RESEARCH ARTICLE

A robust ECC based mutual authentication protocol with anonymity for session initiation protocol

Zahid Mehmood1*, Gongliang Chen1*, Jianhua Li1*, Linsen Li1*, Bander Alzahrani2*

1 School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China, 2 Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia

* These authors contributed equally to this work.
* zaidi@sjtu.edu.cn

Abstract

Over the past few years, Session Initiation Protocol (SIP) is found as a substantial application-layer protocol for the multimedia services. It is extensively used for managing, altering, terminating and distributing the multimedia sessions. Authentication plays a pivotal role in SIP environment. Currently, Lu et al. presented an authentication protocol for SIP and profess that newly proposed protocol is protected against all the familiar attacks. However, the detailed analysis describes that the Lu et al.’s protocol is exposed against server masquerading attack and user’s masquerading attack. Moreover, it also fails to protect the user’s identity as well as it possesses incorrect login and authentication phase. In order to establish a suitable and efficient protocol, having ability to overcome all these discrepancies, a robust ECC-based novel mutual authentication mechanism with anonymity for SIP is presented in this manuscript. The improved protocol contains an explicit parameter for user to cope the issues of security and correctness and is found to be more secure and relatively effective to protect the user’s privacy, user’s masquerading and server masquerading as it is verified through the comprehensive formal and informal security analysis.

1 Introduction

The applications of multimedia services have great significance in advanced networks. The SIP is a valued application-layer protocol used in controlling and signaling the multimedia sessions. The prime responsibility of SIP is the internet telephone services such as voice call, video call and instant messaging over the public network. Furthermore, SIP is responsible to establish, modify and terminate the multimedia sessions [1]. Authentication process is performed by the users in order to login the server through SIP. So, the authentication plays a vital role for the SIP protocol services. Nowadays, due to keen interest of the researchers for security maintenance and authentication of SIP, there is an immense scope for research in authentication of multimedia services. Recently, numerous scholars have presented some secure and efficient authentication techniques to sustain the security of SIP [2–6]. Many
researchers have consensus that Hypertext Transport Protocol (HTTP) digest authentication for SIP is found vulnerable for stolen verifier, server spoofing and off-line password guessing attacks and unable to provide mutual authentication [1, 7–9]. In order to counter these weaknesses, Yang et al. [7] introduced an authentication protocol based on Diffie-Hellman key exchange protocol. Afterwords, Huang et al. [10] pointed out that Yang et al.’s protocol fails to resist off-line password guessing attack and proposed an updated scheme to fix the identified issues appeared in Yang et al.’s scheme. However, Huang’s protocol is found unprotected against off-linen password guessing attack indicated by Jo et al. [11]. In order to enhance Yang et al.’s proposed technique, Durlanik and Sogukpinar [12] presented a secure as well as effective authentication technique based on Elliptic Curve Cryptography (ECC) [13]. ECC can provide same security with relatively smaller key size than the other cryptosystems [13–18]. In 2009, Wu et al. [19] presented an improved and secure authentication protocol for SIP based on ECC. Later on, Yoon et al. [20] demonstrated that Durlanik and Sogukpinar as well as Wu et al.’s proposed protocols are not secure against Denning-Sacco [21], off-line password guessing and stolen verifier attacks. Then Yoon et al.’s introduced a sophisticated technique for SIP with higher security. Pu et al. [22] identified that Yoon et al.’s technique is vulnerable against replay and off-line password guessing attacks. Then a comparatively lightweight authentication and a key agreement protocol by using hash function and exclusive-OR operation is presented by Tsai [23]. Later on, Arshad and Ikram [24] proved that Tsai’s protocol is breakable against the off-line password guessing and stolen-verifier attacks. Moreover, Tsai’s protocol remained unable to maintain forward secrecy and known-key secrecy. Though Yoon et al. [25] presented a robust authentication technique with a key agreement to address the limitations of Tsai’s scheme, yet Yoon et al.’s scheme is found unprotected against off-line password guessing and stolen verifier attacks indicated by Xie [26] and introduced a new scheme. Unfortunately, Xie’s protocol is exposed against off-line password guessing and impersonation attacks indicated by Farash and Attari [27]. Moreover, they proposed a new technique to counter the limitations of Xie’s scheme. Zhang et al. [28] offered an authentication protocol by using ECC with anonymity. Recently, Lu et al. [29] indicated that Zhang et al.’s scheme was breakable in case of insider attack and failed to offer mutual authentication. To remedy these vulnerabilities, Lu et al.’s [29] suggested an advance scheme, which is claimed to be more appropriate against all possible attacks. However, it is analyzed that Lu et al.’s proposed protocol is found insecure in case of server and user masquerading attacks. Additionally, it also fails to offer user anonymity accompanied with incorrect scheme. Hence, a new robust mutual authentication protocol with anonymity using ECC for SIP is presented in this manuscript. The improved scheme contains a slight modification in both registration and authentication phases. We have

| Notations | Description |
|-----------|-------------|
| S, U | Server and User |
| ID, PW | User Identity and Password |
| r1, r2 | Two Random Numbers |
| Pu, Ps | User and Server Private Key |
| h(.) | One-way hash functions |
| || Concatenation operation |
| ⊕ | XOR operation |
| E_p(a, b) | Elliptic Curve over F_p |
| P | Value of Elliptic Curve Point |
| A | The Adversary |

https://doi.org/10.1371/journal.pone.0186044.t001
supplemented an explicit parameter for user to cope the issues of correctness and security. Furthermore, the protocol is highly secured against all the possible attacks as validated through informal and formal security analysis. Comprehensive analysis also verifies that security and performance of the proposed protocol is more effective and reliable as compared to the recent authentication protocols.

The remainder of the manuscript is arranged as follows: Table 1 describes the notations used in this manuscript. Review and weaknesses of Lu et al.’s scheme is demonstrated in sections 2 and 3, respectively. The proposed protocol is presented in section 4, formal and informal security are figured out in section 5. Performance comparison of the present protocol with recently presented protocols is investigated in sections 6. Concluding statement of the proposed protocol is elaborated in section 7.

2 Review of Lu et al.’s scheme

This segment concisely demonstrates the detail analysis of Lu et al.’s protocol. The overall protocol contains three stages. At the first stage, the user performs the registration process, then use it to login into the server and authenticate itself. It also permits the user to update his/her password in inadmissible condition. All these phases are explained in detail and Fig 1 shows the registration and authentication Phases as follows:

---

**Fig 1. Lu et al.’s scheme.**

https://doi.org/10.1371/journal.pone.0186044.g001
2.1 Registration phase

1. \( U_i \) chooses his/her ID, PW, and his/her secret key \( P_{ui} \). \( U_i \) now computes \( PWD = h(PW_i || P_{ui}) \) and transmits \( \{ID_i, PWD\} \) to \( S \) by private channel.

2. \( S \) determines \( V PW = h(ID_i || PWD) \oplus h(P_s) \) upon receiving the message and stores it in server’s repository.

2.2 Authentication phase

1. A random number \( r_1 \) is generated and computed by \( U_i \):

\[
T = h(ID_i || h(PW_i || P_{ui}))
\]

\[
X = r_1 \cdot P
\]

\[
Y = T \oplus X
\]

\[
HID_i = ID_i \oplus T
\]

\[
Z = h(ID_i || X)
\]

Now the \( U_i \) transmits the \( \text{REQUEST} \{Y, HID_i, Z\} \) to \( S \).

2. \( S \) computes, upon reception of request message from \( U_i \):

\[
T' = V PW \oplus h(P_s)
\]

\[
X' = Y \oplus T'
\]

\[
ID'_i = HID_i \oplus T'
\]

\[
Z' = h(ID'_i || X')
\]

verify \( Z' \overset{?}{=} Z \), in case of failure, the session is aborted otherwise, a random number \( r_2 \) is generated by \( S \) and calculates:

\[
D = r_2 \cdot P
\]

\[
sk_s = r_2 \cdot X'
\]

\[
Auth_s = h(sk_s || T'|| X')
\]

Now \( S \) sends the challenge message \( \text{CHALLENGE} \{\text{realm}, D, Auth_s\} \) to user \( U_i \).

3. \( U_i \) on getting the challenge message from \( S \) calculates:

\[
sk_{ui} = r_1 \cdot D
\]

checks \( Auth_s = h(sk_{ui} || T || X) \) is equal to received \( Auth_s \), if the equation is not satisfied, \( U_i \) aborts the session, otherwise \( U_i \) computes \( Auth_{ui} = h(sk_{ui} || T || D) \) and transmits the \( \text{RESPONSE} \{\text{realm}, Auth_{ui}\} \) message to \( S \).
4. Upon getting the message, $S$ verifies $\text{Auth}_{ui} = h(sk_e \| ID) \overset{?}{=} \text{Auth}_{ui}$, if it true, the already computed session key $sk = sk_{ui} = sk_i$ is treated as legitimate key.

2.3 Password change phase

$U_i$ selects new $PW_{\text{new}}^i$, $P_{\text{new}}^i$ and $r_{\text{new}}^i$ in order to change the password.

The following strides are performed by the $U_i$ and $S$.

1. $U_i$ computes:
   \[
   W = h(ID_i \| h(ID_i \| h(PW_i \| P_{\text{ui}})))
   \]
   \[
   N = h(ID_i \| sk) \oplus h(ID_i \| h(PW_{\text{new}}^i \| P_{\text{ui}}^{\text{new}}))
   \]

Now $U_i$ transmits $\{ID_i, W, N\}$ to the $S$.

2. On getting the message, $S$ concludes: $W' = h(sk_e \| VPW \oplus h(P_s))$ and verifies whether it is equal to the acquired $W$. Then $S$ computes $VPW_{\text{new}} = h(P_s) \oplus h(ID_i \| sk) \oplus N$ and updates $VPW$ with $VPW_{\text{new}}$.

3 Cryptanalysis of Lu et al.’s scheme

In this section, it is revealed that the Lu et al.’s scheme is impressionable to server and user masquerading attacks and also unable to achieve the user anonymity. Moreover, it also has incorrect authentication phase on server side. As per adversary model mentioned in [30–34], $A$ can access the public communication link and can replay, remove, modify, intercept or can send a new devised message.

3.1 User anonymity attack

The user anonymity violation is observed in this subsection. In the Lu et al.’s protocol, any legitimate user can derive the authentic identity of the specific user by intercepting the login request message from the public communication channel.

Assume a legal user $U_j$ try to extract the authentic identity of the another user $U_i$. $U_j$, performs the following steps.

1. User $U_j$ steals the information $VPW$ stored on the server.

2. Now by using his/her $ID_j$, $PW_j$ and $P_{\text{ui}}$, $U_j$ computes $PWD_j = h(PW_j \| P_{\text{ui}})$ and obtains the value $T = h(ID_j \| PWD_j)$. Now, $U_j$ can also extract the server private key $h(P_s) = T \oplus VPW$.

3. $U_j$ intercepts the $U_i$ login request message $\{Y, HID_i, Z\}$ and sends it to the server $S$ from the public communication channel.

4. Now by using the stolen verifier $VPW$, he/she can compute $T' = VPW \oplus h(P_s)$. Finally, $U_j$ extracts the real identity $ID_i$ of user’s $U_i$ as $ID_j = HID_i \oplus T'$.

3.2 Server masquerading attack

In Lu et al.’s scheme, if $A$ devised the server $S$’s secret key $P_s$, another authorized user $U_j$ can easily masquerade as a legal server by executing the subsequent steps.
1. Adversary $A$ can steal the information $V\ PW$ stored in the server’s repository. Then the following steps have to be performed by the $A$

\[ PWD_i = h(PW_i || P) \]  
\[ T = h(ID_i || PWD_i) \]  
\[ h(P_i) = T \oplus V\ PW \]  

2. When $U_i$ a legal user needs to login into the server,$U_i$ calculates:

- generates $r_i$

\[ T = h(ID_i || h(PWi || P)) \]  
\[ X = r_i.P \]  
\[ Y = T \oplus X \]  
\[ HID_i = ID_i \oplus T \]  
\[ Z = h(ID_i || X) \]  

Now $U_i$ conveys the request message $\{ Y, HID_i, Z \}$ to the server $S$.

3. $A$ computes after intercepting the request message:

\[ T' = V\ PW \oplus h(P_i) \]  
\[ X' = Y \oplus T' \]  
\[ \overline{ID}_i' = HID_i \oplus T' \]  

- generates $r_2$

\[ D = r_2.P \]  
\[ sk_i = r_2.X' \]  
\[ Auth_i = h(sk_i || T' || X') \]  

After that $A$ transmits $CHALLENGE(realm, D, Auth_i)$ to the legal user $U_i$. 
4. On getting the challenge message, \( \mathcal{U}_i \) computes:

\[
sk_{ui} = r_1.D \tag{32}
\]

\[
Auth'_i = h(sk_{ui} \| T \| X) = Auth_i \tag{33}
\]

\[
Auth_{ui} = h(sk_{ui} \| T \| D) \tag{34}
\]

5. The \( \mathcal{U}_i \) conveys the response message \( RESPONSE(realm, Auth_{ui}) \) to the server \( \mathcal{S} \), whereas, \( \mathcal{A} \) intercepts the message. Hence, \( \mathcal{A} \) successfully masquerades the server for legal users.

### 3.3 User masquerading attack

For user masquerading attack, an attacker \( \mathcal{A} \) will get the request message \( \{Y, HID_i, Z\} \) and derive the identity \( ID_i \) as mentioned in 3.1. Now, any legitimate user \( \mathcal{U}_j \) can easily masquerade another user \( \mathcal{U}_i \) by performing subsequent steps:

1. \( \mathcal{A} \) intercepts the remote user \( \mathcal{U}_i \) request message \( \{Y, HID_i, Z\} \) and computes:

\[
\bar{T'} = HID_i \oplus ID_i \tag{35}
\]

Generate \( r_1 \) \hspace{1cm} (36)

\[
\bar{X'} = r_1.P \tag{37}
\]

\[
\bar{Y} = \bar{T'} \oplus \bar{X'} \tag{38}
\]

\[
Z = h(ID_i \| \bar{X'}) \tag{39}
\]

\( \mathcal{A} \) transmits his own request message \( \{\bar{Y}, \bar{HID}_i, Z\} \).

2. \( \mathcal{S} \) upon getting the message computes:

\[
T' = V PW \oplus h(P_i) \tag{40}
\]

\[
X' = \bar{Y} \oplus T' \tag{41}
\]

\[
ID'_i = \bar{HID}_i \oplus T' \tag{42}
\]

Verify \( Z = h(ID'_i \| X') \neq Z \) \hspace{1cm} (43)

Generate \( r_2 \) \hspace{1cm} (44)

Computes \( D = r_2.P \) \hspace{1cm} (45)

\[
sk_i = r_2.X' \tag{46}
\]

\[
Auth_i = h(sk_i \| T' \| X') \tag{47}
\]
S transmits the challenge message \{realm, D, Auth_s\} to U.

3. Upon getting the message A computes:

\[ sk_u = r_1 \cdot D \]  
\[ Auth_u = h(sk_u \| T' \| X) = Auth_s \]  
\[ Auth_{ui} = h(sk_u \| T' \| D) \]

Therefore, A sends the response message to S.

4. On receiving the message, the S authenticates the adversary as a legal user by verifying \( Auth_{ui} = h(sk_u \| T' \| D) \) equation. Therefore, A has successfully misled the server S and S treats the shared session key as a valid key.

### 3.4 Incorrectness problem

In this segment, it is demonstrated that while authentication is performed on the server side the server, computes \( T' = VPW \oplus h(\mathcal{P}_s) \), where, \( h(\mathcal{P}_s) \) is the private key of the server which is secret within the server. But how the server can compute the exact value of \( T' \), without knowing the valid ID_i of the specific user as the verifier table contains the \( T \) values of all the legal users of the system.

### 4 Proposed scheme

In this segment, a new proposed protocol is presented. The improved protocol is divided into three phases, i.e., System Setup, Registration and Authentication phase. Before going into the details of proposed protocol, it explains that the insecurity of Lu et al.’s scheme against server and user’s masquerading attacks was due to a generic secret value \( h(\mathcal{P}_s) \) hideously stored in the verifier table \( VPW \) into the server. A legitimate but dishonest user (say \( U_j \)) can easily extract \( h(\mathcal{P}_s) \) by using his/her \( T \) which is computed as \( T = h(ID_j \| PWD_j) \) and then with the help of this \( T \), it can compute server private key \( h(\mathcal{P}_s) = T \oplus VPW \). After obtaining \( h(\mathcal{P}_s) \), the illegitimate but authorized user \( U_j \) can easily find the real identity of any other user. Moreover, the \( U_j \) after stealing the \( VPW \) from the server can easily masquerade himself as \( U_i \) as well as the legal server. In present protocol, \( VPW \) consist of user’s particular identity \( ID_i \). Hence, if A successfully gets the secrets from the verifiers table, one can retrieve his/her own value of \( PWD \) as user \( ID_i \) is inserted with server secret key. So, he cannot masquerade himself as another user or server of the systems though he has also \( VPW \) verifier table. The scheme is illustrated in Fig 2 and is explain as follows:

### 4.1 System setup phase

1. The server S selects elliptic curve [35] points \( (E(a, b)) \) of order n and gets initialized with a base point \( P \).

2. The secret key \( \mathcal{P}_s \in_R Z_p^* \) is being generated by S ranging from \( (\mathcal{P}_s \in [0, n-1]) \) and S computes the public key as \( Q_s = \mathcal{P}_s \cdot P \). Then S selects one-way hash function \( h() \), which keeps the secret key \( \mathcal{P}_s \) safe and publishes the rest of the public parameters.
4.2 Registration phase

1. $U_i$ computes $PWD_i = h(ID_i \| PW_i \| P_{ui})$ and conveys $\{ID_i, PWD_i\}$ to $S$ through secure channel.

2. On getting the message, $S$ computes $VPW_i = PWD_i \oplus h(P_s \| ID_i)$ and saves the $VPW_i$ in the server database.

4.3 Authentication phase

1. First of all, a random number $r_1$ is generated by $U_i$ and it computes:

\[
PWD_i = h(ID_i \| PW_i \| P_{ui})
\]

Fig 2. Proposed scheme.

https://doi.org/10.1371/journal.pone.0186044.g002
A robust ECC based mutual authentication protocol with anonymity for SIP

\[ X = r_1.P \] (52)

\[ M_1 = r_1.Q_u \] (53)

\[ M_2 = E_x(t, ID, X, PWD_u) \] (54)

Now \( U_i \) sends request message \( \text{REQUEST} \{ M_1, M_2 \} \) to \( S \).

2. \( S \) computes the following, upon getting the request message

\[ X' = M_1, P_s^{-1} \] (55)

\[ (t, ID, X, PWD_u) = D_s(M_2) \] (56)

Check if \( t \) is fresh

Extract \( V PW_i \) using \( ID_i \)

\[ PWD'_i = V PW_i \oplus h(P_s, ID_i) \] (59)

Compute and check \( PWD'_i \triangleq PWD_i \), failure of which leads to the termination of session, otherwise \( S \) generates \( r_2 \) and computes:

\[ D = r_2.P \] (60)

\[ M_3 = D \oplus X' \] (61)

\[ sk_s = r_2 \cdot X' \] (62)

\[ Auth_i = h(sk_s, PWD'_i, X') \] (63)

\( S \) transmits the message \{\( \text{realm}, M_3, Auth_i \} \) to the \( U_i \).

3. Upon receiving the message, \( U_i \) calculates:

\[ D' = M_3 \oplus X \] (64)

\[ sk_{ui} = r_1 \cdot D' \] (65)

and verifies the condition \( Auth'_i = h(sk_{ui}, PWD'_i, X') \triangleq Auth_i \), failure of which leads to the termination of the session, otherwise \( U_i \) computes \( Auth_{ui} = h(sk_{ui}, PWD_i, D') \) and transmits \( \text{RESPONSE} \{ \text{realm}, Auth_{ui} \} \) message to \( S \).

4. On receipt of the message \{\( \text{realm}, Auth_{ui} \} \), the \( S \) verifies \( h(sk_{ui}, PWD'_i, D') \triangleq Auth_{ui} \), if it withstands, the session key \( sk = sk_{ui} = sk_s \) is considered to be the valid key between \( U_i \) and \( S \).
5 Security analysis

Security analysis informal and formal of the present stated scheme demonstrates that it is resilient against all known attacks over public communication channels.

5.1 Informal security analysis

5.1.1 Resist replay attack. Suppose if an eavesdropper can steal the request message \( \{M_1, M_2\} \) and try to replay it to pretend as a legal user \( U_i \), but on the server side \( S \) verifies the freshness of time stamp \( t_i \) and also the condition \( PWD_i = V^{PW} \ominus h(PW \| ID_i) \ominus PWD_i \). To successfully pass the condition, \( A \) requires \( ID_i \) and server secret key \( P \). But \( A \) is unable to get \( ID_i \) and server secret key \( P \). Hence, the proposed scheme provides appropriate anonymity.

5.1.2 Anonymity and privacy. In the proposed scheme, the \( ID_i \) is protected on the public channel by hash function along with user secret key \( P \). So, it is impossible for \( A \) to get the \( ID_i \) from the public channel. Hence, the proposed scheme provides appropriate anonymity.

5.1.3 Off-line password guessing attack. Suppose if \( A \) can steal the \( REQUEST \{M_1, M_2\} \) but password is secured in \( M_2 \) and for retrieving the password from \( M_2 \) it is required to calculate the \( PWD_i \) and it is impossible for \( A \) to obtain these parameters due to the security of hash function. Even if the password is compromised, it is impossible for \( A \) to prove the legitimacy of the password. Hence, the present protocol withstands against off-line password guessing attack.

5.1.4 Mutual authentication. In the present protocol both user \( U_i \) as well as server \( S \) compute \( Auth'_i = h(sk \| PWD_i \| D) \) and verifies \( Auth'_i = Auth_{ui} \) on server side and similarly, \( Auth'_i = h(sk \| PWD_i \| X) = Auth_{ui} \) on client side. So, improved scheme fulfills the requirement of mutual authentication.

5.1.5 Perfect forward secrecy. Suppose if the secret keys of \( U_i \) and \( S \) are compromised, \( A \) is still unable to guess the session keys \( sk = r_1, r_2, P \). It is infeasible for \( A \) to compute \( r_1 \) and \( r_2 \) from \( X \) and \( D \), respectively, due to ECDLP. Hence, the present protocol provides forward secrecy.

5.1.6 Masquerading attack. For user masquerading, \( A \) requires user password \( PW_i \) to compute the valid value of \( PWD_i \). Assume \( A \) successfully intercepts the request message \( \{M_1, M_2\} \), it is not possible to compute the value of \( PWD_i \) from \( M_1, M_2 \) due to the hardness of ECDLP and \( M_2 \) contains the encrypted value by \( X \). For server masquerading attack, \( A \) requires verifier \( V^{PW} \) from server database and secret key \( P \), which is only known to the server. Without \( P \), server secret key, \( A \) is unable to compute the \( PWD_i \) from \( V^{PW} \). For authenticating the user, \( A \) also needs the \( r_1 \) to compute the \( X \), so, \( A \) is unable to authenticate \( E_X(t_i \| ID_i \| X \| PWD_i) = M_2 \). Moreover, \( r_2 \) is required to compute \( sk \) and \( Auth_{ui} \). Hence, the proposed scheme resists against masquerading attack.

5.1.7 Resist insider attack. In registration phase of the newly stated protocol. \( U_i \) transmits a message containing \( (ID_i, PWD_i) \) instead of \( (ID_i, PW_i) \), where \( PWD_i = h(ID_i \| PW_i \| P \). So, \( A \) is incapable of obtaining the user’s password \( PW_i \) without knowledge of \( P \). Hence, it is impossible for \( A \) to launch the insider attack.

5.1.8 Session key secrecy. The two random numbers \( r_1 \) and \( r_2 \) are used to compute the session key for every session. These two numbers are chosen by the server \( S \) and user \( U_i \), independently, which is different in each session. So, if one of the session key is exposed, the rest of the session keys will persist. Hence, the new proposal achieved the session key secrecy.
5.2 Formal security analysis

This segment, demonstrates the formal security analysis of the present protocol. This analysis validates the claim about the proposed scheme that it is provably secured.

**Theorem 1** The robust authentication protocol with anonymity using ECC for session initiation protocol PREBMAPSIP is provably secured against an adversary \( \mathcal{A} \). Due to ECDLP assumption and security of hash function, it is impossible to obtain the user \( U_i \)'s real identity \( ID_i \), password \( PW_i \), user private key \( P_{ui} \) and shared session key \( sk \) within user \( U_i \) and the server \( S \).

**Proof 1** For analysis of the present stated protocol that it is provably secured, the similar model as [33, 34, 36, 37] is adopted.

Before proceeding ahead, following oracles are defined:

- **Extract 1**: This oracle results from input \( A \) out of a secure one-way hash function \( B = h(A) \).
- **Extract 2**: Result of this oracle is the plain text \( p \) from cipher text \( C = Ek(p) \) without the knowledge of shared symmetric key \( k \).
- **Extract 3**: This oracle returns the integer multiplier \( a \) out of given an ECC point \( aP \).

\( A \) performed the experiment \( \text{exp}^{\text{Hash,Ecdlp,Symenc,A,PREBMAPSIP}} \) to break the proposed PREBMAPSIP protocol. \( A \) is allowed to use Extract 1, Extract 2 and Extract 3 oracles for the said purpose. \( A \) has the potential to retrieve the user's private key \( P_{ui} \), user's password \( PW_i \), and shared session key \( sk \) by executing the experiment \( \text{exp}^{\text{Hash,Ecdlp,Symenc,A,PREBMAPSIP}} \) and by use of oracles Extract 1, Extract 2 and Extract 3. The probability of success for the said experiment

\[ \text{Adv}^{\text{Hash,Ecdlp,Symenc,A,PREBMAPSIP}}(t_{ex}, q_{e1}, q_{e2}, q_{e3}) = \max_{\mathcal{A}} (\text{succ}) , \text{where, } A \text{ performed several queries } q_{e1}, \]

\[ q_{e2} \text{ and } q_{e3} \text{ in polynomial time } t. \]

According to experiment \( \text{exp}^{\text{Hash,Ecdlp,Symenc,A,PREBMAPSIP}} \), \( A \) can break the PREBMAPSIP security if and only if he can (1) break security of One-way hash function (inversion), (2) obtained the plain text without the knowledge of key (Decipher text) and (2) break ECDLP (extracting scalar). However, it is computationally impractical to break One-way hash function, decrypt the message without key and ECDLP. Hence, the newly presented protocol for SIP is provably secure against \( A \) to acquire \( ID_i, PW_i, P_{ui}, \) and \( sk \).

**Algorithm 1** \( \text{exp}^{\text{Hash,Ecdlp,Symenc,A,PREBMAPSIP}} \)

\[
\text{1: Eavesdrop the request message } (M_1, M_2), \text{Where } M_2 = E_X(t_i||ID_i||X||PW_i) \\
\text{2: Call Extract 2 on } E_X(t_i||ID_i||X||PW_i) \text{ to obtain } (f_i||ID_i||X||PW_i) \leftrightarrow \text{ Extract 2 } (M_2) \\
\text{3: Call Extract 3 on } (X') \text{ to obtain } (r_i') \leftrightarrow \text{ Extract } (X') \\
\text{4: Eavesdrop challenge message } (M_3, \text{Auth}_i), \text{Where } \text{Auth}_i = h(sk_\|T||X) \\
\text{5: Call Extract 1 on } h(sk_\|T||X) \text{ and get } (s', T, X) \leftrightarrow \text{ Extract 1 } (\text{Auth}_i) \\
\text{6: Call Extract 3 on } (X') \text{ to obtain } (r_i') \leftrightarrow \text{ Extract } (X') \\
\text{7: then if } (r_i' = r_i) \\
\text{8: Compute } X' = r_i'.P. \\
\text{9: if } X' = X' \text{ then } . \\
\text{10: Accept } ID_i' \\
\text{11: Call Extract on } PW_i \text{ to obtain } (ID_i', PW_i', P_{ui}') \leftrightarrow \text{ Extract 1 } (PW_i). \\
\text{12: Accept the deduced } ID_i', PW_i', P_{ui}' \text{ and } sk_i \text{ as the appropriate user's identity } ID_i, \text{ user's password } PW_i, \text{ user's secret key } P_{ui} \text{ and session key } sk_i \text{ between } U_i \text{ and } S. \\
\text{13: return Success} \text{ \text{\ 14: else} } \\
\text{15: return Fail} \text{ \text{\ 16: end if}}
\]
6 Performance & security comparisons

6.1 Computation cost analysis

The present protocol’s performance and security analysis is evaluated with previously stated schemes [24–29, 38–41] in this segment. Registration phase is performed only once before authentication, so, the authentication phase mainly focuses on the performance comparison. For performance calculation, the notation used for the different cryptographic operation are as follows:

- \( t_{sh} \): time to compute secure One-way hash function
- \( t_{em} \): time to calculate point multiplication
- \( t_{cal} \): time to calculate point addition operations
- \( t_{emp} \): time to calculate map to point operation
- \( t_{E_{e}} \): time for a symmetric encryption/decryption

The running times for \( t_{sh}, t_{em}, t_{cal}, t_{emp} \), and \( t_{E_{e}} \) are approximately 0.0023 ms, 2.226 ms, .0288 ms, 0.947 ms and 0.0046 ms, respectively mentioned by Kilinc and Yanik [42] recently. Furthermore, XOR and inverse operation are neglected due to the insignificance of these operations, as indicated by Kilinc and Yanik. Performance comparison is demonstrated in the Table 2 with the recent allied schemes.

Table 2 demonstrates that the present protocol possess the same running time as compared with the previously proposed schemes [27]. Moreover, [27] is found to be insecure against some known attacks. The remaining schemes [24–26, 28, 29, 38–41] almost have relatively extended running time and they are also found insecure against some known attacks. Moreover, proposed scheme is provably secure and resists against all possible attacks shown in section 5.

6.2 Communication cost analysis

The communication cost analysis is demonstrated in Table 3 of the present protocol with the counter part schemes [24–29, 38–41]. The present protocol acquires same or less communication overhead as compared with relevant schemes [24–26, 28, 29, 38–41], whereas, it has some additional communication overhead as compared to [27]. However, in term of the number of

| Schemes       | User       | Server     | Total     | Running time |
|---------------|------------|------------|-----------|--------------|
| Lu et al. [29]| 4\(t_{sh}\) + 2\(t_{em}\) | 4\(t_{sh}\) + 2\(t_{em}\) | 8\(t_{sh}\) + 4\(t_{em}\) | \(\approx\) 8.9224 |
| Arshad et al. [24]| 4\(t_{sh}\) + 2\(t_{em}\) | 4\(t_{sh}\) + 3\(t_{em}\) | 8\(t_{sh}\) + 5\(t_{em}\) | \(\approx\) 11.1484 |
| Yoon et al. [25]| 2\(t_{sh}\) + 2\(t_{em}\) + 1\(t_{aa}\) | 2\(t_{sh}\) + 4\(t_{em}\) + 2\(t_{aa}\) | 4\(t_{sh}\) + 6\(t_{em}\) + 3\(t_{aa}\) | \(\approx\) 9.4892 |
| Xie’s. [26]    | 3\(t_{sh}\) + 3\(t_{em}\) + 1\(t_{aa}\) | 2\(t_{sh}\) + 3\(t_{em}\) + 1\(t_{Es}\) | 5\(t_{sh}\) + 6\(t_{em}\) + 1\(t_{aa}\) + 1\(t_{Es}\) | \(\approx\) 13.4009 |
| He et al. [38] | 3\(t_{sh}\) + 3\(t_{em}\) | 3\(t_{sh}\) + 3\(t_{em}\) | 6\(t_{sh}\) + 6\(t_{em}\) | \(\approx\) 13.3698 |
| Farash et al. [27]| 4\(t_{sh}\) + 2\(t_{em}\) | 3\(t_{sh}\) + 2\(t_{em}\) | 7\(t_{sh}\) + 4\(t_{em}\) | \(\approx\) 8.9201 |
| Zhang et al. [39]| 6\(t_{sh}\) + 3\(t_{em}\) + 1\(t_{aa}\) | 3\(t_{sh}\) + 3\(t_{em}\) + 2\(t_{aa}\) | 9\(t_{sh}\) + 6\(t_{em}\) + 3\(t_{aa}\) | \(\approx\) 13.4631 |
| Yeh et al. [40]| 7\(t_{sh}\) + 4\(t_{em}\) + 2\(t_{aa}\) | 6\(t_{sh}\) + 4\(t_{em}\) + 2\(t_{aa}\) + 1\(t_{emr}\) | 13\(t_{sh}\) + 8\(t_{em}\) + 4\(t_{aa}\) + 1\(t_{emr}\) | \(\approx\) 18.9001 |
| Zhang et al. [28]| 4\(t_{sh}\) + 3\(t_{em}\) | 5\(t_{sh}\) + 3\(t_{em}\) | 9\(t_{sh}\) + 6\(t_{em}\) | \(\approx\) 13.3767 |
| Tu et al. [41]| 7\(t_{sh}\) + 3\(t_{em}\) + 1\(t_{aa}\) | 3\(t_{sh}\) + 4\(t_{em}\) + 2\(t_{aa}\) | 10\(t_{sh}\) + 7\(t_{em}\) + 3\(t_{aa}\) | \(\approx\) 15.6914 |
| Proposed     | 3\(t_{sh}\) + 2\(t_{em}\) | 4\(t_{sh}\) + 2\(t_{em}\) | 7\(t_{sh}\) + 4\(t_{em}\) | \(\approx\) 8.9247 |

https://doi.org/10.1371/journal.pone.0186044.t002
messages exchanged, the present protocol provides better performance as compared to previously stated schemes.

6.3 Security comparison

In Table 4, the comparison of security parameters for the present protocol with conventional schemes [24–29, 38–41] is summarized. It is easier to draw the conclusion from Table 4 that the proposed scheme results are better as compared to its counterpart other conventional schemes. The proposed scheme not only outrun in efficiency but also provides mutual authentication. The proposed protocol is robust against the user as well as server masquerading attack.

7 Conclusion

In this research work, the Lu et al.’s scheme is cryptanalyzed and it is exhibited that the protocol is insecure against the server and user masquerading attacks. Moreover, the login and authentication phase is found to be incorrect. To overcome these drawbacks, a novel technique is proposed for reducing the processing time and enhancing the system protection. It is proved to be relatively more secure than the conventional techniques as it is verified through well known random oracle model. Hence, the proposed technique provides enhanced security and better performance. So, it is suitable for the practical applications.

Acknowledgments

This Research work is funded by the National key R & D Project Research on New Principle and New Algorithm of Electronic Currency under grant No. yfb0802505(2017), NSFC-
Zhejiang Joint Fund for the Integration of Industrialization and Informatization under grant No. U1509219, National Science Foundation of China Grant No. 61271220 and Priority Development Field Project of Doctoral Fund under grant No. 20130073130006 and Shanghai Municipal Science and Technology Project under grant No. 16511102605 and No. 16DZ1200702.

Author Contributions
Data curation: Linsen Li.
Formal analysis: Zahid Mehmood.
Funding acquisition: Gongliang Chen, Jianhua Li.
Investigation: Zahid Mehmood.
Methodology: Zahid Mehmood.
Resources: Gongliang Chen, Jianhua Li, Linsen Li, Bander Alzahrani.
Software: Jianhua Li.
Supervision: Gongliang Chen.
Writing – original draft: Zahid Mehmood.
Writing – review & editing: Gongliang Chen, Bander Alzahrani.

References
1. Salsano S, Veltri L, Papalilo D. SIP security issues: the SIP authentication procedure and its processing load. IEEE network, 16(6), (2002), 38–44. Available from: http://dx.doi.org/10.1109/MNET.2002.1081764.
2. Chaudhry S. A, Naqvi H, Sher M, Farash M. S, Hassan M U. An improved and provably secure privacy preserving authentication protocol for SIP. Peer-to-Peer Networking and Applications, 10(1) (2017), 1–15. Available from: http://dx.doi.org/10.1007/s12083-015-0400-9.
3. Irshad A, Sher M, Rehman E, Chaudhry S. A, Hassan M. U, Ghani A A single round-trip sip authentication scheme for voice over internet protocol using smart card. Multimedia Tools and Applications, 74(11), (2015), 3967–3984. Available from: http://dx.doi.org/10.1007/s11042-013-1807-z.
4. Kumari S.Design flaws of an anonymous two-factor authenticated key agreement scheme for session initiation protocol using elliptic curve cryptographyMultimedia tools and applications, 76.11 (2017): 13581–13583. Available from: http://dx.doi.org/10.1007/s11042-013-1807-z.
5. Kumari S, Karuppi M, Das A. K, Li X, Wu F, Gupta V. Design of a secure anonymity-preserving authentication scheme for session initiation protocol using elliptic curve cryptography. Journal of Ambient Intelligence and Humanized Computing, 1–11. (2017). Available from: http://dx.doi.org/10.1007/s12652-017-0460-1.
6. Chaudhry S. A. Comment on ‘Robust and efficient password authenticated key agreement with user anonymity for session initiation protocol-based communications IET Communications. 2015; 9 (7): 1034–1034. Available from: http://dx.doi.org/10.1049/iet-com.2014.1082
7. Yang C. C, Wang R. C, Liu W. T. Secure authentication scheme for session initiation protocol. Computers and Security Elsevier. 2005, 24(5), 381–386. Available from: http://dx.doi.org/10.1016/j.cose.2004.10.007
8. Geneiatakis D, Dagiuikas T, Kambourakis G, Lambrinoudakis C, Gritzalis S, Ehert S, Sisalem D. Survey of security vulnerabilities in session initiation protocol. IEEE Communications Surveys and Tutorials 8 (1–4) (2006) 68–81. Available from: http://dx.doi.org/10.1109/COMST.2006.253270
9. Sisalem D, Kuthan J, Ehert S. Denial of service attacks targeting a sip voip infrastructure: attack scenarios and prevention mechanisms, Network IEEE 20 (5) (2006) 26–31. Available from: http://dx.doi.org/10.1109/MNET.2006.1705880
10. Huang H. F, Wei W. C. A new efficient authentication scheme for session initiation protocol. computing 1 (2). Available from: http://dx.doi.org/10.2991/jcis.2006.222
11. Jo H, Lee Y, Kim M, Kim S, Won D. Off-line password-guessing attack to yang’s and huang’s authentication schemes for session initiation protocol. in: INC, IMS and IDC, 2009. NCM’09. Fifth International Joint Conference on IEEE 2009, pp. 618–621. Available from: http://dx.doi.org/10.1109/NCM.2009.251

12. Durukan A, Sogukpinar I. Sip authentication scheme using ecdh. World Enformatika Society Transations on Engineering Computing and Technology 8 (2005) 350–353. Available from: http://citeserxtist.psu.edu/viewdoc/download?doi=10.1.1.192.9488&rep=rep1&type=pdf

13. Koblitz N. Elliptic curve cryptosystems. Mathematics of computation 48 (177) (1987) 203–209. Available from: http://dx.doi.org/10.1090/S0025-5718-1987-0866109-5

14. Islam Hafizul SK, Amin R, Biswas GP, Farash M S, Xiong Li, Kumari S. Improved three party authenticated key exchange protocol using hash function and elliptic curve cryptography for mobile-commerce environments Journal of King Saud University Computer and Information Sciences Available from https://doi.org/10.1016/j.jsuci.2015.08.002.

15. Islam Sk Hafizul, and Biswas G P. Design of two-party authenticated key agreement protocol based on ECC and self-certified public keys. Wireless Personal Communications 82.4 (2015): 2727–2750. Available from: http://dx.doi.org/10.1007/s11277-015-2375-5

16. Islam S H, Biswas G P. An improved pairing-free identity-based authenticated key agreement protocol based on ECC. Procedia Engineering, 30, (2012), 499–507. Available from: http://dx.doi.org/10.1016/j.proeng.2012.01.890

17. Liao Y P, Wang S S. A new secure password authenticated key agreement scheme for sip using self-certified public keys on elliptic curves. Computer Communications 33 (3) (2010) 372–380. Available from: http://dx.doi.org/10.1016/j.comcom.2009.10.005

18. Chaudhry S A, Naqvi H, Sher M, Farash M S, Hassan M U. An improved and provably secure privacy preserving authentication protocol for sip. Peer-to-Peer Networking and Applications (2015) –15. Available from: http://dx.doi.org/10.1016/j.ijpn.2012.01.890

19. Zhang Z, Qi Q, Kumar N, Chilamkurthy, and Jeong H Y. A secure authentication scheme with anonymity for session initiation protocol using elliptic curve cryptography. Multimedia Tools and Applications 74 (10) (2015) 3477–3488. Available from: http://dx.doi.org/10.1007/s11284-014-1885-6

20. Lu Y, Li L, Peng H, Yang Y. A secure and efficient mutual authentication scheme for session initiation protocol. Peer-to-Peer Networking and Applications 9(2) (2016) 449. Available from: http://dx.doi.org/10.1007/s12083-015-0363-x

21. Eisenbarth T, Kasper T, Moradi A, Paar C, M. Salmasizadeh, Shalmani M. T. M. On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme. Advances in Cryptology—CRYPTO 2008 Springer 2008, pp. 203–220. Available from: http://dx.doi.org/10.1007/978-3-540-85174-5_12.
31. Yang W H, Shieh S P. Password authentication schemes with smart cards. Computers & Security 18 (8) (1999) 727–733. Available from: http://dx.doi.org/10.1016/S0167-4048(99)80136-9.
32. Höbl M, Welzer T, Brumen B. An improved two-party identity-based authenticated key agreement protocol using pairings. Journal of Computer and System Sciences 78 (1) (2012) 142–150. Available from: http://dx.doi.org/10.1016/j.jcss.2011.01.002.
33. Kocher P, Jaffe J, Jun B. Differential power analysis. Advances in Cryptology—CRYPTO’99 Springer, 1999, pp. 388–397. Available from: http://dx.doi.org/10.1007/3-540-48405-1.25
34. Messerges T S, Dabbish E, Sloan R H. Examining smart-card security under the threat of power analysis attacks. Computers IEEE Transactions on 51 (5) (2002) 541–552. Available from: http://dx.doi.org/10.1109/TC.2002.1004593
35. Hankerson D, Menezes A J, Vanstone S. Guide to elliptic curve cryptography. Springer Science & Business Media, 2006. Available from: https://link.springer.com/book/10.1007.2Fb97644
36. Odelu V, Das A K, Goswami A. A secure effective key management scheme for dynamic access control in a large leaf class hierarchy. Information Sciences 269 (2014) 270–285. Available from: http://dx.doi.org/10.1016/j.ins.2013.10.022
37. Chatterjee S, Das A K, Sing J K. An enhanced access control scheme in wireless sensor networks. Adhoc & Sensor Wireless Networks 21 (1).
38. He D, Chen J, Chen Y. A secure mutual authentication scheme for session initiation protocol using elliptic curve cryptography. Security and Communication Networks 5 (12) (2012) 1423–1429. Available from: http://dx.doi.org/10.1002/sec.506
39. Zhang L, Tang S, Cai Z. Efficient and flexible password authenticated key agreement for voice over internet protocol session initiation protocol using smart card. International Journal of Communication systems 27 (11) (2014) 2691–2702. Available from: http://dx.doi.org/10.1002/dac.2499
40. Yeh H L, Chen T H., Shih W K. Robust smart card secured authentication scheme on sip using elliptic curve cryptography. Computer Standards & Interfaces 36 (2) (2014) 397−402. Available from: http://dx.doi.org/10.1016/j.csi.2013.08.010
41. Tu H, Kumar N, Chilamkurti N, Rho S. An improved authentication protocol for session initiation protocol using smart card. Peer-to-Peer Networking and Applications (2014) 1–8. Available from: http://dx.doi.org/10.1007/s12033-014-0248-4
42. Kilinc H H, Yanik T. A survey of sip authentication and key agreement schemes. Communications Surveys & Tutorials IEEE 16 (2) (2014) 1005–1023. Available from: http://dx.doi.org/10.1109/SURV.2013.091513.00050