An Untraceable ECC-Based Remote User Authentication Scheme

Zahid Mehmood[1], Gongliang Chen[1], Jianhua Li [1], Aiiad Albeshri[2]
[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, Saudia Arabia
[1]zaidi@sjtu.edu.cn, [1]chengl@sjtu.edu.cn., [1]lijh888@sjtu.edu.cn, [2]aaalbeshri@kau.edu.sa
*Corresponding author: Zahid Mehmood

Received September 22, 2016; revised December 26, 2016; accepted January 15, 2017; published March 31, 2017

Abstract

Recent evolution in the open access internet technology demands that the identifying information of a user must be protected. Authentication is a prerequisite to ensure the protection of user identification. To improve Qu et al.'s scheme for remote user authentication, a recent proposal has been published by Huang et al., which presents a key agreement protocol in combination with ECC. It has been claimed that Huang et al. proposal is more robust and provides improved security. However, in the light of our experiment, it has been observed that Huang et al.'s proposal is breakable in case of user impersonation. Moreover, this paper presents an improved scheme to overcome the limitations of Huang et al.'s scheme. Security of the proposed scheme is evaluated using the well-known random oracle model. In comparison with Huang et al.'s protocol, the proposed scheme is lightweight with improved security.

Keywords: Smart-card, Key agreement, Remote user authentication, Password-based authentication

1. Introduction

Due to the rapid growth in information and communicaion technology, the need for improved protection and security requirments is also climbing to its peak. Therefore, user protection over a public network is a crucial factor. A plathora of security proposals can be found in the recent literature to improve security of the communication systems. The first proposal on password-based authentication came from Lamport [1] in 1981, to protect remote user access. Later followed by many researchers proposing cryptographic authentication schemes [2-6]. Hash function has been used in the proposal in [2], for securing user passwords. An improved version for password authentication has been introduced in Lin et al. [3] including a password change phase. However, the idea of a password based authentication and password change struggled agianst various security breach. This led the research community to investigate the feasibility of two factor authentication in remote user scenarios. Some populare two-factor authentication protocols has been introduced in the literature [4–24,37] in recent years. One such proposal came from Juang et al. [7] where ECC is used for designing a key agreement protocol, claiming reducation in computation and communication costs. Xu et. al. [10] pointed out that Lee et al.'s schemes [21, 22] are breachable in the case of offline password-guessing and forgery attacks, respectively. Later on another authentication protocol using smart-card came from Yung et al. [8], using Diffie-Hellman algorithm verified through random oracle model. However, Xu et al. protocol is analyzed by Sood et al. [23] along with another proposal from Song [24] where both argued that Xu et al.'s protocol is venerable to internal and impersonation attacks. The improved protocol of Sood et al. [23] as well as that of Song [24] is reported to have failure in case of mutual authentication, by Chen et al. [25]. Furthermore, Song's protocol is aslo breachable against internal and password guessing attacks if the smart-card gets stolen. Followed by their new proposal claiming to be attack proof against all known breaches. However, Jiang et al. [26] claimed that Chen et al.'s [25] protocol is venerable to offline dictionary attack and does not achieve the perfect realization of anonymity. Authetication of remote user is also investigated by Qu et al. [19] using a two-factor key agreement protocol based on ECC, claiming it to be user anonymous as well as resistant against masquerade attack and stolen smart-card stolen attack. Later on in 2014, Qu et al.'s protocol is analyzed by Huang et al. [27] reporting it to be vulnerable to impersonation and stolen smart-card attacks. Furthermore, they introduced a scheme for authenticating remote users using key agreement based on ECC. However, analysis of Huang et al.'s protocols presented in this paper shows vulnerability of this protocol in case of user impersonation attack. Furthermore, using elliptic curve cryptography, an untraceable remote user authentication protocol has been presented. The proposed scheme features high security and robustness in comparison to Huang et al.'s protocol.

Remainder of the paper is arranged section wise as follows: In section 2, Huang et al.'s technique is scrutinized. Cryptanalysis of Huang et. al.'s scheme is presented in section 3. Section 4 presents the proposed scheme followed by its security analysis in section 5 and performance comparison in presented in 6. Section 7, finally concludes the paper.

2. Review of Huang et al.'s Scheme

A comprehensive review of Huang et al.'s protocol is being presented in this section. An overall view of the protocol shows that after System Initiallization, it allows a user to register and then use it to login and authenticate itself. It also allows a user to change password in case of any undesired situation. From this perspective the protocol can be divided into four stages

namely; System Initialization, Registration, Login & Authentication whereas the last one being password change. Each of these stages are investigated in details as follows:

2.1 System initialization

The system initializes itself by executing the following steps at the server S:

1. Elliptic curve E(a, b) with base point P along with its corresponding order n, is chosen by the server S to get initialized.
2. m_{sk} being selected as the private key by the server S ranging from ($m_{sk} \in [0, n-1]$) where $n > 2^{160}$ and public key also computed as $m_{pk} = m_{sk}.P$. The server S then selects numerous one-way hash functions which are:
$H_1 : [0, 1]^* \longrightarrow G_p$, $H_2 : G_p \times G_p^* \longrightarrow Z^*_p$, $H_3 : [0, 1]^* \times G_p \times G_p \longrightarrow [0, 1]^k$, $H_4 : [0, 1]^* \times G_p \longrightarrow Z^*_p$ and $H_5 : G_p \times [0, 1] \times G_p \times G_p \longrightarrow [0, 1]^k$ respectively.
3. $\{E_p(a,b), m_{pk}, n, P, H_1, H_2, H_3, H_4, H_5\}$ are treated as public parameter and dissimeminated likewise.

Table 1. Notation Table

Notations	Description
U_x	Legitimate Client Identity
S	Server
ID_x	User Identity
PW_x	User Password
m_{sk}	Server S Secret key
Enc(.)	Symmetric Encryption
Dec()	Symmetric Decryption
Ą	Adversary
r_x	Distinct Random Number of U_x
SC_x	U_x's smart-card
H()	Private hash function
$\oplus$	Bitwise XOR operation
$\|\|$	Concatenation operator

1.2 Registration

A user U_x must register to be able to log on the system. To register a user performs the subsequent steps to complete the registration process.
1. The user U_x chooses his/her own identity ID_x, password PW_x, a random number r_x and computes $H_1 = (ID_x||PW_x||r_x)$. Then the message $\{ID_x, (ID_x||PW_x||r_x)\}$ is transmitted toward the server S through a secure channel.
2. On a registration request, calculation of $AID_x = (H_1(m_{sk}) +1).H_1(ID_x||PW_x||r_x)$ and $BID_x = H_2(H_1(ID_x)||H_1(ID_x||PW_x||r_x))$ is carried out at the server S. Followed by calculation of AID_x and BID_x the server S stores these parameters to the smart-card.
3. After receiving (AID_x,BID_x), the user U_x inserts a random number r_x into the smart-card.

1.3 Login and Authentication

At the end of the registration phase, user requests to log on to the server, followings steps have

been executed by user U_x.

Step 1: A smart-card when entered into the reader, a user must provide a distinct ID_x and a password PW_x. After this the smart-card calculates $BID'_x = H_2(H_1(ID_x)||H_1(ID_x||PW_x||r_x))$ and validates, $BID'_x \stackrel{?}{=} BID_x$. In case of failure, the session is aborted otherwise a random number $r_{tx} \in [1, n-1]$ choosen by the smart-card and computes:

$$R_{tx} = r_{tx}.P \quad (1)$$

$$M_x = r_{tx}.m_{pk} \quad (2)$$

$$TID_x = AID_x - H_1(ID_x||PW_x||r_x).P \quad (3)$$

$$CID_x = H_4(ID_x||M_x) \oplus H_2(M_x||TID_x) \quad (4)$$

$$DID_x = M_x \oplus H_1(ID_x||PW_x||r_x).P \quad (5)$$

$$EID_x = H_3(H_4(ID_x||M_x)||R_{tx}||M_x). \quad (6)$$

Now user U_x sends these entries to the server S like $\{CID_x, DID_x, EID_x, R_{tx}\}$.

Step 2: When the message is received, the server S computes:

$$M'_x = m_{sk}.R_{tx} \quad (7)$$

$$H_1(ID_x||PW_x||r_x).P = DID_x \oplus M_x \quad (8)$$

$$TID'_x = H_1(m_{sk}).(DID_x \oplus M'_x) \quad (9)$$

$$H_4(ID_x||M_x) = CID_x \oplus H_2(M'_x||TID'_x) \quad (10)$$

$$EID'_x = H_3(H_4(ID_x||M_x)||R_{tx}||M'_x) \quad (11)$$

After computing all these parameters, server verifies $EID'_x \stackrel{?}{=} EID_x$, failing the condition will result in termination of the session by the server S, otherwise U_x is considered a legitimate user. Now the server generates a random number $r_s \in [1, n-1]$ and determines:

$$S_{sy} = r_s.R_{tx} \quad (12)$$

$$T_{sy} = S_{sy} \oplus M_x \quad (13)$$

$$H_{sy} = H_3(EID_x||S_{sy}||TID_x). \quad (14)$$

Then server S sends $\{T_{sy}, H_{sy}\}$ to the user U_x.

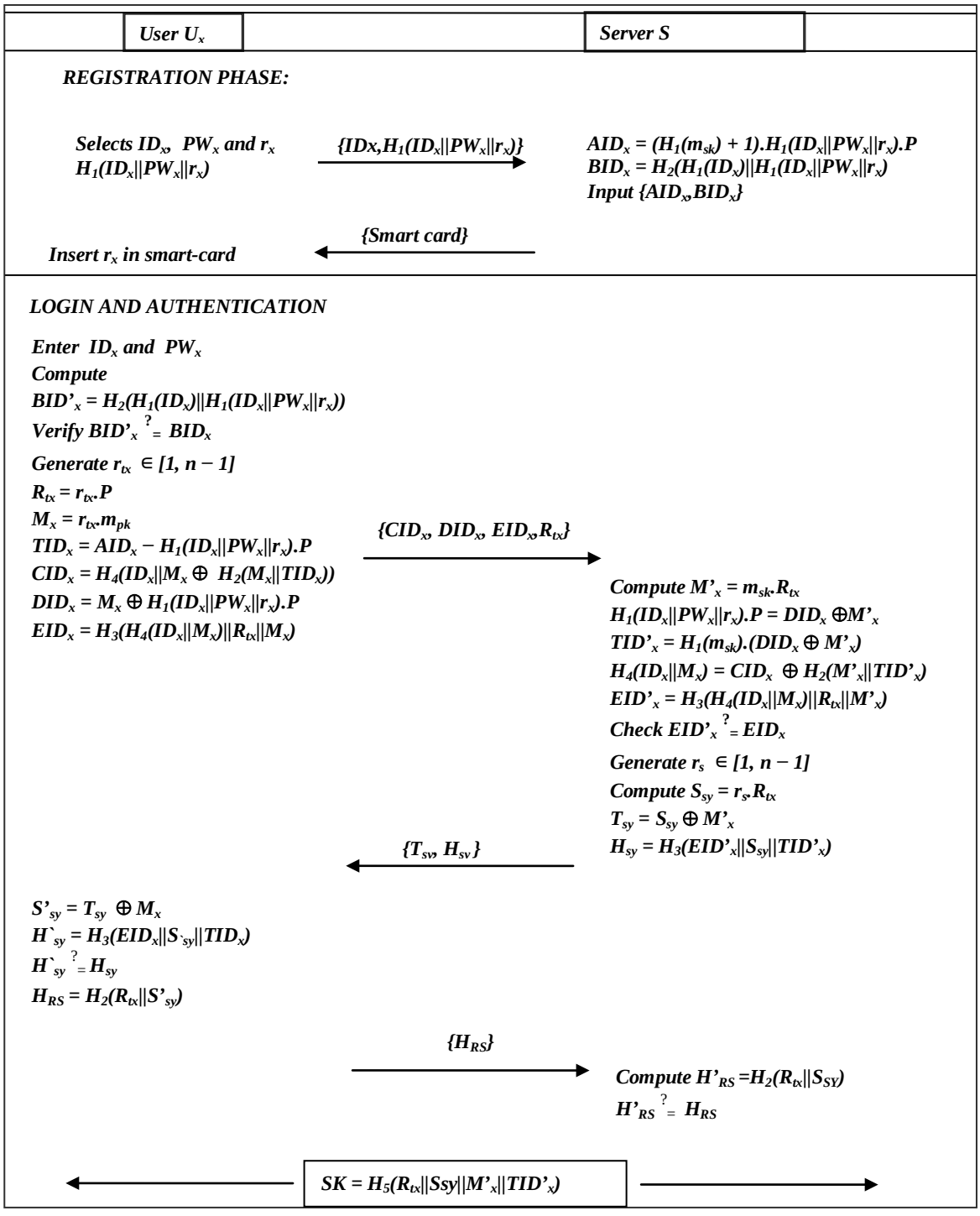

Fig. 1. Review of Huang et al. model

Step 3: The user U_x calculates:

$$S'_{sy} = T_{sy} \oplus M_x \quad (15)$$

$$H_{sy} = H_3(EID_x||S'_{sy}||TID_x) \quad (16)$$

and then checks $H_{sy} \stackrel{?}{=} H_{sy}$, failure of which terminates the session, otherwise the U_x computes $H_{RS} = H_2(R_{tx}||S'_{sy})$ and transmits H_{RS} to the server.

Step 4: In addition $H'_{RS} = H_2(R_{tx}||S_{sy})$ is computed by the server, comparing it with receiving H_{RS}. If both values are equal then the session key is computed as $SK = H_5(R_{tx}||S_{sy}||M'_x||TID'_x)$ and is shared with the User U_x. At last server S and user U_x authenticate and determine the shared session key for encryption or decryption and information exchange among the server S and user U_x.

1.4 Password Change

In case a password change is required, the user U_x must follow the subsequent steps.

1. After entering the smart-card into a reader the user must provide his/her identity ID_x as well as his/her password PW_x.
2. SC_x computes the $BID'_x = H_2(H_1(ID_x)||H_1(ID_x||PW_x||r_x))$ and verifies the BID'_x with BID_x already stored in the SC_x if it holds, the new password PW_x^{new} must be entered by the client.
3. Now the smart-card calculate the $AID_x^{new} = H_1(ID_x||PW_x||r_x)^{-1}.H_1(ID_x||PW_x^{new}||r_x)$. AID_x and $BID_x^{new} = H_2(H_1(ID_x)||H_1(ID_x||PW_x^{new}||r_x))$, the new computed AID_x^{new} and BID_x^{new} is updated with the old AID_x and BID_x respectively.

3. Cryptanalysis of Huang et al.'s Technique

This section, demonstrates that Huang et al.'s technique is insecure against user impersonation attack. Following assumptions have been adopted from [28–32] before heading forth:

1. Ą can access public communication channel and can edit, inject, intercept and delete message over it.
2. Ą can get U_x's smart-card or can predict the password of a specific user but both are not possible simultaneously.
3. Ą malicious legitimate insider may be the attacker within the organization.
4. A stolen smart-card can used to extract any information stored in it [33, 34].

3.1 Impersonation attack

This subsection describes that Huang et al.'s scheme is susceptible to impersonation attack. A legitimate user U_y can impersonate as U_x. Following are the steps executed by U_y to mislead the server:

Step 1: In a first step, U_y calculates $H_1(ID_y||PW_y||r_y)$ using his/her own smart-card and ID_y. The remote user U_y intercepts U_x's login request and computes:

$$W_y = AID_y - H_1(ID_y||PW_y||r_y).P \quad (17)$$

$$ZID_y = W_y.\ \frac{1}{H1(IDy||PWy||ry)} \quad (18)$$

$$ZID_y = H_1(m_{sk}).P \quad (19)$$

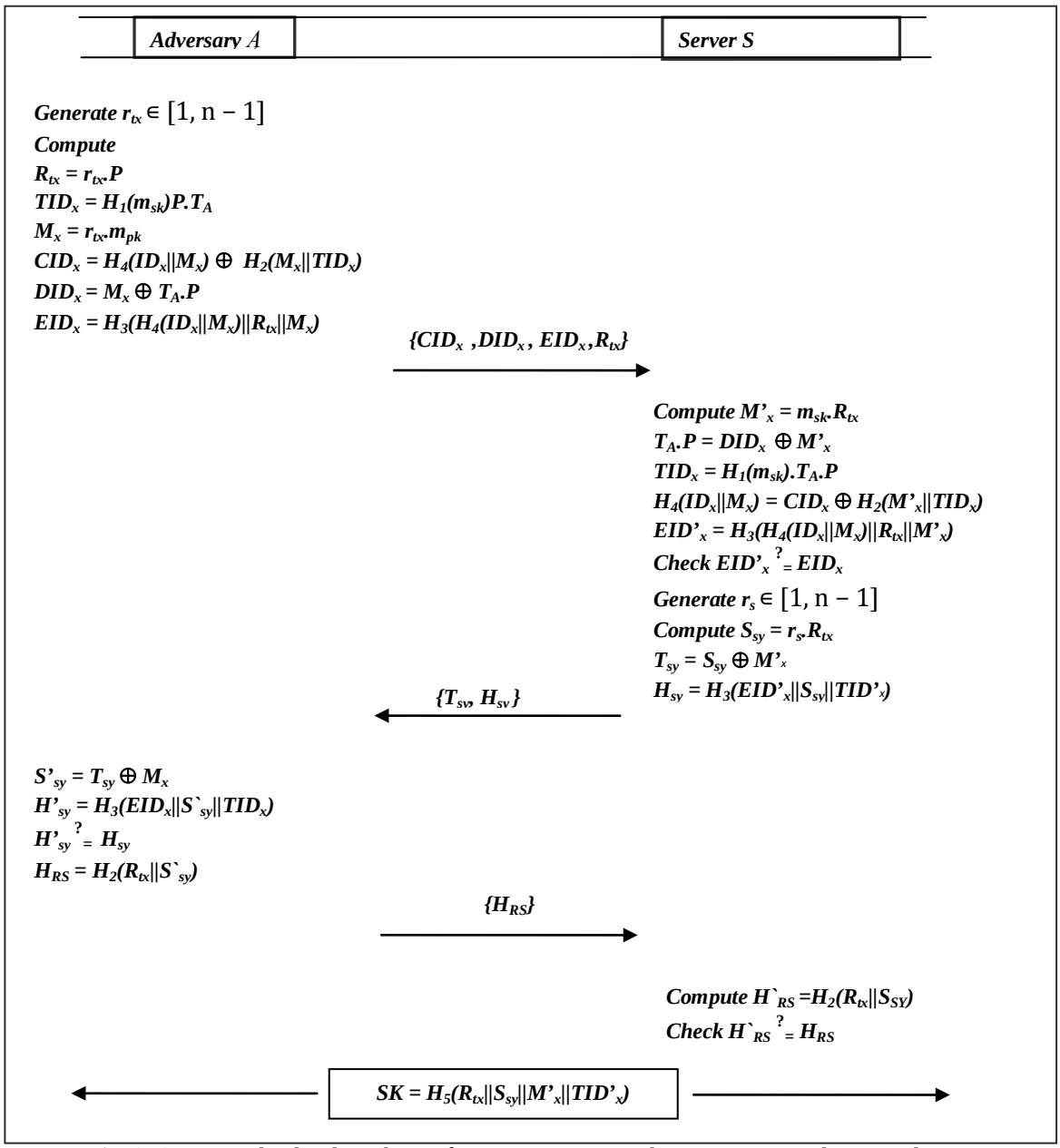

Fig. 2. Setps involved in launching of impersonation attack over Huang et al. protocol

Step 2: U_y selects a random value T_A of size 160 bits and computes:

$$\text{Generate } r_{tx} \in [1, n-1] \tag{20}$$

$$R_{tx} = r_{tx}.P \tag{21}$$

$$TID_x = H_1(m_{sk}).P.T_A \tag{22}$$

$$M_x = r_{tx}.m_{pk} \tag{23}$$

$$CID_x = H_1(ID_x||M_x) \oplus H_2(M_x||TID_x) \tag{24}$$

$$DID_x = M_x \oplus T_A.P \tag{25}$$

$$EID_x = H_3(H_4(ID_x||M_x)||R_{tx}||M_x) \tag{26}$$

Step 3: After that U_y sends $\{CID_x, DID_x, EID_x, R_{tx}\}$ to the servers.

Step 4: On receiving $\{CID_x, DID_x, EID_x, R_{tx}\}$ from U_y. The server computes:

$$M'_x = m_{sk}.R_{tx} \tag{27}$$

$$T_A.P = DID_x \oplus M'_x \tag{28}$$

$$TID_x = H_1(m_{sk}).T_A.P \tag{29}$$

$$H_4(ID_x||M_x) = CID_x \oplus H_2(M'_x||TID_x) \tag{30}$$

$$EID_x = H_3(H_4(ID_x||M'_x)||R_{tx}||M'_x) \tag{31}$$

Step 5: The server S checks $EID'_x \stackrel{?}{=} EID_x$, failure of which terminates the session, otherwise it computes the following using $r_s \in [1, n-1]$ as random number:

$$S_{sy} = r_s.R_{tx} \tag{32}$$

$$T_{sy} = S_{sy} \oplus M'_x \tag{33}$$

$$H_{sy} = H_3(EID'_x||S_{sy}||TID'_x) \tag{34}$$

Step 6: Then the server transmit the message $\{T_{sy}, H_{sy}\}$.

Step 7: On intercepting the message$\{T_{sy}, H_{sy}\}$, U_y computes:

$$S_{sy} = T_{sy} \oplus M_x \tag{35}$$

$$H_{sy} = H_3(EID_x||S'_{sy}||TID_x) \tag{36}$$

Step 8: U_y verifies $H'_{sy} \stackrel{?}{=} H_{sy}$, failure of which terminates the session, otherwise U_y calculates:

$$H_{RS} = H_2(R_{tx}||S_{sy}) \quad (37)$$

Step 9: $\{H_{RS}\}$ is sent to the server S.

Step 10: On reception of $\{H_{RS}\}$ the server S computes $H'_{RS} = H_2(R_{tx}||S_{sy})$.

Step 11: Finally, the server S checks $H'_{RS} \stackrel{?}{=} H_{RS}$, if the condition stands proving authenticity of the server, now computes shared session key $SK = H_5(R_{tx}||S_{sy}||M_x||TID_x)$. Hence, it proves that U_y has successfully impersonated U_x.

4. Proposed Scheme

The insecurity of Huang's scheme against smart-card stolen attack and user impersonation attacks was due to a generic secret value $(H_1(m_{sk})+1)$ hideously stored in a parameter $AID_x = (H_1(m_{sk}) + 1).H_1(ID_x||PW_x||r_x).P$ in each user's smart-card. A legitimate but dishonest user (say U_y) can easily extract AID_x using power analysis [33, 34] then making use of his own password and smart-card U_y can compute $H_1(m_{sk}).P$. After extracting $H_1(m_{sk}).P$, the dishonest user U_y can easily impersonate any other user. Furthermore, the U_y after stealing the smart-card of another user (say U_x) can easily impersonate himself as U_x. In proposed scheme, the smart-card contains only user specific parameters. So, even after extracting the secrets stored in one's own smart-card, he cannot impersonate himself as another user of the systems provided he has also the smart-card of the victim. The proposed scheme is robust which prevents an adversary from impersonating a legitimate user explained as follows:

4.1 System Initialization

System Initialization of the proposed scheme is identical to the one used in the Huang et al.'s scheme, where random numbers are of atleast 2^{160} bits.

4.2 The Registration

To register, U_x chooses his unique ID_x, password PW_x and random number r_x. Then hash function is applied after concatenating all the parameters followed by a registration request $\{ID_x, H_1(ID_x||PW_x||r_x)\}$ from user U_x via a secure channel to the server S. Upon getting this request the server S computes $PID_x = (H1(m_{sk}||ID_x) \oplus H_1(ID_x||PW_x||r_x))$ and $BID_x = H_2(H_1(ID_x).H_1(ID_x||PW_x||r_x))$. Now the server saves PID_x and BID_x in smart-card before passing it to the user through secured channel. The user stores r_x in the smart-card after receiving it. Hence the smart-card contains $\{PID_x, BID_x, r_x\}$ on completion of registration phase.

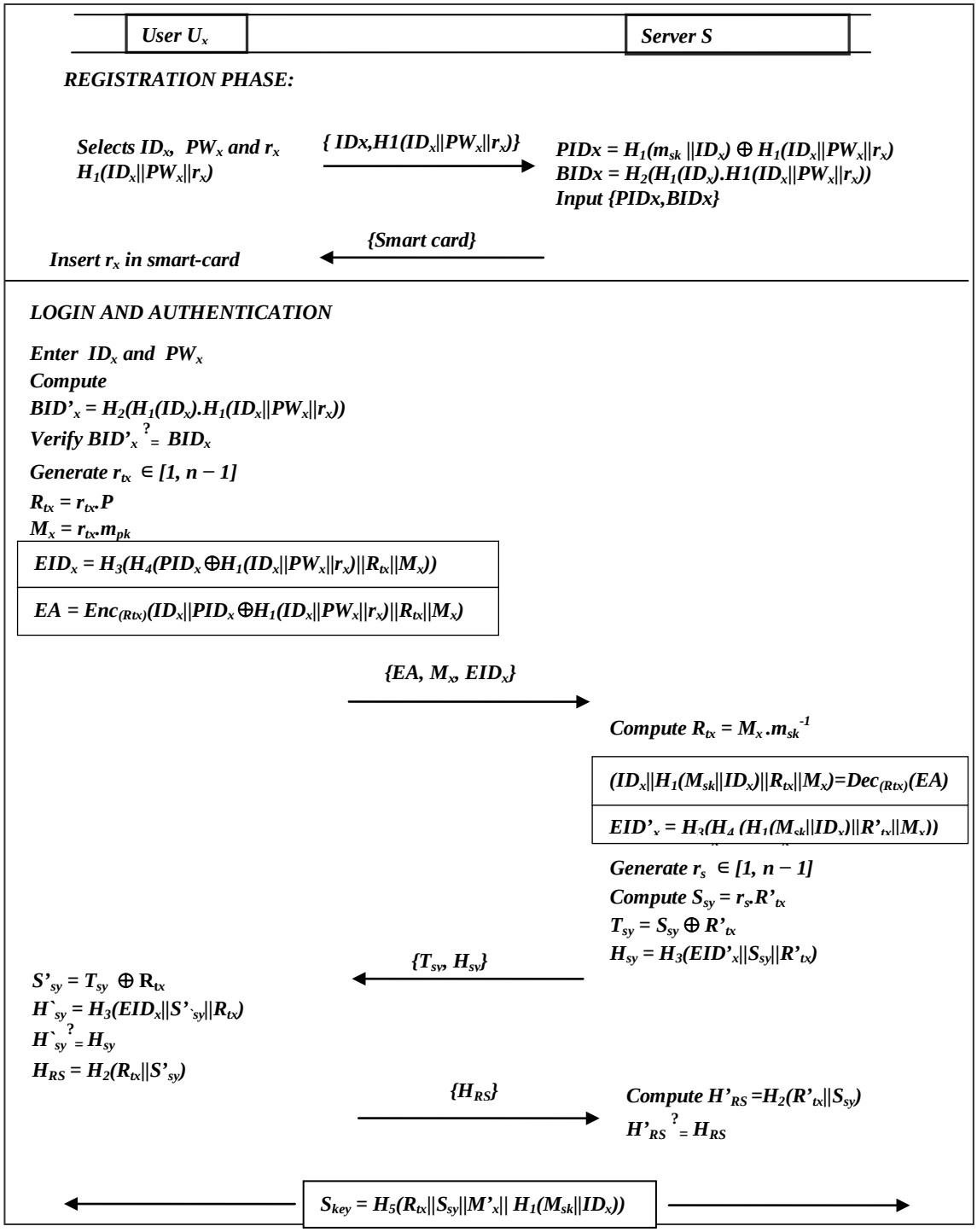

Fig. 3. Proposed Model

4.3 The Login and Authentication

To login and authenticate, a user must perform the following steps:
Step 1: User U_x attempts to login using smart-card and inputs his/her unique ID_x and Pass -word PWx. Now smart-card calculates $BID'_x = H_2(H_1(ID_x).H_1(ID_x||PW_x||r_x))$ and checks it against BID_x already in the smart-card, as $BID'_x =? BID_x$, failure of which terminates the session, otherwise, ID_x and password PW_x seems to be valid.
Step 2: In second step the smart-card picks $r_{tx} \in [1, n-1]$ and computes:

$$R_{tx} = r_{tx}.P \tag{38}$$

$$M_x = r_{tx}.m_{pk} \tag{39}$$

$$EID_x = H_3(H_4(PID_x \oplus H_1(ID_x||PW_x||r_{tx})||R_{tx}||M_x)) \tag{40}$$

$$EA = E_{nc}(R_{tx})(ID_x||PID_x \oplus H_1(ID_x||PW_x||r_{tx})||R_{tx}||M_x) \tag{41}$$

Now the user U_x tranmits the calculated values $\{EA, M_x, EID_x\}$ to the server.
Step 3: The following steps are performed by the server S after receiving the entries from the user U_x:

$$R'_{tx} = M_x \times (m_{sk})^{-1} \tag{42}$$

$$(ID_x||H_1(m_{sk}||ID_x)||R_{tx}||M_x) = D_{ec(R_{tx'})}(EA) \tag{43}$$

$$EID'_x = H_3(H_4(H_1(m_{sk}||ID_x)||R'_{tx}||M_x)) \tag{44}$$

Then server verifies $EID'_x \stackrel{?}{=} EID_x$ condition holds, if it does, U_x is considered as legal user otherwise the session is terminated. When user is assumed to be authorized, the server selects a random number r_s in $[1, n-1]$ and calculates:

$$S_{sy} = r_s.R'_{tx} \tag{45}$$

$$T_{sy} = S_{sy} \oplus R'_{tx} \tag{46}$$

$$H_{sy} = H_3(EID'_x||S_{sy}||R'_{tx}) \tag{47}$$

Now the server S conveys $\{T_{sy}, H_{sy}\}$ to the user U_x.
Step 4: The user U_x computes:

$$S'_{sy} = T_{sy} \oplus R_{tx} \tag{48}$$

$$H'_{sy} = H_3(EID_x||S'_{sy}||R_{tx}) \tag{49}$$

and checks the condition $H'_{sy} \stackrel{?}{=} H_{sy}$. The session will be terminated if the condition does not hold, else $H_{RS} = H_2(R_{tx}||S'_{sy})$ is computed and transmitted to the server S.

Step 5: Upon reception of $\{H_{RS}\}$, the server correspondingly determine $H'_{RS} = H_2(R'_{tx}||S_{sy})$ and confirms $H'_{RS} \stackrel{?}{=} H_{RS}$, failure of which terminates the session, otherwise the servers S calculate the session key as $S_{key} = H_5(R_{tx}||S_{sy}||M_x||H_1(m_{sk}||ID_x))$ and share it with the user U_x.

5. SECURITY ANALYSIS

The proposed scheme is analyzed against various security attacks in this section. The analysis reveals that the proposed protocol while communicating over public communication channel, can resists all the attacks detailed in the following subsections, reflecting high its robustness.

5.1 Security Properties

This subsection provide a brief description of various security properties and resistance ability of the proposed scheme against some known attacks.

5.1.1 Resist Replay Attack

In every session of login and registration phase, user must select a random number and compute EA,EID_x and M_x in every login and authentication section. In case, if an adversary steals the message $\{EA ,EID_x,M_x\}$, he/she fails to calculate $S_{sy} = T_{sy} \oplus R_{tx}$ without r_{tx} in login and authentication phase. The attacker correspondingly is unable to calculates $H_{RS} = H_2(R_{tx}||S'_{sy})$. Hence, the technique withstands replay attack.

5.1.2 Anonymity and Privacy

In proposed scheme, the ID_x is not independently embedded in the server repository and also in the smart-card. So, it is difficult to obtain ID_x in case of loss/stolen smart-card. A user U_x in the login and authentication phase, transmits a message containing $\{EA,M_x,EID_x\}$ to the server S making the server a soul entity to calculate EID'_x . Therefore, the proposed scheme provide anonymity.

5.1.3 Off-line Password Guessing Attack

An attacker if steals the smart-card, may gain access to the stored parameters $\{PID_x,BID_x, r_{tx}\}$. In such a case, the attacker Ą needs real identity ID_x and password PW_x of the user for launching the attack. However, ID_x and PW_x are secret to the legitimate user only, so the attacker is unable to calculate the user ID_x and PW_x from PID_x and BID_x, proving that the improved protocol withstans off-line password guessing attack.

5.1.4 Mutual Authentication

U_x sends the message $\{EA,M_x,EID_x\}$ to S in login and mutual authentication stage. On receiving the message, S computes $EID'_x = H_3(H_4(H_1(m_{sk}||ID_x)||R_{tx}||M_x))$ and checks $EID'_x = EID_x$ if the condition holds then the user U_x is considered to be the authenticated user. On the hand, the user also authenticates the server on getting the request message $\{T_{sy},H_{sy}\}$ from the server S, the user calculates the H'_{sy} and verify $H'_{sy} = H_{sy}$ if true then the user U_x successfully authenticate the server S. So, the proposed scheme maintains mutual authentication.

5.1.5 Resist Smart-Card Stolen Attack

In case of a stolen/lost smart-card, an attakcer U'_x can get the smart-card to access the stored parameters $\{BID_x, PID_x, r_{tx}\}$ from it. The adversary is unable to obtain the ID_x and PW_x from the $BID_x = H_2(H_1(ID_x).H_1(ID_x||PW_x||r_x))$, $PID_x = H1(m_{sk}||ID_x) \oplus H_1(ID_x||PW_x||r_x)$ performing

the off-line password guessing attack. Normally a successful and instantaneous prediction of the U_x's identity ID_x and password PW_x for an attacker is infeasible. Hence, the proposed technique resists the loss/stolen smart-card attack.

5.1.6 Perfect Forward Secrecy

During authentication, two random number (r_{tx}, r_s) are generated by the user and server respectively . Further, these two numbers are also involved for computation of session key. Therefore, even if private key of the server S as well as password of user U_x are exposed, generating the keys used in previous sessions is not possible for the attacker. Hence, the proposed technique provides forward secrecy.

5.1.7 Resist Impersonation Attack

For impersonating U'_x, an attacker must have to obtain ID_x and password PW_x concurrently to calculate EA, M_x, EID_x. Moreover, in order to get identity ID_x and password PW_x the attacker has to attack the protocol with offline password guessing. However, as discussed earlier in subsection 5.1.3, offline password guessing attack is not possible on the proposed protocol, therefore, launching impersonation will fail.

5.1.8 Resist Insider Attack

This scheme does not maintain any database to store identities and passwords of users therefore, it can be concluded that this scheme is robust against insider attacker.

5.1.9 No Key Control

To calculating $S_{key} = H_5(R_{tx}||S_{sy}||M_x||H_1(m_{sk}||ID_x))$ as the session key, a user U_x and the server S have to compute both R_{tx} and S_{sy}. Server alone cannot compute a session key, rather both User U_x and server S must compute the session simultaneously. Showing that the proposed protocol has no key control.

5.1.10 Resist Server Spoofing Attack

In case when an adversary pretends to be a ligetimate server and communicates with a user, the adversary has to imitate $H_{sy} = H_3(EID'_x||S_{sy}||R'_{tx})$ message to transmit the user in login and authentication phase. Without R_{tx} and S_{sy} attacker is not able to calculate the S_{key} and H_{sy}. Therefore, the protocol proposed in this article impervious to server spoofing attack.

5.2 Formal Security Analysis

To analyzed that the proposed protocol is provably secure, models used in [33, 34] are adapted. For analysis purpose, the following oracles are defined:

– ***Reveal 1:*** This oracle results an input 'x' out of one hash function Y = h(x).

– ***Reveal 2:*** Result of this oracle is the plain text p from cipher text $C = E_k(p)$ without the knowledge of shared symmetric key k.

– ***Reveal 3***: The result here is the scalar multiplier a, from an Elliptic curve's point a.P.

Theorem 1 *The proposed untraceable authentication using ECC technique for authenticating a remote user PUECCUA is protected against an adversary $\mathcal{A}$ for extraction of user U_x's identity ID_x, the server private key m_{sk} , user password PW_x and the session key S_{key} shared by a user U_x and the server S, assuming hash function and symmetric encryption as a random oracle which computationally hard to calculate due to the hardness of ECDLP(discrete logarithmic problem).*

Proof 1 *The proof consists of an imaginary attacker Ą who can extract ID_x, PW_x of user U_x. Similarly, m_{sk} is also known to Ą, which used as session key $S_{key,}$ by the server S. For verification of the proof, the experiment $EXP1_{A,PUECCUA}^{HASH,ECDLP,SYMENC}$ has been simulated to verify untraceability of the proposed protocol in case of authenticating a remote user using ECC by considering the random oracles Reveal1, Reveal2 and Reveal 3. Probability of success of the experiment is defined as* $Succ1 = [Prob[EXP1_{A,PUECCUA}^{HASH,ECDLP,SYMENC} = 1] - 1]$. *Advantage of the adversary Ą is solicited as* $Adt1_{A,PUECCUA}^{HASH,ECDLP}(Texe, qrv1, qrv2, qrv3) = maximum\ A\ (Succ1)$. *For the mentioned experiment Ą is allowed to mark qrv_1, qrv_2 and qrv_3 Reveal1, Reveal2 and Reveal3 queries respectively in polynomial time texe. This experiment may successfully break security of the proposed protocol. if it can (i) extract a plain text out of cipher text without having the shared key, (ii) using one-way hash function to extract the input string, and (iii) break ECDLP. However, achieving requirement (i) and (ii) are computationally impractical.*

Similarly breaking ECDLP is also computationally impractical since it is based on Discrete Logrithmic Problem. Therefore, the Ą's advantage is as follows: $Adt1_{A,PUECCUA}^{HASH,ECDLP,SYMENC}(texe, qrv1, qrv2, qrv3) \leq \mathcal{E}$. *Hence it can be concluded that the improved scheme is secure to an attacker Ą to extract ID_x, PW_x, m_{sk} and S_{key}.*

Algorithm 1. ***Algorithm*** $EXP1_{A,PUECCUA}^{HASH,ECDLP,SYMENC}$

1. Eavesdrop the request message (EA, M_x, EID_x), Where $EA = Enc(R_{tx)}(ID_x||PID_x \oplus H_1(ID_x||PW_x||r_x)||R_{tx}||M_x)$,$M_x = r_{tx}.m_{pk}$, $EID_x = H_3(H_4(PID_x \oplus H_1(ID_x||PW_x||r_x)||R_{tx}||M_x))$
2. Call Reveal 1 on EID_x to obtain $H_4(PID_x \oplus H_1(ID_x||PW_x||r_x)||R_{tx}||M_x)$ Reveal1 EID_x
3. Call Reveal 1 on $H_4(PID_x \oplus H_1(ID_x||PW_x||r_x)||R_{tx}||M_x)$ and get $(PID_x \oplus H_1(ID_x||PW_x||r_x)||R_{tx}||M_x))$ Reveal1$(PID_x \oplus H_1(ID_x||PW_x||r_x)||R_{tx}||M_x)$'.
4. Call Reveal 1 on $H_1(ID_x||PW_x||r_x)$ to obtain $(ID_x||PW_x||r_x)$'' Reveal 1$(ID_x||PW_x||r_x)$'.
5. Call Reveal 2 on EA to obtain $(ID_x||(PID_x \oplus H_1(ID_x||PW_x||r_x)||R_{tx}||M_x))$ Reveal 2 $(Enc_{(Rtx)})$ and get $ID'_x||(PID_x \oplus H_1(ID_x||PW_x||r_x)''||R''_{tx}||M''_x)$
6. If $(PID_x \oplus H_1(ID_x||PW_x||r_x)' = (PID_x \oplus H_1(ID_x||PW_x||r_x)'' = H_1(m'_{sk}||ID_x)$ then
7. Then if $R'_{tx} = R''_{tx}$
8. Then if $M'_x = M''_x$
9. Accept ID'_x
10. Call Reveal on $PID_x \oplus H_1(ID_x||PW_x||r_x)$ and obtain $(m'_{sk}||ID''_x)$
11. If $ID'_x = ID''_x$ Then
12. Accept m_{sk} as private key of server.
13. Compute $r'_{tx}.P = M'_x.msk^{-1}$
14. If $R''_{tx} = r'_{tx}.P$ Then
15. Call Reveal 3 on R''_{tx} and get r'_{tx} Reveal3.(R''_{tx})
16. Eavesdrop the challenge message (H_{sy}, T_{sy})
17. Compute $S'_{sy} = T_{sy} \oplus R''_{tx}$
18. $H'_{sy} = H_3(EID_x||S_{sy}||R'_{,tx})$
19. If then($H'_{sy} = H_{sy}$)
20. Accept r'_{tx}
21. Else
22. Call Reveal on
23. End If

24. Else
25. Return Fail
26. End If
27. Else
28. Return Fail
29. End If
30. End If

6. COMPARISON AND PERFORMANCE ANALYSIS

The proposed protocol is evaluated against the existing protocols in terms of security and performance in this section. The proposed protocol is compared against its most relevant counterparts including Huang et al.'s [27], Qu et al.'s [19], Yang et al.'s [8] and Islam et al.'s [35] schemes. Performance is evaluated using running time (computation cost), communication cost whereas security is gauged in terms of resistance against different attacks as shown in **Table 2**. In the computation of computation cost, only significant operations are considered such as multiplication operation of ECC, addition/subtraction operation of ECC, hash operation and map to point operation. Trivial operations such as concatenation and XOR are overlooked. From **Table 2**, it can be analyzed that the proposed protocol is cost efficient in comparison to the other existing protocols.

Various notations used in performance comparison:

– T_{owh} : hash function computation time
– T_{pm} : point multiplication computation time
– T_{pa} : time to calculate point addition operations
– T_{mtp} : time to calculate map to point operation
– T_{Es} : time taken by symmetric encryption/decryption

According to an analysis in Kilinc and Yanik [36], the computation times for T_{owh}, T_{pm}, T_{pa}, T_{mtp} and T_{Es} are 0.0023 ms, 2.226 ms, .0288 ms, 0.947 ms and 0.0046 ms respectively. Comparison of the proposed protocol with the existing protocols in terms of communication cost is shown in **Table 3**.

Table 2. Computation Cost Analysis for cryptographic schemes

Schemes	User	Server	Total	Running Time
Huang et al. [27]	9*Towh*+3*Tpm*+1*Tpa*	6*Towh* +2*Tpm*	15*Towh* + 5*Tpm* + 1*Tpa*	≈ 11.1933
Qu et al. [19]	8*Towh* + 6*Tpm* + 3*Tpa*	5*Towh* + 3*Tpm* + 2*Tpa*	13*Towh* + 9*Tpm* + 5*Tpa*	≈ 20.2079
Yang et al. [8]	4*Towh* + 4*Tpm* + 2*Tpa* + 1*Tmtp*	3*Towh* + 4*Tpm* + 2*Tpa* + 1*Tmtp*	7*Towh* + 8*Tpm* + 4*Tpa* + 2*Tmtp*	≈ 17.9849
Islam et al. [35]	3*Towh* + 4*Tpm* + 2*Tpa* + 1*Tmtp*	3*Towh* + 4*Tpm* + 2*Tpa* + 1*Tmtp*	6*Towh* + 8*Tpm* + 4*Tpa* + 2*Tmtp*	≈ 17.9622
Proposed	7*Towh* + 1T_{Es} + 2*Tpm*	6*Towh* + 1T_{Es} + 2*Tpm*	13*Towh* + 2T_{Es} + 4*Tpm*	≈ 8 .9431

Table 3. Communication Cost Analysis for various cryptographic schemes

Schemes	Proposed	[27]	[19]	[8]	[35]
Communication Overhead(Bits)	960	1120	992	864	864
Exchanged Messages	3	3	3	2	2

Table 4 presents a security comparison analysis of the proposed protocol with its counterparts i.e. Huang et al.'s [27], Qu et al.'s [19], Yang et al.'s [8] and Islam et al.'s [35] protocols. An overall analysis of the table shows that the proposed protocol out-performs the existing protocols in terms of achieving high security, mutual authentication and resists impersonation attack.

Table 4. Security Parameters Comparison for various cryptographic schemes

Scheme:	Proposed	[27]	[19]	[8]	[35]
Resist Replay Attack	√	√	√	x	√
Anonymity and Privacy	√	√	x	x	√
Off-Line Password Guessing Attack	√	√	x	-	-
Mutual Authentication	√	x	√	√	√
Resist Smart-Card Stolen Attack	√	√	x	-	-
Perfect Forward Secrecy	√	√	√	√	√
Resist Impersonation Attack	√	x	√	√	√
Resist insider attack	√	√	√	√	√
No Key Control	√	√	√	x	x
Resist server spoofing Attack	√	√	√	√	√

Yes=√, No= x , N/A= -

7. Conclusion

A cryptanalysis of Huang et al.'s showing that it cannot resists user impersonation attack has been presented. Moreover, to over this weakness, an improved and untraceable protocol for remote user authentication has been proposed in this paper. Random oracle model is used to evaluate security of the improved protocol showing that it provides more security while reducing the overall computation cost in comparison to Huang et al.'s as well as other related schemes.

8. Acknowledgments

This Research work funded by International Researcher Exchange project of National Science Foundation of china, Centre national de la recherche scientifique de France (NSFC-CNRS) under Grant no, 61211130104 and National Science Foundation of China Grant no. 61271220.

References

[1] Lamport L., "Password authentication with insecure communication," *Communications of the ACM*, 24(11):770–772, 1981. Article (CrossRef Link)

[2] Peyravian M, Zunic N., "Methods for protecting password transmission. Computers & Security, 19(5):466–469, 2000. Article (CrossRef Link)

[3] Lin CL, Hwang T., "A password authentication scheme with secure password updating," *Computers & Security*, 22(1):68–72, 2003. Article (CrossRef Link)

[4] Yoon, Eun-Jun, et al., "A secure and efficient SIP authentication scheme for converged VoIP networks," *Computer Communications*, 33.14, 1674-1681, 2010. Article (CrossRef Link)

[5] Nikooghadam, Morteza, Reza Jahantigh, and Hamed Arshad, "A lightweight authentication and key agreement protocol preserving user anonymity," *Multimedia Tools and Applications*, 1-23, 2016. Article (CrossRef Link)

[6] Arshad, Hamed, and Morteza Nikooghadam, "An efficient and secure authentication and key agreement scheme for session initiation protocol using ECC," *Multimedia Tools and Applications*, 75.1, 181-197, 2016. Article (CrossRef Link)

[7] Juang WS, Chen ST, Liaw HT., "Robust and efficient password-authenticated key agreement using smart cards," *Industrial Electronics*, IEEE Transactions on, 55(6):2551–2556, 2008.

[8] Yang G, Wong DS, Wang H, Deng X., "Two-factor mutual authentication based on smart cards and passwords," *Journal of Computer and System Sciences*, 74(7):1160–1172, 2008. Article (CrossRef Link)

[9] Kumari, S., Karuppiah, M., Li, X., Wu, F., Das, A. K., and Odelu, V., "An enhanced and secure trust-extended authentication mechanism for vehicular ad-hoc networks," *Security Comm. Networks*, 9: 4255–4271, 2016. Article (CrossRef Link)

[10] Xu J, Zhu WT, Feng DG., "An improved smart card based password authentication scheme with provable security," *Computer Standards & Interfaces*, 31(4):723–728, 2009. Article (CrossRef Link)

[11] Saru Kumari, Xiong Li, Fan Wu, Ashok Kumar Das, Hamed Arshad, Muhammad Khurram Khan, "A user friendly mutual authentication and key agreement scheme for wireless sensor networks using chaotic maps," *Future Generation Computer Systems*, Volume 63, Pages 56-75, ISSN 0167-739X, October 2016. Article (CrossRef Link)

[12] Arshad, Hamed, and Morteza Nikooghadam, "Security analysis and improvement of two authentication and key agreement schemes for session initiation protocol," *The Journal of Supercomputing*, 71.8, 3163-3180, 2015. Article (CrossRef Link)

[13] Kumari, Saru, Muhammad Khurram Khan, and Xiong Li, "An improved remote user authentication scheme with key agreement," *Computers & Electrical Engineering*, 40.6, 2014. Article (CrossRef Link)

[14] Mir, Omid, and Morteza Nikooghadam, "A secure biometrics based authentication with key agreement scheme in telemedicine networks for e-health services," *Wireless Personal Communications*, 83.4, 2439-2461, 2015. Article (CrossRef Link)

[15] Kumari, S., Das, A. K., Wazid, M., Li, X., Wu, F., Choo, K.-K. R., and Khan, M. K., "On the design of a secure user authentication and key agreement scheme for wireless sensor networks," *Concurrency Computat.: Pract. Exper.* Article (CrossRef Link)

[16] He D, Kumar N, Chilamkurti N., "A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks," *Information Sciences*, 2015. Article (CrossRef Link)

[17] Kumari, S., Chaudhry, S.A., Wu, F., Farash, M.S., Khan, M.K., "An improved smart card based authentication scheme for session initiation protocol, Peer-to-Peer Netw," Appl., 2015. Article (CrossRef Link)

[18] Chaudhry, S. A., Khan, I., Irshad, A., Ashraf, M. U., Khan, M. K., and Ahmad, H. F., "A provably secure anonymous authentication scheme for Session Initiation Protocol," *Security Comm. Networks*, 2016. Article (CrossRef Link)

[19] Khalid Mahmood, Shehzad Ashraf Chaudhry, Husnain Naqvi, Taeshik Shon, Hafiz Farooq Ahmad, "A lightweight message authentication scheme for Smart Grid communications in power sector," *Computers & Electrical Engineering*, Volume 52, Pages 114-124, ISSN 0045-7906, May 2016. Article (CrossRef Link)
[20] Qu J, Tan XL., "Two-factor user authentication with key agreement scheme based on elliptic curve cryptosystem," *Journal of Electrical and Computer Engineering 2014*, 2014. Article (CrossRef Link)
[21] Chaudhry, S.A., Naqvi, H., Mahmood, K. Ahmad, H.F., Khan, M.K., An Improved Remote User Authentication Scheme Using Elliptic Curve Cryptography Wireless Pers Commun, 2016. Article (CrossRef Link)
[22] Lee SW, Kim HS, Yoo KY., "Improvement of chien et al.'s remote user authentication scheme using smart cards," *Computer Standards & Interfaces*, 27(2):181–183, 2005. Article (CrossRef Link)
[23] Lee NY, Chiu YC., "Improved remote authentication scheme with smart card," *Computer Standards & Interfaces*, 27(2):177–180, 2005. Article (CrossRef Link)
[24] Sood SK, Sarje AK, Singh K., "An improvement of xu et al.'s authentication scheme using smart cards," in *Proc. of the third annual ACM Bangalore conference*, ACM, 15, 2010. Article (CrossRef Link)
[25] Song R., "Advanced smart card based password authentication protocol," *Computer Standards & Interfaces*, 32(5):321–325, 2010. Article (CrossRef Link)
[26] Chen BL, KuoWC,Wuu LC., "Robust smart-card-based remote user password authentication scheme," *International Journal of Communication Systems*, 27(2):377–389, 2014. Article (CrossRef Link)
[27] Jiang Q, Ma J, Li G, Ma Z., "An improved password-based remote user authentication protocol without smart cards," *Information technology And control*, 42(2):113–123, 2013. Article (CrossRef Link)
[28] Huang B, Khan MK, Wu L, Muhaya FTB, He D., "An efficient remote user authentication with key agreement scheme using elliptic curve cryptography," *Wireless Personal Communications*, 1–16, 2015. Article (CrossRef Link)
[29] Cao X, Zhong S., "Breaking a remote user authentication scheme for multi-server architecture," *IEEE Communications Letters*, 10(8):580–581, 2006. Article (CrossRef Link)
[30] Eisenbarth T, Kasper T, Moradi A, Paar C, Salmasizadeh M, Shalmani MTM., "On the power of power analysis in the real world: A complete break of the keeloq code hopping scheme," *Advances in Cryptology–CRYPTO*, Springer, 203–220, 2008.
[31] Dolev D, Yao AC, "On the security of public key protocols," *Information Theory, IEEE Transactions on*, 29(2):198–208, 1983. Article (CrossRef Link)
[32] Chaudhry SA, Naqvi H, Farash MS, Shon T, Sher M., "An improved and robust biometricsbased three factor authentication scheme for multiserver environments," *The Journal of Supercomputing* 1–17, 2015. Article (CrossRef Link)
[33] Chaudhry SA., "A secure biometric based multi-server authentication scheme for social multimedia networks," *Multimedia Tools and Applications*, 1–21, 2015. Article (CrossRef Link)
[34] Kocher P, Jaffe J, Jun B., "Differential power analysis," *Advances in CryptologyUCRYPTOŠ99*, Springer, 388–397, 1999.
[35] Messerges TS, Dabbish E, Sloan RH, et al., "Examining smart-card security under the threat of power analysis attacks," *Computers, IEEE Transactions on*, 51(5):541–552, 2002. Article (CrossRef Link)
[36] Islam SH, Biswas G., "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, 2011. Article (CrossRef Link)
[37] Kilinc HH, Yanik T., "A survey of sip authentication and key agreement schemes," *Communications Surveys & Tutorials, IEEE*, 16(2):1005–1023, 2014. Article (CrossRef Link)

[38] Chaudhry, S. A., Farash, M. S., Naqvi, H., Kumari, S., and Khan, M. K., "An enhanced privacy preserving remote user authentication scheme with provable security," *Security Comm. Networks*, 8: 3782–3795, 2015. Article (CrossRef Link)

Zahid Mehmood received his MS Computer Science from International Islamic University Islamabad, Pakistan in 2010. He is currently a Ph.D candidate in Shanghai JiaoTong University, Shanghai. His research interests include Elliptic Curve Cryptography, SIP authentication, Security of Internet of Things, authentication protocols specifically based on lightweight cryptosystems.

Gongliang CHEN received MS Mathematics from Institute of Applied Mathematics, Academy of Sciences of China, in 1986, his Ph.D Mathematics from University de Saint-Etienne, France 1993. He is currently Professor / Doctoral supervisor, School of Electronic Information and Electrical Engineering (SEIEE) / School of Information Security Engineering (SISE), SJTU-ParisTech Elite Institute of Technology, Shanghai Jiaotong university (SJTU). Visiting Fellow / Doctoral supervisor (Institute of Information Engineering, Chinese Academy of Sciences, IIECAS). His research interests include Network Security, Information security, Security of RFID, Lightweight cryptology, Cryptography Technology and its application.

Jianhua Li received MS and Ph.D Electronic information from Shanghai Jiaotong University, in 1998. He is currently Professor / Doctoral supervisor, School of Electronic Information and Electrical Engineering (SEIEE) / School of Information Security Engineering (SISE), Shanghai Jiaotong University His research interests include Network Security, Information security.

Aiid Albeshri received M.S. and Ph.D. degrees in Information Technology from Queensland University of Technology, Brisbane, Australia in 2007 and 2013 respectively. He has been an assistant professor at the Computer Science Department of the King Abdulaziz University, Jeddah, Saudi Arabia since 2013. His current research focuses on Security and Trust in Cloud computing and big data.