous two subsections that the proposed scheme is secure against the user and server impersonation attacks, so man-in-the-middle attacks, which can only succeed if an adversary can pass through the authentication from the user and TIMS server, are impossible.

5.7 User anonymity

The proposed scheme ensures user anonymity. In the login & authentication phase $U_i$’s identity $ID_i$ is not sent over a public channel but rather a pseudo identity $C_i$, which is fresh for each session. $ID_i$ can only be revealed by using the server’s master secret key $x$ to get $K_1$. Hence the proposed scheme provides user anonymity.

5.8 Perfect forward secrecy

In the proposed scheme, the session key $SK = h(ID_i\|K_2)$ where $K_2 = a_S a_i G$. The freshness of $SK$ is guaranteed as $U_i$ chooses a new random $a_i$ and $S$ selects a new random $a_S$ for each session. The adversary who has a knowledge of $Q_S = a_S G$, $Q_i = a_i G$, $x$ and $pw_i$ is not able to compute the session key unless he knows the session specific $a_i$ or $a_S$. Therefore the proposed scheme provides perfect forward secrecy.

6 Performance analysis

In this section we compare our proposed scheme with Amin et al.’s scheme [1] and other related schemes [16,7] in terms of computation cost and size of exchanged message and smart card storage. The results are summarized in Table 4.

In order to evaluate computation cost, we neglect the XOR and concatenation operations due to their minor costs and introduce the following notations:

1. $T_{tec}$: time for performing a modular exponentiation;
Table 4 Performance analysis

| Schemes                      | Khan et al. [16] | Giri et al. [7] | Amin et al. [1] | Proposed |
|------------------------------|------------------|-----------------|-----------------|----------|
| Computation cost in the registration phase | $4T_h + 1T_{mc}$ ≈ 524ms | $5T_h$ ≈ 2.5ms | $5T_h + 1T_{mc}$ ≈ 524.5ms | $2T_h$ ≈ 1ms |
| Computation cost in the login & authentication phase | $10T_h + 5T_{mc}$ ≈ 2615ms | $6T_h + 1T_{mc}$ ≈ 525ms | $8T_h + 1T_{mc}$ ≈ 526ms | $6T_{pm} + 12T_h$ ≈ 384.45ms |
| Exchanged message size       | 120 bytes        | 228 bytes       | 228 bytes       | 160 bytes |
| Smart card storage size      | 100 bytes        | 208 bytes       | 188 bytes       | 80 bytes  |

2. $T_{pm}$: time for performing an elliptic curve point multiplication;
3. $T_h$: time for performing a hash function operation.

According to [12,11], in average we have $T_{mc}$ ≈ 522ms, $T_{pm}$ ≈ 63.075ms and $T_h$ ≈ 0.5ms.

For comparison of size, we assume that the hash values and timestamps are 160 bits long and the key length of ECC is 160 bits while 1024 bits for RSA to achieve the equivalent level of security [24].

In the registration phase the proposed scheme requires two hash function operations, so the computation cost is $2T_h$ ≈ 1ms. In the login & authentication phase the proposed scheme requires six elliptic curve point multiplication operations and twelve hash function operations, so the computation cost is $6T_{pm} + 12T_h$ ≈ 384.45ms. The size of exchanged message in the login & authentication phase is $8 \times 160$ bits = 160 bytes ($\{Q_i, C_i, V_1, V_2, V_3, T_1, Q_S, V_2, V_3\}$) and of smart card storage is $4 \times 160$ bits = 80 bytes ($\{A_i, p, G, Y\}$).

We can see from Table 3 that our proposed scheme resists all known attacks while others are vulnerable to various kinds of attacks, and our proposed scheme supports user anonymity and perfect forward secrecy while others may be in lack. Besides, Table 4 reveals that our proposed scheme is much faster in both the registration phase and login & authentication phase than others. For size comparison, except taking a relatively little bit more than Khan et al.’s scheme [10] in terms of exchanged message size, our proposed scheme is superior. Therefore, the proposed scheme is an eligible authentication and key agreement scheme for TMIS.

7 Conclusion

In this paper, we analyse Amin et al.’s RSA based user authentication and session key agreement protocol for TMIS and show that it is insecure against offline identity-password guessing attacks as well as no providing perfect forward secrecy. In order to improve Amin et al.’s scheme, we propose a new ECC based anonymous authentication and key agreement scheme for TIMS. Detailed analyses confirm that the proposed scheme is robust against all known attacks and more efficient than previous schemes.
References

1. Ruhul Amin and G. P. Biswas. An improved rsa based user authentication and session key agreement protocol usable in tmis. *Journal of Medical Systems*, 39, 2015.

2. Hamed Arshad and Mortaza Nikooghadam. Three-factor anonymous authentication and key agreement scheme for telecare medicine information systems. *Journal of Medical Systems*, 38(38):130–136, 2014.

3. Shelzad Ashraf Ch, Muhammad Sher, Anwar Ghani, Husnain Naqvi, Azeem Irshad, et al. An efficient signcryption scheme with forward secrecy and public verifiability based on hyper elliptic curve cryptography. *Multimedia Tools and Applications*, 74(5):1711–1723, 2015.

4. C. C. Chang and T. C. Wu. Remote password authentication with smart cards. *Computers & Digital Techniques Iee Proceedings E*, 138(3):165–168, 1991.

5. Mishra Dheerendra, Mukhopadhyay Sourav, Chaturvedi Ankit, Kumari Saru, and Khan Muhammad Khurram. Cryptanalysis and improvement of yan et al.’s biometric-based authentication scheme for telecare medicine information systems. *Journal of Medical Systems*, 38(6):136–136, 2014.

6. Whitfield Diffie and Martin E Hellman. New directions in cryptography. *Information Theory, IEEE Transactions on*, 22(6):644–654, 1976.

7. Debasis Giri, Tanmoy Maitra, Ruhul Amin, and P. D. Srivastava. An efficient and robust rsa-based remote user authentication for telecare medical information systems. *Journal of Medical Systems*, 39:145–145, 2015.

8. Debiao He, Jianhua Chen, Jin Hu, Debiao He, Jianhua Chen, and Jin Hu. An id-based client authentication with key agreement protocol for mobile clientserver environment on ecc with provable security. *Information Fusion*, 13(3):223230, 2012.

9. Debiao He, Jianhua Chen, and Rui Zhang. A more secure authentication scheme for telecare medicine information systems. *Journal of Medical Systems*, 36(3):1989–1995, 2012.

10. Debiao He, Neeraj Kumar, Naveen Chilamkurti, and Jong Hyouk Lee. Lightweight ecc based ftd authentication integrated with an id verifier transfer protocol. *Journal of Medical Systems*, 38(10):460–483, 2014.

11. WenBin Hsieh and JenqShiou Leu. Anonymous authentication protocol based on elliptic curve diffie & hellman for wireless access networks. *Wireless Communications & Mobile Computing*, 14(10):995–1006, 2014.

12. Qi Jiang, Jianfeng Ma, Guangsong Li, and Li Yang. An efficient ticket based authentication protocol with unlinkability for wireless access networks. *Wireless Personal Communications*, 77(2):1–18, 2014.

13. Yixin Jiang, Chuang Lin, Xuemin Shen, and Minghui Shi. Mutual authentication and key exchange protocols for roaming services in wireless mobile networks. *Wireless Communications IEEE Transactions on*, 5(9):2569 – 2577, 2006.

14. Nam Junghyun, Kim Kwang Raymond, Paik Juryon, and Won Dongho. An offline dictionary attack against abdalla and pointcheval key exchange in the password-only three-party setting. *Ieee Trans Fundamentals*, 2015.

15. Jonathan Katz, Rafail Ostrovsky, and Moti Yung. Efficient and secure authenticated key exchange using weak passwords. In *JOURNAL OF THE ACM*, 2009.

16. Muhammad Khurram Khan and Saru Kumari. An authentication scheme for secure access to healthcare services. *Journal of Medical Systems*, 37(4):656–658, 2012.

17. Kee-Won Kim and Jae-Dong Lee. On the security of two remote user authentication schemes for telecare medical information systems. *Journal of medical systems*, 38(5):1–11, 2014.

18. P. Kocher, J. Jaffe, B. Jun, P. Kocher, J. Jaffe, and B. Jun. Introduction to differential power analysis and related attacks. *Journal of Cryptographic Engineering*, 1(1):5–27, 2011.

19. Saru Kumari and Muhammad Khurram Khan. More secure smart cardbased remote user authentication scheme with user anonymity. *Security & Communication Networks*, volume 7(11):2039–2053(15), 2013.

20. Leslie Lamport. Password authentication with insecure communication. *Communications of the ACM*, 24(11):770–772, 1981.
21. Thomas S. Messerges, Ezzat A. Dabbish, Robert H. Sloan, and Senior Member. Examining smart-card security under the threat of power analysis attacks. In IEEE Transactions on Computers, pages 541–552, 2002.
22. Dheerendra Mishra. On the security flaws in id-based password authentication schemes for telecare medical information systems. Journal of medical systems, 39(1):1–16, 2015.
23. Chwei Shyong Tsai, Cheng Chi Lee, and Min Shiang Hwang. Password authentication schemes: Current status and key issues. International Journal of Network Security, (2):101–115, 2006.
24. Scott A Vanstone. Elliptic curve cryptosystem—the answer to strong, fast public-key cryptography for securing constrained environments. Information Security Technical Report, 2(2):78–87, 1997.
25. Yongge Wang. Password protected smart card and memory stick authentication against off-line dictionary attacks. In Information Security and Privacy Research, pages 489–500. Springer, 2012.
26. Jianghong Wei, Xuexian Hu, and Wenfen Liu. An improved authentication scheme for telecare medicine information systems. Journal of Medical Systems, 36(6):3597–3604, 2012.
27. Zhen Yu Wu, Yueh Chun Lee, Feipei Lai, Hung Chang Lee, and Yufang Chung. A secure authentication scheme for telecare medicine information systems. Journal of Medical Systems, 36(3):1529–1535, 2012.
28. Qi Xie, Jun Zhang, and Na Dong. Robust anonymous authentication scheme for telecare medical information systems. Journal of medical systems, 37(2):1–8, 2013.
29. Zhian Zhu. An efficient authentication scheme for telecare medicine information systems. Journal of Medical Systems, 36(6):3833–3838, 2012.