RESEARCH ARTICLE

# Security Analysis and Improvement of 'a More Secure Anonymous User Authentication Scheme for the Integrated EPR Information System'

**SK Hafizul Islam**[1] *, **Muhammad Khurram Khan**[2], **Xiong Li**[3]

**1** Department of Computer Science and Information Systems, Birla Institute of Technology and Science, Pilani, Rajasthan 333031, India, **2** Center of Excellence in Information Assurance, King Saud University, Riyadh, Saudi Arabia, **3** School of Computer Science and Engineering, Hunan University of Science and Technology, Hunan 411201, Xiangtan, China

* hafi786@gmail.com

**Citation:** Islam SH, Khan MK, Li X (2015) Security Analysis and Improvement of 'a More Secure Anonymous User Authentication Scheme for the Integrated EPR Information System'. PLoS ONE 10 (8): e0131368. doi:10.1371/journal.pone.0131368

**Editor:** Yongtang Shi, Nankai University, CHINA

**Received:** January 5, 2015

**Accepted:** June 1, 2015

**Published:** August 11, 2015

**Data Availability Statement:** All data are avaliable in the paper.

**Funding:** The first author is supported by the Outstanding Potential for Excellence in Research and Academics (OPERA) award, Birla Institute of Technology and Science (BITS) Pilani, Pilani Campus, Rajasthan, India. The authors also extend their sincere appreciation to the Deanship of Scientific Research at King Saud University for its funding of this Prolific Research Group (PRG-1436-16). The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

## Abstract

Over the past few years, secure and privacy-preserving user authentication scheme has become an integral part of the applications of the healthcare systems. Recently, Wen has designed an improved user authentication system over the Lee et al.'s scheme for integrated electronic patient record (EPR) information system, which has been analyzed in this study. We have found that Wen's scheme still has the following inefficiencies: (1) the correctness of identity and password are not verified during the login and password change phases; (2) it is vulnerable to impersonation attack and privileged-insider attack; (3) it is designed without the revocation of lost/stolen smart card; (4) the explicit key confirmation and the no key control properties are absent, and (5) user cannot update his/her password without the help of server and secure channel. Then we aimed to propose an enhanced two-factor user authentication system based on the intractable assumption of the quadratic residue problem (QRP) in the multiplicative group. Our scheme bears more securities and functionalities than other schemes found in the literature.

## 1 Introduction

Due to the rapid progress of the communication technologies and information security, anonymous and secure remote user mutual authentication schemes are widely employed in the integrated electronic patient record (EPR) information system [1–8]. The online services provided by the EPR information system not only save patient's valuable time, but also helps doctor to take correct and quick clinical decision based on the digital information available on the remote location server of EPR information system [9–11]. In addition, with this online facility, the patient residing at home can access his/her confidential health report [12–15] stored on the EPR server through the internet. On the other hand, the doctor can access and analyze patient's

**Competing Interests:** The authors have declared that no competing interests exist.

data and can also inform the patients in a timely manner. Accordingly, to provide such type of facilities to the patients and the doctors, many healthcare systems are now being replaced the traditional paper-based system with digital service over wireless networks [16–21]. However, the privacy and confidentiality of patient health data must be maintained when these are accessed from the server over the internet [22–24]. Since the internet is ubiquitous in nature and thus the malicious adversaries may try to collect the confidential data of the patients. Thus, a robust and flexible authentication scheme usable in integrated EPR information system is required to access patient's data over any insecure channel [25–29].

## 1.1 Related Works

In order to maintain the security and privacy of the integrated EPR information system, many smart card based (two-factor) user authentication systems have been presented recently [2, 3, 30–34]. However, it has been analyzed from the security community that the previous schemes are no longer provide required security and functional requirements of a robust user authentication system [12, 13, 17, 25, 28, 29]. In 2012, Wu et al. [32] devised a new user authentication scheme for the integrated EPR information system with password and smart card. Then they argued that their scheme [32] resists all the vulnerabilities and includes all the functionalities. However, Lee et al. [2] demonstrated that Wu et al.'s scheme [32] is incapable to resist the stolen verifier attack and the lost smart card attack. Then an improved scheme was proposed by them and claimed that the scheme [2] is strong enough to remove the known vulnerabilities. Recently, Wen [3] has adopted the intractability assumption of the quadratic residue problem (QRP) [35, 36] and designed an enhanced scheme over the scheme proposed by Lee et al. [2].

## 1.2 Motivation and Contribution

The Wen's scheme [3] is analyzed to be secure and efficient than other schemes [2, 35], however, this paper identifies many inefficiencies on Wen's scheme [3]. This paper carefully analyzed that Wen's scheme [3] is suffering from the following problems: (1) it can not check user identity and password in the login and password change phases; (2) it is weak against the impersonation attack and privileged-insider attacks; (3) it has no facility to revoke the lost/stolen smart card; (4) the *explicit key confirmation* and the *no key control* properties of the session key are absent, and (5) it does not update user password without any secure channel and the remote server's assistance. In this study, the authors have considered all the security and functionality features, and consequently presented a new user authentication scheme, which is suitable for the application of integrated EPR information system. The performance studies have proved that the proposed design has eliminated the pitfalls of Wen's scheme [3]. Our user authentication would be more applicable for healthcare applications, such as the integrated EPR information system.

## 1.3 Organization of the Paper

We organized the rest parts of this paper as follows. The quadratic residue problem required to understand the rest of this paper is explained in Section 2. We explained the Wen's authentication scheme in Section 3. The weaknesses of Wen's scheme are presented in Section 4. The improved scheme is proposed in Section 5, and its security and functionality discussions are proposed in Section 6. The Section 7 provides a comparative analysis and the Section 8 concludes the paper.

## 2 Quadratic Residue Problem

In this section, we briefly introduce the quadratic residue problem (QRP) [36]. Suppose that the composite number $n$ is the product of two large prime numbers $p$ and $q$. We can say that $b$ is a quadratic residue modulus $n$, if the equation $b \equiv a^2 \bmod n$ is solvable in the multiplicative group $Z_n^*$. The set of quadratic residue modulo $n$ is defined as

$$QR_n \quad = \quad \{b : \exists\ a \in Z_n^* \text{ such that } b \equiv a^2 \bmod n\} \tag{1}$$

In cryptography, many schemes/protocols [3, 35] are designed under the intractability assumption of the QRP. The hardness assumption of QRP is equivalent to the factoring the large modulus $n$. That is for given $b \in QR_n$, it is infeasible for a polynomial time bounded algorithm to find $a$ without factoring the public modulus $n$.

## 3 Description of the Wen's User Authentication Scheme

Here, we present Wen's two-factor user authentication scheme [3]. Initially, the remote medical server $S$ selects two large prime numbers $p$, $q$ and calculates the modulus as $n = pq$. Now, $S$ made public $n$, whereas $p$ and $q$ are kept secret. The list of notations needed to understand the later part of the paper are described in Table 1.

The following phases are used to described Wen's authentication scheme.

### 3.1 Registration Phase

In this phase, the patient $U_i$ performs the registration through secure channel to the integrated EPR information server $S$ in order to obtain a valid smart card. We explained this phase by the following steps:

**Step 1**. $U_i$ sends a registration request with his/her $\langle ID_i, PW_i\rangle$ to $S$ over a secure channel.

**Step 2**. $S$ verifies the correctness of $ID_i$ and computes $v = H(K \oplus ID_i)$.

**Step 3**. $S$ calculates $s_1 = H(PW_i||K)$, $s_2 = H(H(PW_i||s_1))$ and $N = v \oplus s_2$.

**Step 4**. $S$ initiates a counter $c_i = 0$ against $U_i$ and insert a tuple $\langle ID_i, c_i\rangle$ in the database. Then $S$ issues a new smart card against $U_i$ that includes the information $\langle H(\cdot), N, s_1, c_i\rangle$.

**Table 1. Descriptions of various notations.**

| Notations | Description |
|---|---|
| $U_i$ | The patient (User) |
| $ID_i$ | The identity of $U_i$ |
| $PW_i$ | The password of $U_i$ |
| $S$ | The medical server of integrated EPR information system |
| $K$ | The secret key of $S$ |
| $c_i$ | The counter maintained in $S$'s database against the user $U_i$ |
| $H(\cdot)$ | The secure and collision-resistance one-way hash function |
| $p$, $q$ | Two large prime numbers |
| $n$ | The publicly known modulus such that $n = pq$ |
| $b \in_R Z_n^*$ | The number $b$ randomly chosen from $Z_n^*$ |
| $\oplus$ | The bitwise XOR operator |
| $\|\|$ | The concatenation operator |
| $SK$ | The session key agreed between $U_i$ and $S$ |
| $\mathcal{A}$ | The active/passive adversary |

doi:10.1371/journal.pone.0131368.t001

**Step 5**. $S$ sends the smart card to $U_i$ over a secure channel.

## 3.2 Login Phase

For the login purpose, $U_i$ performs the following steps:

**Step 1**. $U_i$ inserts the smart card into the specific card reader and keys his/her $\langle ID_i, PW_i\rangle$. Smart card then selects a number $r$ and computes $s_2 = H(H(PW_i||s_1))$.

**Step 2**. Smart card computes $c_i = c_i + 1$ and $M_1 = (ID_i||N||s_2||r||c_i)^2 \bmod n$. Now, $U_i$ sends $M_1$ as a login message to $S$ over a public network.

## 3.3 Authentication Phase

In this phase, the user (patient) $U_i$ and the server $S$ perform mutual authentication and then agreed on common secret session key. The description of this phase is given with the following steps:

**Step 1**. When $S$ received $M_1$, then extracts $(ID_i||N||s_2||r||c_i)$ from $M_1$ based on Chinese Remainder Theorem (CRT) using the secret primes $p$ and $q$. Now, $S$ takes the tuple $\langle ID_i, c_i'\rangle$ from his/her own database and verifies whether $c_i' > c_i$ holds. If $c_i' > c_i$ is incorrect, then $S$ aborts the session. Otherwise, $S$ updates the tuple $\langle ID_i, c_i'\rangle$ to $\langle ID_i, c_i\rangle$ and continues to the next steps.

**Step 2**. $S$ computes $v = H(K \oplus ID_i)$, $s_2' = N \oplus v$ and verifies it with $s_2$. If $s_2' = s_2$, $S$ then accepts $U_i$ as an legitimate user. $S$ computes the session key $SK = H(s_2||r||1)$.

**Step 3**. $S$ also performs the calculation of the response message as $M_2 = H(s_2||r||0)$ and then sends it to $U_i$ over a public network.

**Step 4**. When $U_i$ received $M_2$, then computes $M_2' = H(s_2||r||0)$ and checks whether $M_2' = M_2$ is correct or not. If $M_2' \neq M_2$, $U_i$ aborts the session. Otherwise, $U_i$ authenticates $S$ and computes the session key $SK = H(s_2||r||1)$.

The complete description of login phase and authentication phase of Wen's scheme [3] is further presented in Table 2.

## 3.4 Password Change Phase

This phase is executed by $U_i$ and in the cooperation of $S$. By this phase, $U_i$ is allowed to update his/her old password to a new password with the following operations:

**Step 1**. $U_i$ delivers his/her $\langle ID_i, PW_i, PW_{new}\rangle$ to $S$ using a secure channel.

**Step 2**. $S$ computes $v = H(K||ID_i)$, $s_1^* = H(PW_{new}||K)$, $s_2^* = H(H(PW_{new} \, || \, s_1^*))$ and $N^* = v \oplus s_2^*$. $S$ then securely sends $\langle s_1^*, N^*\rangle$ to $U_i$. On receiving $\langle s_1^*, N^*\rangle$ from $S$, $U_i$ updates the old smart card's memory as $\langle ID_i, H(\cdot), N^*, s_1^*\rangle$.

**Note**: In the password change phase of Wen's scheme [3], the counter $c_i$ is not incorporated in the smart card and we consider it as typo. Here we assumed that $S$ sends the tuple $\langle s_1^*, N^*\rangle$ to $U_i$ and then $U_i$ updates the old smart card's memory to $\langle H(\cdot), N^*, s_1^*, c_i\rangle$.

# 4 Security Pitfalls of Wen's Authentication Scheme

This section is presented to identify and analyze the security and design issues of Wen's authentication scheme [3]. The following problems have been observed and their detailed descriptions are given below:

**Table 2. Login and Authentication phases of Wen's scheme [3].**

| **User $U_i$/Smartcard** | **Server $S$** |
|---|---|
| **User $U_i$**: | |
| Insert $\langle ID_i, PW_i\rangle$ | |
| **Smartcard**: | |
| Select a random number $r$ | |
| Compute $s_2 = H(H(PW_i\|\|s_1)$, $c_i = c_i + 1$ | |
| Compute $M_1 = (ID_i\|\|N\|\|s_2\|\|r\|\|c_i)^2 \bmod n$ | |
| $\xrightarrow[\text{(via a public channel)}]{M_1}$ | |
| | Extract $\langle ID_i, N, s_2, r, c_i\rangle$ from $M_1$ |
| | Obtain $\langle ID_i, c_i'\rangle$ from database |
| | If $(c_i' \leq c_i)$ |
| | abort the session |
| | Else |
| | update $\langle ID_i, c_i'\rangle$ to $\langle ID_i, c_i\rangle$ |
| | Compute $v = H(K \oplus ID_i)$, $s_2' = N \oplus v$ |
| | If $(s_2' \neq s_2)$ |
| | abort the session |
| | Else |
| | authenticate $U_i$ |
| | Compute the session key $SK = H(s_2\|\|r\|\|1)$ |
| | Compute $M_2 = H(s_2\|\|r\|\|0)$ |
| $\xleftarrow[\text{(via a public channel)}]{M_2}$ | |
| **Smartcard**: | |
| Compute $M_2' = H(s_2\|\|r\|\|0)$ | |
| If $(M_2' M_2)$ | |
| abort the session | |
| Else | |
| authenticate $S$ | |
| Compute the session key $SK = H(s_2\|\|r\|\|1)$ | |

doi:10.1371/journal.pone.0131368.t002

## 4.1 Login Phase is Inefficient and Unfriendly

We claimed that the design of login phase of Wen's authentication scheme is inefficient and unfriendly. In this phase, $U_i$ keys his/her $\langle ID_i, PW_i\rangle$ into the smart card and then the smart card computes the login message $M_1$ without verifying the correctness of the entered login identity $ID_i$ and the password $PW_i$. If $U_i$ incorrectly enters the login identity and the password by mistake, then the smart card computes the incorrect login message $M_1$ and then transfer it to $S$. On receiving $M_1$, $S$ checks it and accordingly informs $U_i$. Therefore, the correctness of $\langle ID_i, PW_i\rangle$ will be checked by $S$ not by the smart card. However, this kind of design puts unnecessary burden on $S$. In the literature, efficient smart card based authentication schemes are proposed [28, 29, 37] where instead of $S$, the smart card is responsible for checking the correctness of $\langle ID_i, PW_i\rangle$ before computing the login message $M_1$. The complete description of the problem we pointed out in Wen's scheme [3] is explained as follows:

**Case 1**: Here we will show how the login and authentication phases will faced problem if $U_i$ mistakenly insert the incorrect login identity $ID_i^*$ instead of the correct identity $ID_i$.

**Step 1**. $U_i$ enters $\langle ID_i^*, PW_i\rangle$ into the smart card and then the smart card selects a random number $r$ and calculates $s_2 = H(H(PW_i||s_1)$, $c_i = c_i + 1$ and $M_1 = (ID_i^* \ || \ N \ || \ s_2 \ || \ r \ || \ c_i)^2$ mod $n$. The smart card then sends $M_1$ to $S$ over a public channel.

**Step 2**. In the authentication phase, $S$ extracts $(ID_i^* \ || \ N \ || \ s_2 \ || \ r \ || \ c_i)$ from $M_1$ based on the Chinese Remainder Theorem (CRT) using the secret primes $p$ and $q$. Now, $S$ observed that $ID_i^*$ is incorrect by comparing it with the tuples $\langle ID_i, c_i'\rangle$ stored in the database and accordingly he/she aborts the session.

**Case 2**: Now we show that the login and authentication phases of Wen's scheme [3] will suffer from the problem as described below if $U_i$ mistakenly insert the incorrect password $PW_i^*$ instead of the correct password $PW_i$.

**Step 1**. $U_i$ enters $\langle ID_i, PW_i^*\rangle$ into the smart card and then the smart card selects a random number $r$ and calculates $s_2^* = H(H(PW_i^* \ || \ s_1)$, $c_i = c_i + 1$ and $M_1 = (ID_i \ || \ N \ || \ s_2^* \ || \ r \ || \ c_i)^2$ mod $n$. The smart card then sends $M_1$ to $S$ over a public network.

**Step 2**. In the authentication phase, $S$ extracts $(ID_i \ || \ N \ || \ s_2^* \ || \ r \ || \ c_i)$ from $M_1$ based on the Chinese Remainder Theorem (CRT) using the secret primes $p$ and $q$. In this case, $S$ found that $ID_i$ and the condition $c_i' > c_i$ are correct and thus performs additional verifications. Then $S$ computes $v = H(K \oplus ID_i)$ and

$$\begin{aligned} s_2' &= N \oplus v \\ &= v \oplus s_2 \oplus v \\ &= s_2 \\ &= H(H(PW_i||s_1)) \\ &\neq s_2^*[\text{Since } H(H(PW_i^*||s_1) \neq H(H(PW_i||s_1)] \end{aligned}$$

Although, $U_i$ is a legal user, however, $S$ rejects him/her since the verification equation $s_2' = s_2^*$ is not satisfied.

From the above discussions, we can assured that an efficient and robust authentication scheme must verifies the login identity and password before proceed to the authentication phase.

## 4.2 Password Change Phase is Inefficient and Unfriendly

The password change phase of Wen's scheme [3] is also inefficient and unfriendly [28, 29, 37]. In this phase, $U_i$ sends his/her $\langle ID_i, PW_i, PW_{new}\rangle$ to $S$ through a secure channel. $S$ computes $v = H(K||ID_i)$, $s_1^* = H(PW_{new}||K)$, $s_2^* = H(H(PW_{new} \ || \ s_1^*))$ and $N^* = v \oplus s_2^*$. $S$ then securely sends $\langle s_1^*, N^*\rangle$ to $U_i$. On receiving $\langle s_1^*, N^*\rangle$ from $S$, $U_i$ updates the smart card's memory as $\langle ID_i, H(\cdot), N^*, s_1^*, c_i\rangle$. However, the following inefficiencies have been observed in Wen's scheme:

**Case 1**: The user $U_i$ must used a secure channel to deliver $\langle ID_i, PW_i, PW_{new}\rangle$ to $S$ and $S$ also used the secure channel to send $\langle s_1^*, N^*\rangle$ to $U_i$. However, each and every password change, Wen's scheme [3] needs two secure communication channels and it is costly and difficult to achieve in real environments. As a result, $U_i$ will not be interested to change his/her password periodically. However, due to the security reasons, it is recommended to change the password periodically.

**Case 2**: For the password change operation of smart card based authentication scheme, it is recommended that the smart card itself change the password without any connection with the remote server $S$ [37].

**Case 3**: During the password change, the correctness of the entered old identity and password $\langle ID_i, PW_i\rangle$ must be verified before changing the old password $PW_i$ to a new password $PW_{new}$.

However, all of the aforesaid conditions are not incorporated in the password change phase of the Wen's authentication scheme [3].

## 4.3 Impersonation Attack

In Wen's scheme, the old password $PW_i$ has no role in the password change operation. Therefore, if the adversary chooses two random passwords $PW_i'$ and $PW_i''$, and issues a password change request on behalf of $U_i$ to $S$ by sending $\langle ID_i, PW_i', PW_i''\rangle$. Upon receiving the password change request, $S$ computes $v = H(K||ID_i)$, $s_1'' = H(PW_i'' \mid\mid K)$, $s_2'' = H(H(PW_i'' \mid\mid s_1''))$ and $N'' = v \oplus s_2''$, and sends $\langle s_1'', N''\rangle$ to the adversary. Upon receiving $\langle s_1'', N''\rangle$, the adversary chooses a sufficiently large value $c_i''$ as the counter and then stores the tuple $\langle ID_i, H(\cdot), N'', s_1'', c_i''\rangle$ into a smart card. It can be noted that, the adversary can successfully impersonate $U_i$ by using this smart card and $\langle ID_i, PW_i''\rangle$.

## 4.4 Privileged-Insider Attack

It is difficult for a user to remember a number of passwords, if he/she registers himself/herself to different applications or servers with different passwords [37, 38]. Therefore, it is common in real-life environments that a user accesses a number of servers with the common password and identity. However, if the password of the user is known by some means to the privileged-insider of a server, then of course he may try to impersonate the user to access other application servers. We can define the insider attacker is any manager of the authentication server, whose intention is to leak the secret information leading to compromise the system. In the registration phase of Wen's authentication scheme [3], $U_i$ transmitted $\langle ID_i, PW_i\rangle$ in plaintext form to $S$, then the malicious privileged-insider of $S$ may impersonate $U_i$ by login to other application servers using the known $\langle ID_i, PW_i\rangle$. Therefore, Wen's authentication scheme is not secure against privileged-insider attack.

## 4.5 Absence of Lost/Stolen Smart Card Revocation Phase

In a smart card based authentication scheme, the revocation of lost/stolen smart card plays a vital role in order to provide the adequate security to the end user [39]. However, Wen's scheme [3] has not offered such an important security features. In the design of two-factor user authentication system, most of the researchers offers a realistic assumption that the smart card is non-temper resistance. It includes that if an adversary obtains a smart card, then he/she can perform some off-line analysis by monitoring the timing information, power consumption and reverse engineering techniques as presented in [40–42] and can obtain the information from the lost smart card. Now the adversary may apply some off-line procedure on the extracted information and may get success to find the correct password of the user. If the adversary found the correct password, then he/she can masquerade the corresponding legal user by using the guessed password and the lost smart card [37–39]. Thus, the cryptographic research community suggested that the lost/stolen smart card revocation phase must be incorporated in two-factor user authentication scheme so that the remote server can distinguish the lost smart card and the new smart card.

## 4.6 Absence of Explicit Session Key Confirmation Property

According to the analysis provided in [43], an authenticated key agreement (AKA) scheme must have the explicit session key confirmation (implicit key authentication and key confirmation) property. The implicit key conformation property includes that the user $X$ is assured that $Y$ can compute the session key. However, the explicit key confirmation property states that the user $X$ is assured that the user $Y$ has actually computed the session key. Therefore, only the explicit key confirmation property provides the stronger assurances that $X$ and $Y$ hold the same session key. A key agreement scheme that includes explicit key authentication is termed as authenticated key agreement with key confirmation (AKC) scheme. In the authentication phase of Wen's scheme [3], $S$ computes $M_2 = H(s_2||r||0)$ and sends it to $U_i$. On receiving $M_2$, $U_i$ computes $M_2' = H(s_2||r||0)$ and authenticates $S$ if the verification $M_2' = M_2$ is correct. After this verification, $U_i$ computes the session key as $SK = H(s_2||r||1)$. As the authentication message $M_2$ does not include the session key information, therefore, the explicit session key confirmation property is not achieved in Wen's authentication scheme.

## 4.7 Absence of No Key Control Property

The no key control property of an AKA scheme means that none of the users have control over others [38, 43, 44]. That is none of the users or even an adversary can force other so that the session key to be a pre-selected value or it may lie within a set consisting of small number of elements. Thus, we can say that an AKA scheme has the no key control property if the session key is computed with the contributions of all the participants. In Wen's scheme [3], we observed that the final session key agreed between $U_i$ and $S$ is $SK = H(s_2||r||1)$, where $U_i$ chooses the random number $r$. Now it is clear that $S$ has no contribution on the session key. Therefore, the *no key control* property is absent in Wen's authentication scheme.

# 5 The Proposed User Authentication Scheme

In the following, an improved user authentication scheme is presented that not only eliminates the inefficiencies of Wen's authentication scheme [3], but also includes additional security and functional properties of a two-factor authentication scheme. Similar to the Wen's scheme, the security of our user authentication scheme is based on the intractable assumption of the quadratic residue problem (QRP) in the multiplicative group $Z_n^*$ [3, 35, 36]. Initially, the remote server $S$ of the integrated EPR information system selects two large prime numbers $p$, $q$. $S$ discloses the public modulus $n$, whereas $p$ and $q$ are kept secret from the outsiders. $S$ also selects $K \in_R Z_n^*$ as his/her secret (private) key. Our enhanced scheme includes the following phases, called *registration phase*, *login phase*, *authentication phase*, *password change phase* and *lost/stolen smart card revocation phase*. The complete explanation of these phases are given below.

## 5.1 Registration Phase

In this phase, a legal user $U_i$ registerers himself/herself to the remote server $S$ and obtains a valid medical smart card from $S$. The following steps are executed by $U_i$ and $S$:

**Step 1**. $U_i$ issues a registration request with his/her identity $ID_i$ to $S$ over a secure channel.

**Step 2**. On receiving $ID_i$, $S$ checks whether $ID_i$ is fresh or not. If it is found in the $S$'s database, then $S$ informs $U_i$ to supply a fresh login identity. Otherwise, $S$ selects a number $b_i \in_R Z_n^*$ and then computes $A_i = H(ID_i||K||b_i)$. After that, $S$ initiates a counter $c_i = 0$ [3] and selects a new smart card that includes the information $\langle H(\cdot), n, A_i, c_i \rangle$. Then $S$ securely delivers the smart card to the user $U_i$. $S$ includes the tuple $\langle ID_i, c_i, b_i \rangle$ into the database [45].

**Step 3**. On receiving the smart card, $U_i$ inserts the smart card into the card reader and keys his/her login identity $ID_i$ and the password $PW_i$ into the smart card. Then the smart card computes $B_i = H(ID_i||PW_i)$, $C_i = A_i \oplus B_i$ and $D_i = H(A_i||B_i)$. Now the smart card deletes the information $\langle A_i, B_i\rangle$ from the memory and then updates it by the tuple $\langle H(\cdot), n, C_i, D_i, c_i\rangle$.

## 5.2 Login Phase

In this phase, $U_i$ computes a login message and sends it to $S$ for verification. The login phase includes the following steps:

**Step 1**. $U_i$ inserts the smart card into the specific card reader and keys his/her $\langle ID_i, PW_i\rangle$ into the smart card. The smart card computes $B_i = H(ID_i||PW_i)$, $A_i = C_i \oplus B_i$ and $D_i' = H(A_i||B_i)$. The smart card aborts the login process if $D_i' \neq D_i$ holds. Otherwise, the smart card executes the following steps.

**Step 2**. The smart card computes $c_i = c_i + 1$ and the login message $M_1 = (ID_i||A_i||a||c_i)^2 \bmod n$, where the number $a \in_R Z_n^*$ is chosen by the smart card. Then the smart card sends $M_1$ to $S$ over a public network.

## 5.3 Authentication Phase

**Step 1**. Upon receiving $M_1$, $S$ then obtains $(ID_i||A_i||a||c_i)$ from $M_1$ using the Chinese Remainder Theorem (CRT) with $p$ and $q$. Now, $S$ retrieves the tuple $\langle ID_i, c_i', b_i\rangle$, which is indexed by $ID_i$, from the database and compares whether $c_i' > c_i$ holds. If it is incorrect, $S$ terminates the session. Otherwise, $S$ updates the tuple $\langle ID_i, c_i', b_i\rangle$ to $\langle ID_i, c_i, b_i\rangle$ and continues to the next step.

**Step 2**. Now, $S$ computes $A_i' = H(ID_i||K||b_i)$ and verifies whether $A_i' = A_i$ holds. If it is incorrect, $S$ terminates the session, otherwise accepts the login message $M_1$ and authenticates $U_i$.

**Step 3**. $S$ selects a number $b \in_R Z_n^*$ and computes $d = a \oplus b$, the session key $SK = H(ID_i||a||b||A_i)$ shared with $U_i$ and $M_2 = H(ID_i||A_i||d||SK)$. Then $S$ delivers the message $\{d, M_2\}$ to $U_i$ over a public network.

**Step 4**. On receiving $\{d, M_2\}$, $U_i$ computes $b = d \oplus a$, the session key $SK = H(ID_i||a||b||A_i)$ and $M_2' = H(ID_i||A_i||d||SK)$. If $M_2' \neq M_2$, $U_i$ terminates the session. Otherwise, $U_i$ authenticates $S$ and accepts $SK$ as the correct session key shared with $S$.

## 5.4 Password Change Phase

In the password change phase, the smart card is allowed to independently (i.e., without any assistance of $S$) change $U_i$'s old password $PW_i$ to the new password $PW_i^n$. We described the password change phase with the following steps:

**Step 1**. $U_i$ inserts the smart card into the specific device and then keys his/her $\langle ID_i, PW_i\rangle$ into the smart card. The smart card then computes $B_i = H(ID_i||PW_i)$, $A_i = C_i \oplus B_i$ and $D_i' = H(A_i||B_i)$. The smart card aborts the password change if $D_i' \neq D_i$ holds. Otherwise, the smart card executes the next step.

**Step 2**. The smart card computes $B_i^n = H(ID_i \ || \ PW_i^n)$, $C_i^n = A_i \oplus B_i^n$ and $D_i^n = H(A_i \ || \ B_i^n)$. Now, the smart card updates the tuple $\langle H(\cdot), n, C_i, D_i, c_i\rangle$ to tuple $\langle H(\cdot), n, C_i^n, D_i^n, c_i\rangle$ into the memory.

## 5.5 Stolen/Lost Smart Card Revocation Phase

This phase is designed to issue a new smart card if $U_i$ lost his/her old smart card. The description of this phase includes the following steps:

**Step 1**. The user $U_i$ sends the smart card revocation request with his/her identity $ID_i$ to $S$ over a secure channel.

**Step 2**. $S$ verifies the correctness of the identity $ID_i$. If it is invalid, $S$ terminates the request. Otherwise, $S$ selects a new number $b'_i \in_R Z_n^*$ and then computes $A'_i = H(ID_i \mid\mid K \mid\mid b'_i)$. $S$ updates the tuple $\langle ID_i, c_i, b_i \rangle$ to $\langle ID_i, c_i, b'_i \rangle$ into his/her database. Now, $S$ writes the information $\langle H(\cdot), n, A'_i, c_i \rangle$ into a new smart card and delivers it to $U_i$ through a secure channel.

**Step 3**. On receiving the new smart card, $U_i$ inserts it into the card reader and inputs his/her login identity $ID_i$ and the new password $PW'_i$ into the smart card. Then the smart card computes $B'_i = H(ID_i \mid\mid PW'_i)$, $C'_i = A'_i \oplus B'_i$ and $D'_i = H(A'_i \mid\mid B'_i)$. Now the smart card deletes the information $\langle A'_i, B'_i \rangle$ form the smart card and then updates the smart card's memory with the tuple $\langle H(\cdot), n, C'_i, D'_i, c_i \rangle$.

The complete description of the Login and Authentication phases of our user authentication scheme is further presented in Table 3.

# 6 Security and Functionality Analysis of the Proposed Scheme

This section is designed to prove the security and functionality strengths of our proposed scheme [46–48]. Now, we described the following assumptions about the attack capability of active and passive adversaries:

- The adversary $\mathcal{A}$ controls the communication channel [49, 50] i.e., he/she may intercept, block, inject, remove, or modify, any messages transmitted over the public media, in other words, all the messages communicated between $U_i$ and $S$ are transmitted via $\mathcal{A}$.
- $\mathcal{A}$ may either (i) theft $U_i$'s smart card and obtain the secret data from it through monitoring the timing information, power consumption and reverse engineering techniques which are proposed in [40–42] and try to obtain $U_i$'s correct password in any off-line manner; or (ii) obtain $U_i$'s password directly by some means. However, $\mathcal{A}$ cannot do both (i) and (ii) [37, 38].

Based on the aforesaid assumptions, the following theorems have been stated and proved against the proposed user authentication scheme.

**Theorem 1**. The proposed user authentication scheme could provide the user anonymity and user unlinkability.

*Proof*. Users' anonymity or secrecy, i.e., the protection of user's identity from the adversary is a great concern in many internet applications including integrated EPR information system, telecare medical information system (TMIS), online order placement, Pay-TV, wireless communications, banking transactions, etc [51–53]. The anonymity means that an adversary $\mathcal{A}$ cannot figure out the real identity $ID_i$ of $U_i$ from the eavesdropped authentication messages $M_1$ and $\{d, M_2\}$. Suppose that $\mathcal{A}$ captures $U_i$'s authentication message $M_1 = (ID_i||A_i||a||c_i)^2 \bmod n$ for a session. However, $\mathcal{A}$ cannot retrieve the identity $ID_i$ from $M_1$ due to the difficulties of quadratic residue problem and from $M_2$ due to the one-way property of the hash function $H(\cdot)$. On the other hand, $\mathcal{A}$ cannot link that the two authentication messages $M_1 = (ID_i||A_i||a||c_i)^2$ mod $n$ and $M'_1 = (ID_i \mid\mid A_i \mid\mid a' \mid\mid c'_i)^2$ mod $n$ belong to the same user $U_i$ and as a result the proposed scheme satisfies user anonymity and unlinkability [38, 45, 54].

Table 3. Login and authentication phases of the proposed user authentication scheme.

| User $U_i$/Smartcard | Server $S$ |
|---|---|
| **User $U_i$**: | |
| Insert $\langle ID_i, PW_i \rangle$ | |
| **Smartcard**: | |
| Compute $B_i = H(ID_i \vert\vert PW_i)$, $A_i = C_i \oplus B_i$ | |
| Compute $D'_i = H(A_i \vert\vert B_i)$ | |
| If $(D'_i \neq D_i)$ | |
| terminate the session | |
| Else | |
| compute $c_i = c_i + 1$ | |
| Choose $a \in_R Z_n^*$ | |
| Compute $M_1 = (ID_i \vert\vert A_i \vert\vert a \vert\vert c_i)^2 \bmod n$ | |
| $\xrightarrow[\text{(via a public channel)}]{M_1}$ | |
| | Obtain $ID_i$, $A_i$, $a$, $c_i$ from $M_1$ |
| | Retrieve $\langle ID_i, c'_i, b_i \rangle$ from database |
| | If $(c'_i \leq c_i)$ |
| | terminate the session |
| | Else |
| | update $\langle ID_i, c'_i, b_i \rangle$ to $\langle ID_i, c_i, b_i \rangle$ |
| | Compute $A'_i = H(ID_i \vert\vert K \vert\vert b_i)$ |
| | If $(A'_i \neq A_i)$ |
| | terminate the session |
| | Else |
| | select $b \in_R Z_n^*$ |
| | Compute $d = a \oplus b$ and |
| | Session key $SK = H(ID_i \vert\vert a \vert\vert b \vert\vert A_i)$ |
| | Compute $M_2 = H(ID_i \vert\vert A_i \vert\vert d \vert\vert SK)$ |
| $\xleftarrow[\text{(via a public channel)}]{\{d, M_2\}}$ | |
| **Smartcard**: | |
| Compute $b = d \oplus a$ and | |
| Session key $SK = H(ID_i \vert\vert a \vert\vert b \vert\vert A_i)$ | |
| Compute $M'_2 = H(ID_i \vert\vert A_i \vert\vert d \vert\vert SK)$ | |
| If $(M'_2 \neq M_2)$ | |
| terminate the session | |
| Else | |
| authenticate $S$ and | |
| Accept $SK$ as session key | |

doi:10.1371/journal.pone.0131368.t003

**Theorem 2**. The proposed user authentication scheme could provide the perfect forward secrecy of the session key.

*Proof*. The perfect forward secrecy [43, 45, 55] ensures that a session key derived in a session will remains undisclosed even if the server's secret key is compromised. In the proposed scheme, the session key is computed as $SK = H(ID_i||a||b||A_i)$, where $A_i = H(ID_i||K||b_i)$ and the random numbers $a$ and $b$ are chosen by $U_i$ and $S$, respectively. Therefore, even if $\mathcal{A}$ has the knowledge of secret key $K$ of $S$, $\mathcal{A}$ needs to be extract $a$ and $b$ from $M_1 = (ID_i||A_i||a||c_i)^2 \bmod n$

and $\{d = a \oplus b, M_2 = H(ID_i||A_i||d||SK)\}$ to derive the session key $SK$, however this is infeasible due to the quadratic residue problem [3, 35]. Thus, our scheme provides the functionality of session key perfect forward secrecy.

**Theorem 3**. The proposed user authentication scheme could resist the replay attack.

*Proof*. In replay attack, the adversary $\mathcal{A}$ captured a valid login message of previous session and then fraudulently replayed to current session to impersonate $U_i$ or $S$. Assume that, in our scheme, $\mathcal{A}$ captured the previous login message $M_1 = (ID_i||A_i||a||c_i)^2 \bmod n$ of $U_i$ and replays it in the current session. However, $S$ quickly detects that $M_1$ is a replay message by comparing the counter $c_i$ in the message $M_1$ with the counter $c_i'$ retrieves from $S$'s database. When $U_i$ sends $M_1 = (ID_i||A_i||a||c_i)^2 \bmod n$ to $S$, then $S$ verifies it and stores the counter $c_i$ to the tuple $\langle ID_i, c_i, b_i\rangle$. Now, if the same $M_1$ is replayed by the adversary in future session then the computed counter $c_i$ is equal to or less than the retrieved counter $c_i$. The counter $c_i$ helps $S$ to detect the replay attack [3]. Thus, the proposed user authentication scheme avoids the replay attack.

**Theorem 4**. The proposed user authentication scheme could resist the modification/forgery attack.

*Proof*. In the login phase, $U_i$ sends $M_1 = (ID_i||A_i||a||c_i)^2 \bmod n$ to $S$ and $S$ responds with the message $\{d = a \oplus b, M_2 = H(ID_i||A_i||d||SK)\}$ to $U_i$ over an open channel. Since $A_i$ is protected in $M_1$ based on the difficulty of solving the QRP and in $M_2$ by the one-way property of the hash function $H(\cdot)$, any modification of $M_1$ and $M_2$ by the adversary $\mathcal{A}$ will be detected by $U_i$ and $S$ through the verification equations $c_i' > c_i$, $A_i' = A_i$ and $M_2' = M_2$. Therefore, our authentication scheme protects this kind of modification/forgery attack.

**Theorem 5**. The proposed user authentication scheme could resist the privileged-insider attack.

*Proof*. To make the convenient access of different application servers, user generally registers himself/herself by the common login identity and passwords. It is harmful for the user that if the password is compromised to the privileged-insider of a server, then he/she can easily impersonate the user and can login to other applications. In the registration phase of our scheme, $U_i$ only sends his/her login identity $ID_i$ not any password to $S$. Upon receiving the smart card from $S$, $U_i$ inserts his/her $PW_i$ into the smart card. As a result, $PW_i$ is not exposed to the privileged-insider of $S$. Therefore, our scheme withstands the privileged-insider attack.

**Theorem 6**. The proposed user authentication scheme could provide the off-line password guessing attack from lost/stolen smart card.

*Proof*. The off-line password guessing attack is infeasible in our scheme. Assume that $\mathcal{A}$ obtains $U_i$'s smart card and extracts the parameters $\langle H(\cdot), n, C_i, D_i, c_i\rangle$, where $C_i = H(ID_i||K||b_i) \oplus H(ID_i||PW_i)$ and $D_i = H(H(ID_i||K||b_i)||H(ID_i||PW_i))$. Now $\mathcal{A}$ may try to guess the correct password $PW_i$ of $U_i$ in off-line processes. However, without knowing $K$ and $b_i$, $\mathcal{A}$ cannot find $PW_i$. Thus, our user authentication scheme strongly resists the off-line password guessing attack from lost/stolen smart card.

**Theorem 7**. The proposed user authentication scheme could resist the ephemeral secret leakage attack.

*Proof*. This attacks states that the none of the session keys should be compromised with the disclosures of session random numbers (ephemeral secrets) [56]. The ephemeral secrets may be compromised [37, 45] and it is quite common in real environments due to the following reasons: (i) user and server depended on the internal/external source of random number generator which may be controlled by $\mathcal{A}$ and (ii) the random numbers are generally stored in insecure device. If the random numbers aren't erased properly in each session, $\mathcal{A}$ may hijack users' computer and learn the random numbers. In our scheme, $U_i$ and $S$ generate the session key as $SK = H(ID_i||a||b||A_i)$, where $A_i = H(ID_i||K||b_i)$. Suppose that $\langle a, b\rangle$ is disclosed and $\mathcal{A}$ knows it.

However, $\mathcal{A}$ cannot compute $SK$ without $A_i$. Therefore, the ephemeral secret leakage attack is infeasible in the proposed scheme.

**Theorem 8**. The proposed user authentication scheme could resist the known-key attack.

*Proof*. This attack states that, none of the session keys are compromised even if the adversary $\mathcal{A}$ knows some other session keys [43]. In our scheme, $U_i$ and $S$ establish a session key $SK = H(ID_i||a||b||A_i)$, where $A_i = H(ID_i||K||b_i)$. The numbers $a$ and $b$ are randomly chosen from $Z_n^*$ and hence $SK$ is also random and independent in each session. Therefore, with the knowledge of previous session keys $\mathcal{A}$ cannot compute a new session key. Accordingly, the known-key attack is impossible in our user authentication scheme.

**Theorem 9**. The proposed user authentication scheme could resist the unknown key-share attack and provide the explicit key confirmation property of the agreed session key.

*Proof*. The unknown key-share attack [43] is a situation that $U_i$ finishes the session by believing that he/she shares the session key $SK$ correctly with $S$, however, $S$ mistakenly believes that $SK$ is instead shared with the adversary $\mathcal{A}$. In the proposed scheme, $S$ computes the session key $SK$ after validating the messages $M_1$. To validate the message $\{d, M_2\}$ and to get the confirmation about the agreed session key $SK$, $U_i$ computes $SK = H(ID_i||a||b||A_i)$, $M_2' = H(ID_i||A_i||d||SK)$ and authenticates $S$ and accepts $SK$ as the correct session key if the condition $M_2' = M_2$ hold. Therefore, $U_i$ and $S$ mutually authenticate each other and then compute the session key $SK$, accordingly our scheme enjoys the unknown key-share attack resilience and explicit key confirmation of the session key.

**Theorem 10**. The proposed user authentication scheme could provide efficient and user friendly password change option.

*Proof*. Our scheme gives the flexibility to the user to choose low-entropy password by himself/herself and change the password periodically without remote server's assistance [28, 29]. Moreover, the proposed scheme detects the wrong password and identity during the login phase and password change phase. In these processes, if $U_i$ keys either wrong password $PW_i^*$ or identity $ID_i^*$ by mistake, the smart card reports the error message to $U_i$ without any consultation with $S$ [37]. On the other hand, if $\mathcal{A}$ thefts $U_i$'s smart card, however, he/she does not have the capability to update smart card's memory without correct password $PW_i$, and consequently the denial of service (DoS) attack is eliminated in our scheme. If $\mathcal{A}$ tries to do the same with wrong password, the smart card will be locked immediately if the number of login failure exceeds the pre-defined limit.

**Theorem 11**. The proposed user authentication scheme could provide mutual authentication and session key agreement between the user and the remote server.

*Proof*. In our scheme, $S$ authenticates $U_i$'s login message $M_1 = (ID_i||A_i||a||c_i)^2 \bmod n$ by verifying the conditions $c_i' > c_i$ and $A_i' = ?A_i$. Similarly, $U_i$ verifies $S$'s response message $\langle d, M_2\rangle$ by validating whether $M_2' = M_2$ holds. Without $\langle PW_i, K\rangle$, $\mathcal{A}$ cannot impersonate none of $U_i$ and $S$. Hence, the secure mutual authentication between $U_i$ and $S$ is achieved in our scheme. Moreover, after mutual authentication, $U_i$ and $S$ compute a random and unique session key $SK = H(ID_i||a||b||A_i)$, where $A_i = H(ID_i||K||b_i)$.

## 7 Performance Analysis of the Proposed Scheme

In the following, we have performed the comparison analysis of our authentication scheme with the schemes proposed in [3, 34, 57–59]. Here, the following notations are described for this purpose:

- $t_h$ : Time needed to execute a hash function.
- $t_m$ : Time needed to execute a modular squaring computation.

**Table 4. Computation cost comparison of the proposed user authentication scheme with others.**

| Attributes | Wen [3] | Zhu [34] | Wu et al. [57] | Cheng et al. [58] | Lee [59] | Proposed |
|---|---|---|---|---|---|---|
| $A_1$ | $2t_h + t_m$ | $2t_h + t_m$ | $2t_h + t_m$ | $t_h$ | $2t_h$ | $2t_h$ |
| $A_2$ | $9t_h + t_q$ | $5t_h + t_q$ | $6t_h + t_m + 2t_q$ | $12t_h + t_m + t_q$ | $8t_h + t_m + 2t_q$ | $5t_h + t_m + t_q$ |
| $A_3$ | $4t_h$ | $4t_h + t_m$ | NA | NA | NA | $4t_h$ |
| $A_4$ | NA | NA | NA | NA | NA | $3t_h$ |
| $A_5$ | 2 | 3 | 2 | 2 | 2 | 2 |

$A_1$: Computation cost in registration phase, $A_2$: Computation cost in login phase and authentication phase, $A_3$: Computation cost in password change phase, $A_4$: Computation cost in smartcard revocation phase, $A_5$: Number of message communications, **NA**: Not applicable (this pase is not proposed by the author (s)).

doi:10.1371/journal.pone.0131368.t004

- $t_q$ : Time needed to execute a square root operation with the modulus $n$.

The comparative result of the proposed scheme and the schemes in [3, 34, 57–59] from the aspects of computation cost and communication round is listed in the Table 4. Our scheme proposed all the required phases where the schemes in [3, 34, 57–59] do not have password change phase and smartcard revocation phase. Furthermore, we observed that our scheme is more robust and computation and communication cost efficient than the schemes devised in [3, 34, 57–59].

We also given a comparison in Fig 1 against the number of operations used in the registration and login phased of the schemes in [3, 34, 57–59] with the proposed scheme.

In 2011, based on QRP, Wu et al [57] proposed a user authentication scheme using smartcard. However, the scheme is vulnerable to (1) privileged-insider attack since the plaintext password is sending to the server for registration, (2) the scheme does not verify the keyed password and identity in the login phase, (3) the scheme does not have password change phase, (4) it has no provision to revoke the lost/stolen smart card, (5) no session key agreement method is proposed and (6) user anonymity and unlinkability are violated as the identity is transmitted in plaintext form. In the year 2012, in order to ensure users' privacy, Zhu [34] proposed a user authentication schemes for telecare medicine information systems. We carefully observed that the Zhu's scheme [34] is not free from attack since (1) the scheme does not verify the correctness of the login identity and password in the login phase, (2) the scheme does not verify the correctness of the login identity and password in the password change phase, (3) the scheme has no provision to revoke the smartcard in case if the smartcard is stolen or lost, (4) the scheme does not design a session key agreement method during login and authentication phases, (5) user anonymity and user untracibility are not present in this scheme. In 2013, Cheng et al. [58] proposed a a biometric-based remote user mutual authentication and session key agreement scheme using QRP. However, Yoon [60] showed that the scheme is insecure from the stolen smart card attack, server spoofing attack and does not provide session key forward secrecy. We also observed that the scheme does not have provision for password change and lost/stolen smart card revocation. In addition, the scheme does not verify the correctness of keyed identity and password in the login phase. Further, the scheme is also suffered from the ephemeral secrets leakage attack as the session key solely depended on the random numbers chosen by the user and server. In 2015, Lee [59] proposed an efficient smartcard-based two-factor remote user mutual authentication scheme. However, we observed that the scheme is not secure since (1) the scheme does not proposed any password change method, (2) the scheme

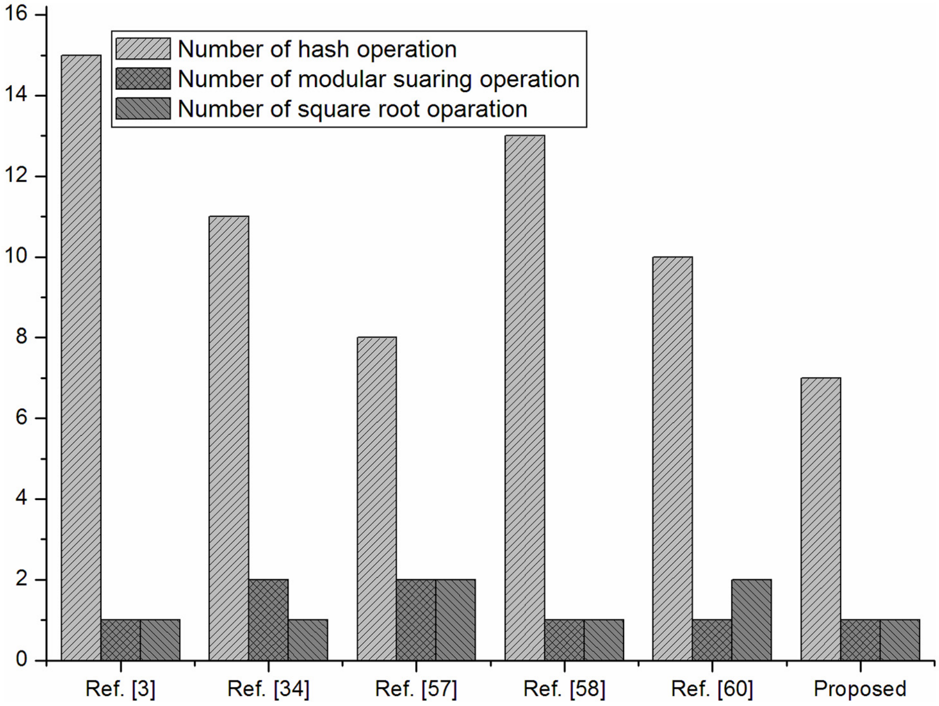

**Fig 1. Number of hash, modular squaring and square root operations for registration and login phases.**

doi:10.1371/journal.pone.0131368.g001

does not proposed any lost/stolen smart card revocation method, (3) The scheme has no provision for session key agreement during login and authentication phases, (4) the scheme does not verify the keyed password and identity in the login phase, (5) the privileged-insider attack since the plaintext password is sending to the server for registration.

In the comparative analysis of the proposed scheme and the schemes [3, 34, 57–59] with respect to security and functionality are included in the Table 5. Form Tables 4 and 5, it can be see that the proposed user authentication scheme includes more security and functional features compared to [3, 34, 57–59].

## 8 Conclusions

The privacy and confidentiality of patient information and the untraceability and anonymity of patient have considered important factors from the security research communities for any user authentication system used in different healthcare applications. In keeping with these requirements, Wen proposed an enhanced user authentication scheme against Lee et al.'s authentication scheme for the EPR information system. However, this paper analyzed Wen's scheme and demonstrated that it has many security and design problems and thus, it may not be considered appropriate for the secure and efficient healthcare applications. We have then taken into consideration the intractability assumption of the quadratic residue problem in the multiplicative group and proposed another two-factor user authentication scheme with more security and functionality aspects than existing schemes.

**Table 5. Security and functionality comparison of the proposed scheme with other existing schemes.**

| Attributes | Wen [3] | Zhu [34] | Wu et al. [57] | Cheng et al. [58] | Lee [59] | Proposed |
|---|---|---|---|---|---|---|
| $F_1$ | No | No | No | No | No | Yes |
| $F_2$ | No | No | NA | NA | NA | Yes |
| $F_3$ | No | Yes | Yes | No | Yes | Yes |
| $F_4$ | No | Yes | No | Yes | No | Yes |
| $F_5$ | No | No | No | No | No | Yes |
| $F_6$ | No | NA | NA | No | NA | Yes |
| $F_7$ | No | NA | NA | Yes | NA | Yes |
| $F_8$ | No | Yes | NA | No | No | Yes |
| $F_9$ | Yes | NA | NA | No | No | Yes |
| $F_{10}$ | Yes | No | No | Yes | Yes | Yes |
| $F_{11}$ | Yes | Yes | Yes | Yes | Yes | Yes |
| $F_{12}$ | Yes | Yes | Yes | Yes | Yes | Yes |
| $F_{13}$ | Yes | Yes | NA | No | Yes | Yes |
| $F_{14}$ | Yes | Yes | Yes | Yes | Yes | Yes |

$F_1$: Login identity and password detection in the login phase; $F_2$: Login identity and password detection in the password change phase; $F_3$: Impersonation attack is avoided; $F_4$: Privileged-insider attack is avoided; $F_5$: Lost/stolen smart card revocation phase is present; $F_6$: Explicit session key confirmation property is present; $F_7$: No key control property is present; $F_8$: Password is changed without any help from the server; $F_9$: Ephemeral secrets leakage attack is avoided; $F_{10}$: User anonymity and unlinkability are present; $F_{11}$: Password guessing attack from lost smart card is avoided; $F_{12}$: Replay attack is avoided; $F_{13}$: Forward secrecy of the session key is present; $F_{14}$: modification/forgery attack is avoided.

doi:10.1371/journal.pone.0131368.t005

## Acknowledgments

The authors would like to acknowledge the many helpful suggestions of the anonymous reviewers and the editor, which have improved the content and the presentation of this paper.

## Author Contributions

Conceived and designed the experiments: SKHI MKK XL. Performed the experiments: SKHI MKK XL. Analyzed the data: SKHI MKK XL. Contributed reagents/materials/analysis tools: SKHI MKK XL. Wrote the paper: SKHI MKK XL. Designed the scheme: SKHI MKK XL. Proved the security of the scheme: SKHI MKK XL.

## References

1. Wu Z-Y, Chung Y, Lai F, Chen T-S (2012) A Password-based user authentication scheme for the integrated EPR information system. Journal of Medical Systems 36(2): 631–638. doi: 10.1007/s10916-010-9527-7 PMID: 20703670
2. Lee TF, Chang IP, Lin TH, Wang CC (2013) A secure and efficient password-based user authentication scheme using smart cards for the integrated EPR information system. Journal of Medical Systems 37 (3): 9941. doi: 10.1007/s10916-013-9933-8 PMID: 23553734
3. Wen FT (2014) A more secure anonymous user authentication scheme for the integrated EPR information system. Journal of Medical Systems. doi: 10.1007/s10916-014-0042-0
4. Islam SH, Khan MK (2014) Cryptanalysis and Improvement of Authentication and Key Agreement Protocols for Telecare Medicine Information Systems. Journal of Medical Systems 38(10): 1–16. doi: 10.1007/s10916-014-0135-9

5. Islam SH, Biswas GP (2015) Cryptanalysis and improvement of a password-based user authentication scheme for the integrated EPR information system. Journal of King Saud University—Computer and Information Sciences. doi: 10.1016/j.jksuci.2014.03.018

6. Li X, Xiong YP, Ma J, Wang WD (2012) An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards. Journal of Network and Computer Applications 35(2): 763–769. doi: 10.1016/j.jnca.2011.11.009

7. Li X, Niu JW, Khan MK, Liao JG (2013) An enhanced smart card based remote user password authentication scheme. Journal of Network and Computer Applications 36(5): 1365–1371. doi: 10.1016/j.jnca.2013.02.034

8. Li X, Ma J, Wang WD, Xiong YP, Zhang JS (2013) A novel smart card and dynamic ID based remote user authentication scheme for multi-server environments. Mathematical and Computer Modelling 58 (1): 85–95. doi: 10.1016/j.mcm.2012.06.033

9. Ding S, Yang S, Zhang Y, Liang C, Xia C (2014) Combining QoS prediction and customer satisfaction estimation to solve cloud service trustworthiness evaluation problems. Knowledge-Based Systems 56: 216–225. doi: 10.1016/j.knosys.2013.11.014

10. Ding S, Wang J, Ruan S, Xia C (2015) Inferring to individual diversity promotes the cooperation in the spatial prisoner's dilemma game. Chaos, Solitons & Fractals 71: 91–99. doi: 10.1016/j.chaos.2014.12.014

11. Ding S, Xia C-Y, Zhou K-L, Yang S-L, Shang JS (2014) Decision Support for Personalized Cloud Service Selection through Multi-Attribute Trustworthiness Evaluation. PLoS ONE 9(6): e97762. doi: 10.1371/journal.pone.0097762 PMID: 24972237

12. He D, Chen J, Zhang R (2012) A more secure authentication scheme for telecare medicine information systems. Journal of Medical Systems 36(3): 1989–1995. doi: 10.1007/s10916-011-9658-5

13. Wei J, Hu X, Liu W (2012) An improved authentication scheme for telecare medicine information systems. Journal of Medical Systems 36(6): 3597–3604. doi: 10.1007/s10916-012-9835-1 PMID: 22374237

14. Li SH, Wang CY, Lu WH, Lin YY, Yen DC (2012) Design and implementation of a telecare information platform. Journal of Medical Systems 36(3): 1629–1650. doi: 10.1007/s10916-010-9625-6 PMID: 21120592

15. Chen H. M., Lo J. W., Yeh C. K., An efficient and secure dynamic ID-based authentication scheme for telecare medical information systems. Journal of Medical Systems (2012) 36(6): 3907–3915. doi: 10.1007/s10916-012-9862-y PMID: 22673892

16. Wu Z-Y, Lee Y-C, Lai F, Lee H-C, Chung Y (2010) A secure authentication scheme for telecare medicine information systems. Journal of Medical Systems 36(3): 1529–1535. doi: 10.1007/s10916-010-9614-9 PMID: 20978928

17. Pu Q, Wang J, Zhao R (2012) Strong authentication scheme for telecare medicine information systems. Journal of Medical Systems 36(4): 2609–2619. doi: 10.1007/s10916-011-9735-9 PMID: 21594637

18. Kraus V, Dehmer M, Schutte M (2013) On Sphere-Regular Graphs and the Extremality of Information-Theoretic Network Measures. Communications in Mathematical and in Computer Chemistry 70: 885–900.

19. Cao S, Dehmer M, Shi Y (2014) Extremality of degree-based graph entropies. Information Sciences 278: 22–33. doi: 10.1016/j.ins.2014.03.133

20. Dehmer M, Grabner M (2013) The Discrimination Power of Molecular Identification Numbers Revisited. Communications in Mathematical and in Computer Chemistry 69: 785–794.

21. Li X, Li Y, Shi Y, Gutman I (2013) Note on the HOMO.LUMO Index of Graphs. Communications in Mathematical and in Computer Chemistry 70: 85–96.

22. Islam SH, Biswas GP (2014) Dynamic ID-based remote user authentication scheme with smartcard using elliptic curve cryptography. Journal of Electronics 31(5): 473–488.

23. Islam SH (2014) Provably secure dynamic identity-based three-factor password authentication scheme using extended chaotic maps. Nonlinear Dynamics 78(3): 2261–2276. doi: 10.1007/s11071-014-1584-x

24. Islam SH (2014) A provably secure ID-based mutual authentication and key agreement scheme for mobile multi-server environment without ESL attack. Wireless Personal Communications 79: 1975–1991. doi: 10.1007/s11277-014-1968-8

25. Jiang Q, Ma J, Ma Z, Li G (2013) A privacy enhanced authentication scheme for telecare medical information systems. Journal of Medical Systems 37: 9897. doi: 10.1007/s10916-012-9897-0 PMID: 23321959

26. Kumari S, Khan MK, Kumar R (2013) Cryptanalysis and improvement of 'a privacy enhanced scheme for telecare medical information systems'. Journal of Medical Systems 37: 9952–9962. doi: 10.1007/s10916-013-9952-5 PMID: 23689993

27. Xu X, Zhu P, Wen Q, Jin Z, Zhang H, He L (2014) A secure and efficient authentication and key agreement scheme based on ECC for telecare medicine information systems. Journal of Medical Systems 38: 9994. doi: 10.1007/s10916-013-9994-8 PMID: 24346928

28. Das AK, Goswami A (2013) A secure and efficient uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care. Journal of Medical Systems 37(3): 1–16. doi: 10.1007/s10916-013-9948-1

29. Das AK, Bruhadeshwar B (2013) An improved and effective secure password-based authentication and key agreement scheme using smart cards for the telecare medicine information system. Journal of Medical Systems 37(5): 1–17. doi: 10.1007/s10916-013-9969-9

30. Lee TF (2013) An efficient chaotic maps-based authentication and key agreement scheme using smart cards for telecare medicine information systems. Journal of Medical Systems 37(6): 9985. doi: 10.1007/s10916-013-9985-9 PMID: 24141492

31. Wen FT (2013) A robust uniqueness and anonymity preserving remote user authentication scheme for connected health care. Journal of Medical System 37(6): 9980. doi: 10.1007/s10916-013-9980-1

32. Wu ZY, Lee YC, Lai F, Lee HC, Chung Y (2012) A secure authentication scheme for telecare medicine information systems. Journal of Medical System 36(3): 1529–1535. doi: 10.1007/s10916-010-9614-9

33. Yau WC, Raphael C, Phan W (2013) Security analysis of a chaotic map-based authentication scheme for telecare medicine information systems. Journal of Medical System 37(6): 9993. doi: 10.1007/s10916-013-9993-9

34. Zhu Z (2012) An efficient authentication scheme for telecare medicine information systems. Journal of Medical System 36(6): 3833–3838. doi: 10.1007/s10916-012-9856-9

35. Chen Y, Chou J, Sun H (2008) A novel mutual-authentication scheme based on quadratic residues for RFID systems. Computer Networks 52(12): 2373–2380. doi: 10.1016/j.comnet.2008.04.016

36. Rosen K (2008) Elementary number theory and its applications. Reading. MA: Addison-Wesley.

37. Islam SH (2014) Design and analysis of an improved smart card based remote user password authentication scheme. International Journal of Communication Systems. doi: 10.1002/dac.2793

38. Islam SH, Biswas GP, Choo K-KR (2014) Cryptanalysis of an improved smart card-based remote password authentication scheme. Information Sciences Letters 3(1): 35–40. doi: 10.12785/isl/030105

39. Fan C-I, Chan Y-C, Zhang Z-K (2005) Robust remote authentication scheme with smart cards. Computers and Security 24: 619–628. doi: 10.1016/j.cose.2005.03.006

40. Messerges TS, Dabbish EA, Sloan RH (2012) Examining smart card security under the threat of power analysis attacks. IEEE Transactions on Computers 51(5): 541–552. doi: 10.1109/TC.2002.1004593

41. Joye M, Olivier F (2005) Side-channel analysis, Encyclopedia of Cryptography and Security. Kluwer Academic Publishers, pp. 571–576.

42. Kocher P, Jaffe J, Jun B (1999) Differential power analysis. In: Proceedings of Advances in Cryptology (Crypto'99), LNCS, pp. 388–397.

43. Blake-Wilson S, Johnson D, Menezes A (1997) Key agreement protocols and their security analysis. In: Proceedings of Sixth IMA International Conference on Cryptography and Coding, Cirencester, pp. 30–45.

44. Islam SH, Biswas GP (2012) A pairing-free identity-based authenticated group key agreement protocol for imbalanced mobile networks. Annals of telecommunication 67: 547–558. doi: 10.1007/s12243-012-0296-9

45. Islam SH, Biswas GP (2011) A more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem. Journal of Systems and Software 84 (11): 1892–1898. doi: 10.1016/j.jss.2011.06.061

46. He D, Kumar N, Chilamkurti N (2015) A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks. Information Sciences. doi: 10.1016/j.ins.2015.02.010

47. He D, Zeadally S (2015) Authentication protocol for ambient assisted living system. IEEE Communications Magazine 35(1):71–77. doi: 10.1109/MCOM.2015.7010518

48. He D, Kumar N, Chen J, Lee C-C, Chilamkurti N, Yeo S-S (2015) Robust anonymous authentication protocol for healthcare applications using wireless medical sensor networks. Multimedia Systems 21 (1):49–60. doi: 10.1007/s00530-013-0346-9

49. Dolev D, Yao A (1983) On the security of public key protocols. IEEE Transactions on Information Theory 29(2): 198–208. doi: 10.1109/TIT.1983.1056650

50. Li X, Niu J, Ma J, Wang W, Liu C (2011) Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards. Journal of Network and Computer Applications 34(1): 73–79. doi: 10.1016/j.jnca.2010.09.003

51. Wu S, Zhu Y, Pu Q (2012) Robust smart-cards-based user authentication scheme with user anonymity. Security and Communication Networks (2012) 5(2): 236–248. doi: 10.1002/sec.315

52. Li X, Qiu W, Zheng D, Chen K, Li J (2010) Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards. IEEE Transaction on Industrial Electronics 57(2): 793–800. doi: 10.1109/TIE.2009.2028351

53. Khan MK, Kim S-K, Alghathbar K (2011) Cryptanalysis and security enhancement of a 'more efficient & secure dynamic ID-based remote user authentication scheme. Computer Communications 34(3): 305–309. doi: 10.1016/j.comcom.2010.02.011

54. Islam SH, Biswas GP (2012) An improved ID-based client authentication with key agreement scheme on ECC for mobile client-server environments. Theoretical and Applied Informatics 24(4): 293–312. doi: 10.2478/v10179-012-0018-z

55. Islam SH, Biswas GP (2013) Design of improved password authentication and update scheme based on elliptic curve cryptography. Mathematical and Computer Modelling 57 (11-12): 2703–2717. doi: 10.1016/j.mcm.2011.07.001

56. Islam SH, Biswas GP (2011) Improved remote login scheme based on ECE. In: Proceedings of the International Conference on Recent Trends in Information Technology, pp. 1221–1226.

57. Wu T-S, Lin H-Y, Lee M-L, Chen W-Y (2011) Fast Remote User Authentication Scheme with Smart Card Based on Quadratic Residue. Journal of Digital Information Management 9(2): 51–54.

58. Cheng ZY, Liu Y, Chang CC, Liu CX (2013) A novel biometricbased remote user authentication scheme using quadratic residues. International Journal of Information and Electronics Engineering 3(4):419–422.

59. Lee T-F (2015) An Efficient Dynamic ID-based User Authentication Scheme using Smart Cards without Verifier Tables. Applied Mathematics & Information Sciences 9(1): 485–490. doi: 10.12785/amis/090156

60. Yoon E-J (2014) Security Flaws of Cheng et al.'s Biometric-based Remote User Authentication Scheme Using Quadratic Residues. Contemporary Engineering Sciences 7(26): 1467–1473.