An Improved Lightweight Two-Factor Authentication and Key Agreement Protocol with Dynamic Identity Based on Elliptic Curve Cryptography

Shuming Qiu[1,2,*], Guosheng Xu[2], Haseeb Ahmad[3], Guoai Xu[2], Xinping Qiu[4] and Hong Xu[5]

[1]Elementary Educational College, Jiangxi Normal University
Nanchang 330022, China
[e-mail: qiushuming2008@163.com]
[2]School of CyberSpace Security, Beijing University of Posts and Telecommunications
Beijing 100876, China
[3] Department of Computer Science, National Textile University
Faisalabad 37610, Pakistan
[4]Jiangxi University of Finance and Economics, Nanchang 330013, China
[5]High-Tech Research and Development Center, the Ministry of Science and Technology
Beijing 100044, China
*Corresponding author: Shuming Qiu

Received April 10, 2018; revised July 24, 2018; revised August 23, 2018; accepted September 5, 2018; published February 28, 2019

Abstract

With the rapid development of the Internet of Things, the problem of privacy protection has been paid great attention. Recently, Nikooghadam et al. pointed out that Kumari et al.'s protocol can neither resist off-line guessing attack nor preserve user anonymity. Moreover, the authors also proposed an authentication supportive session initial protocol, claiming to resist various vulnerability attacks. Unfortunately, this paper proves that the authentication protocols of Kumari et al. and Nikooghadam et al. have neither the ability to preserve perfect forward secrecy nor the ability to resist key-compromise impersonation attack. In order to remedy such flaws in their protocols, we design a lightweight authentication protocol using elliptic curve cryptography. By way of informal security analysis, it is shown that the proposed protocol can both resist a variety of attacks and provide more security. Afterward, it is also proved that the protocol is resistant against active and passive attacks under Dolev-Yao model by means of Burrows-Abadi-Needham logic (BAN-Logic), and fulfills mutual authentication using Automated Validation of Internet Security Protocols and Applications (AVISPA) software. Subsequently, we compare the protocol with the related scheme in terms of computational complexity and security. The comparative analytics witness that the proposed protocol is more suitable for practical application scenarios.

Keywords: Elliptic curve cryptography, Two-factor, Authentication, AVISPA, BAN-Logic

http://doi.org/10.3837/tiis.2019.02.027 **ISSN : 1976-7277**

1. Introduction

With the growing applications of cloud computing and multimedia services, the issue of communication privacy protection has gained more attention. To solve the privacy problem, numerous authentication and key agreement protocols are presented [1-20]. In order to login the server, the users execute the authentication process through session initial protocol (SIP). More precisely, SIP is a communication protocol that signals and controlls multimedia communication sessions in practical applications, such as telecare medical information systems, distributed cloud computing environment, and internet telephony etc. Authentication and key agreement is a vital part of SIP. After the first authentication protocol was presented by Franks et al. in 1999 [21], many researchers analyzed and designed a lot of authentication and key agreement protocols based on the work of Franks et al. However, most of these schemes have at least one security vulnerability, such as perfect forward secrecy and off-line password guessing attack, etc [22-25].

1.1 Related Work

Recently, Chang et al. [26] observed that Wang et al.'s protocol [27] is unable to resist impersonation attack and provides user-untraceability because the identity is transmitted in login request message. Moreover, Chang et al. [26] also pointed out that password changing phase has no verification step in Wang et al's protocol [27]. Implying that the legitimate user will not be able to access the remote server anymore. In order to solve these problems, Chang et al. [26] presented a dynamic-identity based remote user authentication scheme while only incorporating hash function without session key agreement. In 2014, Kumari et al. [28] revealed that Chang et al. [26] protocol cannot resist off-line password guessing attack, impersonation attacks, etc. Further, Chang et al. [26] protocol also faces denial of service and cannot provide session key. For eliminating these vulnerabilities in Chang et al. protocol [26], Kumari et al. [28] also designed an authentication protocol. However, Chaudhry et al.[29] identified that Kumari et al.'s protocol [28] is still vulnerable against smart card stolen attack and cannot provide user anonymity in 2015. Subsequently, Chaudhry et al. [29] proposed an improved remote user authentication scheme with privacy preserving to remedy those flaws of Kumari et al.'s protocol [28]. But in 2016, Nikooghadam et al. [30] proved that Kumari et al. [28]'s and Chaudhry et al. [29]'s protocols are unable to resist offline-password-guessing attacks. Afterward, Nikooghadam et al. [30] designed a new authentication protocol and asserted that their protocol can both resist various attacks and provide user-anonymity. But, we remark that Nikooghadam et al.'s protocol [30] also has some flaws including perfect forward secrecy and off-line password guessing attack, etc. In fact, in throughout aforementioned protocols, the authors only used one-way hash function to provide security. Moreover, there exist several defects in the designs of authentication protocols. Under these circumstances, it is impossible to preserve perfect-forward-secrecy and avoid some known attacks, such as impersonation attacks and off-line password guessing attack, etc. In order to establish secure shared key in an authentication scheme, public key cryptography, which can efficiently provide perfect-forward-secrecy and resist various known attacks according to [47-52], is considered as the first choice including elliptic curve cryptography (ECC), RSA, etc. Because, the elliptic curve cryptography is more efficient than RSA under the same security condition, therefore, it is widely used in many special scenarios, especially for resource-constrained devices.

1.2 Contributions and Organization

In order to fill the aforementioned gaps, we present an improved authentication protocol with a full security function. The contributions of this paper are following:

(1) We present a supplementary cryptanalysis of Kumari et al.'s protocol and point out that it is still vulnerable to key-compromise impersonation attack and is unable to provide perfect-forward-secrecy. Moreover, we also remark that Nikooghadam et al.'s protocol is unable to provide perfect forward secrecy and is also vulnerable to off-line password guessing attack and key-compromise impersonation attack.

(2) We establish a novel lightweight authentication protocol for SIP using ECC.

(3) By heuristic security analysis, we illustrate that the proposed protocol is immune to all known attacks. Moreover, the proposed protocol can provide more comprehensive security functions including perfect forward secrecy, dynamic identity, and anonymity, etc.

(4) Via AVISPA software simulation verification, we show that the improved protocol is SAFE against active and passive attacks including replay and man-in-the-middle attacks under the Dolev-Yao model[31].

(5) According to BAN-Logic proof, we show that user and server can mutual authenticate successfully each other in the improved protocol.

(6) Comparing with the relevant solutions, we remark that our protocol is more secure and suitable for application in the actual scene.

The rest of this paper is organized as follows: attacker model and intractable problems are listed in Section 2. The protocol of Kumari et al. and its cryptanalysis is explained in Section 3. The protocol of Nikooghadam et al. and its cryptanalysis is provided in Section 4. The proposed scheme is presented in Section 5. The heuristic security analysis, simulation and security proof through AVISPA software and BAN-Logic are presented in Sections 6, 7 and 8, respectively. Security and performance comparisons are depicted in Section 9. Finally, the conclusion is summarised in Section 10.

2. Preliminaries

In this section, we introduce the capacities of the adversary of the authentication protocol. Some notations used in this paper are listed in **Table 1**.

2.1 Attacker model

According to [32–35], throughout this paper, we summarize the capacities of the attacker $\mathcal{A}$ suitable for the whole paper as follows:

(1) According to [33,34], if $\mathcal{A}$ steals the smart card of user or is in the effective range of the smart card being attacked, $\mathcal{A}$ may have the ability to obtain all datum stored in smart card by using the power-analysis technology.

(2) In open channels, all datum transmitted on these channels are public. So $\mathcal{A}$ has the capacity to eavesdrop, delete, modify, insert, replay, and block these messages on pubic channels.

(3) According to [32,35], $\mathcal{A}$ can have the ability to guess identity and password simultaneously in polynomial time. Thus, $\mathcal{A}$ can traverse all pairs of identity and password in dictionary space with in polynomial time.

(4) According to [32,35], $\mathcal{A}$ can either steal password or get all datum from user's smart card, but not both. If they are compromised by $\mathcal{A}$ simultaneously, then any two-factor authentication protocol is insecure.

(5) When perfect forward secrecy [32,35] and key-compromise user impersonation attack are discussed, the long-term private key of the server can be leaked to $\mathcal{A}$. Since perfect forward security is the ultimate security, and key-compromise user impersonation attack is the ultimate attack, if an authentication protocol can both provide forward security and resist key-compromise user impersonation attack, it will be a better protocol. When assessing any attack, key-compromise user impersonation attack in particular, it is assumed that any adversary cannot get the verifiers and the private key of server simultaneously.

2.2 Intractable problems over ECC

Generally, let p be a secure prime number and F_p be a finite field, the elliptic curve equation in ECC is defined in the following form:

$E_p(a,b): y^2 = x^3 + ax + b \ (mod\ p)$ over F_p with $4a^3 + 27b \neq 0 \ (mod\ p)$.

Where $a, b \in F_p$.

- **Elliptic curve discrete logarithm problem (ECDLP):** Let P is a generator of $E_p(a,b)$ and $Q = xP$, where $x \in_R F_p$, it is almost impossible for $\mathcal{A}^{\text{PPT}}$ (probabilistic polynomial time adversary) to figure out the random number x satisfying $Q = xP$.
- **Elliptic curve computational Diffie-Hellman problem (ECCDHP):** Let $x_1P, x_2P \in E_p(a,b)$, it is almost impossible for $\mathcal{A}^{\text{PPT}}$ to figure out $(x_1x_2)P$.

Table 1. Notations

Notations	Description
U_i	User
S	Server
Id_i	Identity of user U_i
Pw_i	Password of user U_i
x	Private key of server S
$E_p(a,b)$	Elliptic curve over a finite field
P	A generator of $E_p(a,b)$
$E_k(\cdot)$ / $D_k(\cdot)$	The private encryption/decryption with the key k
$\|\|$	Concatenation operation
$\oplus$	Exclusive-OR operation
$H(\cdot)$	Hash function
SK	The session key between U_i and S
$\Longrightarrow$ $\Longleftarrow$	Secure channel
$\longrightarrow$	Insecure/Open channel
$\mathcal{A}$	Adversary/ malicious attacker

3. A Brief Review and Supplementary Cryptanalysis of Kumari et al.'s Protocol

3.1 A brief introduction of Kumari et al.'s protocol

This part simply describes Kumari et al.'s protocol [28]. We omit the password changing phase of their protocol. The registration-phase, login and authentication phase are introduced as follows.

3.1.1 Registration phase

User U_i selects identity ID_i, password PW_i in dictionary space and picks a random number b. First, U_i calculates $RPW_i = h(b \| PW_i)$ and sends $\{ID_i, RPW_i\}$ to server S on the secret channel. Second, once the registration-request $\{ID_i, RPW_i\}$ is received, S picks a random number y_i and calculates $N_i = h(ID_i \| x) \oplus RPW_i$, $Y_i = y_i \oplus h(ID_i \| x)$, $D_i = h(ID_i \| y_i \| RPW_i)$ and $E_i = y_i \oplus h(y \| x)$. Subsequently, server S sends N_i and a new smart card SC containing $\{Y_i, D_i, E_i, h(.)\}$ to U_i. Finally, on receiving SC and N_i from server, U_i computes $A_i = (ID_i \| PW_i) \oplus b$, $M_i = N_i \oplus b$. Then, U_i inserts $\{A_i, M_i\}$ into SC. Thus, U_i obtains a smart card in which $\{A_i, M_i, Y_i, D_i, E_i, h(.)\}$ are stored.

3.1.2 Login and authentication phase

In this part, $U_i(SC)$ and S execute the following steps for login and authentication:

(1) U_i inserts his smart card SC into the card reader and inputs correct ID_i, PW_i. Then, SC computes $b = (ID_i \| PW_i) \oplus A_i$, $RPW_i = h(b \| PW_i)$ and calculates $h(ID_i \| x) = M_i \oplus RPW_i \oplus b$, $y_i = h(ID_i \| x) \oplus Y_i$ and $D_i^* = h(ID_i \| y_i \| RPW_i)$. Afterward, SC checks $D_i^* =? D_i$. After finishing this verification, SC figures out $h(y \| x) = y_i \oplus E_i$ and $N_i = M_i \oplus b$. Subsequently, SC selects current timestamp T_i and calculates $CID_i = ID_i \oplus h(N_i \| y_i \| T_i)$, $N_i' = N_i \oplus h(y_i \| T_i)$, $B_i = N_i \oplus RPW_i$, $C_i = h(N_i || y_i || B_i || T_i)$ and $F_i = y_i \oplus (h(y||x)||T_i)$. Finally, SC sends the login request message $\{CID_i, N_i', C_i, F_i, T_i\}$ to S over a public channel.

(2) On receiving $\{CID_i, N_i', C_i, F_i, T_i\}$ from SC, S verifies the timestamp T_i according to the current timestamp. Then S computes $y_i = (h(y \| x) \| T_i) \oplus F_i$, $N_i = N_i' \oplus h(y_i \| T_i)$, $ID_i = CID_i \oplus h(N_i \| y_i \| T_i)$, $B_i^* = h(ID_i \| x)$ and $C_i^* = h(N_i || y_i || B_i^* || T_i)$.

Afterward, S checks $C_i^* =? C_i$. If the equation doesn't, S ends this request, otherwise, S selects the current timestamp T_{ss} and calculates $a = h(B_i^* \| y_i \| T_{ss})$. Afterwards, S sends $\{a, T_{ss}\}$ to SC.

(3) On receiving $\{a, T_{ss}\}$ from S, SC verifies the timestamp T_{ss} according to the current timestamp. Then, SC figures out $a^* = h(B_i \| y_i \| T_{ss})$ and checks $a_i^* =? a_i$.

(4) If the aforementioned steps are performed successfully, then U_i and S can figure out the common session key $SK_i = h(B_i || y_i || T_i || T_{ss} || h(y||x))$.

3.2 Vulnerability analysis of Kumari et al.'s protocol

In this subsection, we prove that the protocol of Kumari et al. [28] can neither resist key-compromise-impersonation attack nor provide perfect-forward-secrecy, except the vulnerability pointed out by Nikooghadam et al. [30].

3.2.1 Perfect-forward-secrecy

According to the analysis of Nikooghadam et al. [30], if a legitimate user U_j acts as an attacker and knows the long-term private key x of S, the malicious client U_j obtains the session key between U_i and S by performing the following steps.

(1) U_j computes $b_j = (ID_j \| PW_j) \oplus A_j$, $RPW_j = h(b_j \| PW_j)$, $h(ID_j \| x) = M_j \oplus RPW_j$, $y_j = Y_j \oplus h(ID_j \| x)$ and $h(y \| x) = y_j \oplus E_j$.
(2) U_j extracts the values $\{Y_i, M_i, A_i, D_i, E_i\}$ of the U_i's smart card and intercepts the login request message $\{CID_i, N_i', C_i, F_i, T_i\}$ and the respond message $\{a, T_{ss}\}$ to U_i from S.
(3) U_j calculates $y_i = F_i \oplus (h(y \| x) \| T_i)$, $N_i = N_i' \oplus (y_i \| T_i)$, $ID_i = CID_i \oplus h(N_i \| y_i \| T_i)$ and $B_i = h(ID_i \| x)$.
(4) Finally, U_j successfully computes the session key $SK_i = h(B_i||y_i||T_i||T_{ss}||h(y||x))$.

3.2.2 Key-compromise-impersonation-attack

If a legitimate user U_j acts as an attacker and compromises the long term secret key x of S, then U_j executes the following steps to impersonate U_i to S.

(1) U_j computes $b = (ID_j||PW_j) \oplus A_j$, $RPW_j = h(b||PW_j)$, $h(ID_j||x) = M_j \oplus RPW_j$, $y_j = Y_j \oplus h(ID_j||x)$ and $h(y||x) = y_j \oplus E_j$.
(2) U_j extracts the values $\{Y_i, M_i, A_i, D_i, E_i\}$ of the U_i's smart card and intercepts the login request message $\{CID_i, N_i', C_i, F_i, T_i\}$.
(3) U_j computes $y_i = F_i \oplus (h(y||x)||T_i)$, $N_i = N_i' \oplus (y_i||T_i)$, $ID_i = CID_i \oplus h(N_i||y_i||T_i)$ and $B_i = h(ID_i||x)$.
(4) U_j selects a new legitimate timestamp T_i'. U_j calculates $CID_i' = ID_i \oplus h(N_i||y_i||T_i')$, $N_i'' = N_i \oplus h(y_i||T_i')$, $C_i^* = h(N_i||y_i||B_i^*||T_i')$ and $F_i' = y_i \oplus (h(y||x)||T_i')$.
(5) U_j transmits the forged login message $\{CID_i', N_i', C_i', F_i', T_i'\}$ to S.
(6) Once $\{CID_i', N_i', C_i', F_i', T_i'\}$ from U_j is received, S verifies T_i', if it's within range, S computes $y_i = F_i' \oplus h(y||x)||T_i')$, $N_i = N_i' \oplus h(y_i||T_i')$, $ID_i = CID_i' \oplus h(N_i||y_i||T_i')$, $B_i^* = h(ID_i||x)$, and $C_i^* = h(N_i||y_i||B_i^*||T_i')$. Afterwards, S verifies whether $C_i^* = C_i'$, if these are equal, S chooses a timestamp T_{ss} and computes $a' = h(B_i^*||y_i||T_{ss})$.
(7) S sends the respond message $\{a', T_{ss}\}$ to U_j.
(8) Finally, S establishes the session key $SK_i = h(B_i||y_i||T_i'||T_{ss}||h(y||x))$ with the malicious user U_j.

4. Introduction and Cryptanalysis of Nikooghadam et al.'s Protocol

4.1 Review of Nikooghadam et al.'s protocol

4.1.1 Registration part

(1) U_i selects his identity ID_i, password PW_i in dictionary space, and then picks a random number r. Afterward, U_i computes $MPW_i = h(ID_i \| r \| PW_i)$. U_i sends $\{ID_i, MPW_i\}$ to S on the secret channel.
(2) Once the registration-request $\{ID_i, MPW_i\}$ is received, S chooses a random element N and calculates $A_i = h(ID_i \| x)$, $B_i = A_i \oplus MPW_i$, $MID_i = E_x(ID_i \| N)$. Then, S

stores ID_i in his database and takes $\{B_i, MID_i, E_k(.), D_k(.), h(.)\}$ into a new smart card SC. Subsequently, S sends SC to U_i.

(3) Finally, on receiving SC from the server, U_i inserts $\{r\}$ into SC. Thus, U_i gets a smart card in which $\{r, B_i, MID_i, E_k(.), D_k(.), h(.)\}$ are stored.

4.1.2 Login & authentication part

$U_i(SC)$ and S can finish login and authentication phase using the following steps:

(1) U_i inserts his smart card SC into the card reader and inputs ID_i, PW_i. Then, SC computes $A_i = B_i \oplus h(ID_i \| r \| PW_i)$. Subsequently, SC selects a random element RN_i and the current timestamp T_i, and computes $M_1 = E_{A_i}(ID_i \| RN_i \| T_i \| MID_i)$. Finally, SC transmits the login-request $\{MID_i, M_i, T_i\}$ to S on public-channel.

(2) On obtaining $\{CID_i, N_i', C_i, F_i, T_i\}$ from SC, S verifies the timestamp T_i according to the current timestamp. Then, S decrypts MID_i to get $(ID_i \| N)$ using his secret element x and figures out $A_i^* = h(ID_i \| x)$, $D_{A_i^*}(M_1) = (ID_i \| RN_i \| T_i \| MID_i)$. Aferwards, S selects random numbers RN_s and N^{New}. Subsequently, S computes $ID_i^{New} = E_x(ID_i \| N^{New})$ and $M_2 = E_{A_i^*}(MID_i^{New} \| RN_s \| ID_i \| RN_i)$. Finally, S sends $\{M_2\}$ to SC.

(3) On receiving $\{M_2\}$ from S, SC decrypts M_2 to be $(MID_i^{New} \| RN_s \| ID_i \| RN_i)$ using A_i^* and verifies ID_i, RN_i. Afterward, SC figures out $M_3 = h(RN_s \| MID^{New} \| RN_i)$ and the session key $SK = h(RN_i \| A_i \| RN_s)$. Then, replaces MID_i with MID_i^{New} by itself. At last, SC sends the response M_3 to S.

(4) After receiving M_3, S figures out $M_3^* = h(RN_s \| MID^{New} \| RN_i)$ and checks $M_3^* =? M_3$. If these are equal, S computes $SK = h(RN_i \| A_i^* \| RN_s)$. Otherwise, ends this session.

(5) Finally, U_i and S get the common session key $SK = h(RN_i \| A_i \| RN_s)$.

4.2 Vulnerability analysis of Nikooghadam et al.'s protocol

4.2.1 Off-line password guessing attack

If $\mathcal{A}$ gets the smart card SC_i of some user U_i, then $\mathcal{A}$ can obtain the useful datum $\{B_i, MID_i, r, E_{key}(\cdot) / D_{key}(\cdot), h(\cdot)\}$ in SC_i and intercepts the request message$\{MID_i, M_i, T_i\}$. Afterwards, $\mathcal{A}$ is able to get the correct password and identity of U_i as follows:

(1) $\mathcal{A}$ selects ID_i^*, PW_i^* as identity and password of U_i in the identity space $\mathcal{D}_{ID}$ and password space $\mathcal{D}_{PW}$.

(2) $\mathcal{A}$ figures out $A_i^* = B_i \oplus h(ID_i^* || r || PW_i^*)$.

(3) $\mathcal{A}$ uses A_i^* to decrypt the value of M_i. If the decryption is failed, then $\mathcal{A}$ repeats 1), 2) and 3) till the decryption becomes succussful. Otherwise, $\mathcal{A}$ calculates $D_{A_i^*}(M_i) = (ID_i || RN_i || T_i || MID_i^*)$ and checks whether $MID_i^* = MID_i$. If these are equal, it infers that ID_i^*, PW_i^* are the correct identity and password of user U_i.

By observing the above steps, we find that two guessing factors are used in login phase, that is, A_i and MID_i. A_i is the decryption key of M_i. On successful decryption, $\mathcal{A}$ cotinues to verify the second guessing factor transmitted through open channel. Moreover, we can compute the computation time complexity of guessing attack as follows: $\mathcal{O}(|\mathcal{D}_{ID}| * |\mathcal{D}_{PW}| * (T_h + T_s))$, where T_h is the computaional cost for a hash fuction computation and T_s is the computaional cost for symmetric encryption or decryption, $|\mathcal{D}_{ID}|$ and $|\mathcal{D}_{PW}|$

respectively denote the number of $\mathcal{D}_{ID}$ and the number of $\mathcal{D}_{PW}$. Usally, $|\mathcal{D}_{ID}| \leq |\mathcal{D}_{PW}| \leq 10^6$ [32,36,37].

Because of the low entropy of identity and password, $\mathcal{A}$ can successfully get the correct identity and password of user U_i within a polynomial time.

4.2.2 Perfect-forward-secrecy

In the protocol of Nikooghadam et al. [30], if $\mathcal{A}$ knows the long term secret key x of S, then $\mathcal{A}$ can obtain the session key between U_i and S.

(1) $\mathcal{A}$ eavesdrops on the login request message $\{MID_i, M_i, T_i\}$ and the respond message $\{M_s\}$ of U_i.
(2) $\mathcal{A}$ decrypts MID_i using the long term private key x of S, that is , $D_x(MID_i) = (ID_i||N)$. Then, $\mathcal{A}$ computes $A_i^* = h(ID_i||x)$.
(3) Afterward, $\mathcal{A}$ decrypts M_i, M_s using A_i^*, that is , $D_{A_i^*}(M_i) = (ID_i||RN_i||T_i||MID_i)$, $D_{A_i^*}(M_s) = (MID_i^{New}||RN_s||ID_i||RN_i)$, respectively. Thus, $\mathcal{A}$ obtains the values of $\{RN_i, h(ID_i||x), RN_s\}$.
(4) Finally, $\mathcal{A}$ successfully calculates the session key $SK = h(RN_i||h(ID_i||x)||RN_s)$.

4.2.3 Key compromise user impersonation attack

If $\mathcal{A}$ compromises the long-term secret key x of S, then $\mathcal{A}$ is able to execute the following steps to impersonate U_i to S.

(1) $\mathcal{A}$ firstly gets the login-message $\{MID_i, M_i, T_i\}$ of U_i. $\mathcal{A}$ computes $D_x(MID_i) = (ID_i||N)$. Afterwards, $\mathcal{A}$ computes $A_i^* = h(ID_i||x)$.
(2) $\mathcal{A}$ chossees a new legitimate timestamp T_i'. And then, $\mathcal{A}$ selects a random element RN_i' and figures out $M_i' = E_{A_i}(ID_i||RN_i'||T_i'||MID_i)$.
(3) $\mathcal{A}$ transmits S the forged message $\{MID_i, M_i', T_i'\}$.
(4) Upon $\{MID_i, M_i', T_i'\}$ from $\mathcal{A}$ is received, S checks T_i'. If it is invalid, S ends the session. Otherwise, S calculates $(ID_i||N) = D_x(MID_i)$, $A_i^* = h(ID_i||x)$ and $D_{A_i^*}(M_i) = (ID_i||RN_i'||T_i'||MID_i)$. Afterwards, S chooses two random numbers RN_s', $N^{New\prime}$. Subsequently, S computes $MID_i^{New\prime} = E_x(ID_i||N^{New\prime})$ and $M_2' = E_{A_i^*}(MID_i^{New'} \parallel RN_s' \parallel ID_i \parallel RN_i')$.
(5) S sends the challenge message $\{M_2'\}$ to $\mathcal{A}$.
(6) After getting the challenge message from S , $\mathcal{A}$ calculates $D_{A_i^*}(M_2') = (MID_i^{New'}||RN_s'||ID_i||RN_i')$. Then, $\mathcal{A}$ verifies the validity of ID_i and RN_i'. If these are invalid, $\mathcal{A}$ ends this attack. Otherwise, $\mathcal{A}$ continues to calculate $M_3' = h(RN_s' \parallel MID_i^{New'} \parallel RN_i')$.
(7) $\mathcal{A}$ forwards the response message $\{M_3'\}$ to S.
(8) On receiving the response message from $\mathcal{A}$, S computes $M_3^* = h(RN_s' \parallel MID_i^{New'} \parallel RN_i')$. Afterwards, S verifies whether $M_3^* = M_3'$. If these are not equal, S terminates this session. Otherwise, S calculates the session key $SK = h(RN_i' \parallel A_i^* \parallel RN_s')$ and believes that he has successfully established this session with the legimate user. Actually, $\mathcal{A}$ is “the legimate user”.

To sum up, the adversary successfully impersonates the legitimate user to S. Therefore, Nikooghadam et al.’s protocol fails to withstand such attack.

5. The Improved Protocol

According to the above cryptanalysis on Nikooghadam et al.'s protocol, first, the information $\{B_i, r\}$ in smart card and the symmetric encryption key A_i are used in the login request phase of their protocol, so that the attacker can perform off-line guessing. Second, their protocol does not employ public key cryptography, which is the key technology to preserve forward secrecy. Third, their protocol is incapable of resisting key-compromise-impersonation attack, because of lacking some secret number. However, the main aim of this part is to remove the weakness of Nikooghadam et al.'s protocol by using ECC and some tricks. And we present an improved lightweight authentication protocol using ECC. The improved protocol consists of four parts: initialization part, registration part, login and authentication part and password updating part. The registration part is depicted in **Fig. 1**. The login and authentication part is depicted in **Fig. 2**.

User U_i		Server S
Registration part:		
Select Id_i, Pw_i		Public key: $Q = xP$
Choose a random element r	$Id_i, h(Id_i \parallel r \parallel Pw_i)$ ⟹	Private key: x
		Compute $A_i = H(Id_i \parallel x \parallel T_i)$
		$B_i = A_i \oplus H(Id_i \parallel r \parallel Pw_i)$
		Select a random number N
		$MId_i = H(Id_i \parallel N) \oplus A_i$
		Store $\{B_i, MId_i, P, Q, E_k(\cdot) / D_k(\cdot), H(\cdot)\}$
	SC ⟸	in a new samrt card SC
Input r into SC		

Fig. 1. Registration part of User U_i

5.1 Initialization part

S chooses an elliptic curve $E_p(a, b)$ over F_p introduced in "Preliminaries". Then S picks a random element $x \in F_p$ and a hash function $H(\cdot)$. Subsequently, S calculates $Q = xP$. Lastly, S makes public the parameters $\{E, Q, H(\cdot)\}$ and preserves x as its long-term secret key.

5.2 Registration part

(1) User U_i chooses Id_i, Pw_i and a random element r and calculates $h(Id_i \parallel r \parallel Pw_i)$. Then, U_i trasmits S the registration request $\{Id_i, h(Id_i \parallel r \parallel Pw_i)\}$ secretly.

(2) S selects a random number T_i as the registration time of U_i. Afterwards, computs $A_i = H(Id_i \parallel x \parallel T_i)$, $B_i = A_i \oplus H(Id_i \parallel r \parallel Pw_i)$. Subsequently, S picks a random element N and computes $MId_i = H(Id_i \parallel N) \oplus A_i$. Lastly, S stores T_i in its database and distributes a new smart card $SC = \{B_i, MId_i, P, Q, E_k(\cdot) / D_k(\cdot), H(\cdot)\}$ to U_i.

(3) On receiving SC, user U_i inserts r into SC. Therefore, $SC = \{r, B_i, MId_i, P, Q, E_k(\cdot) / D_k(\cdot), H(\cdot)\}$.

5.3 Login & authentication part

(1) U_i inserts his smart card into card reader. Then U_i inputs Id_i, Pw_i. Subsequently, SC figures out $A_i = B_i \oplus h(Id_i \parallel r \parallel Pw_i)$ and picks a random element a.

Afterwards, calculates $C_1 = aP, C_2 = aQ$, $M_0 = E_{C_2}(Id_i \| H(A_i) \| MId_i)$, $M_1 = H(Id_i \| C_2 \| A_i \| MId_i)$, and transmits $\{C_1, M_0, M_1\}$ to S via a public channel.

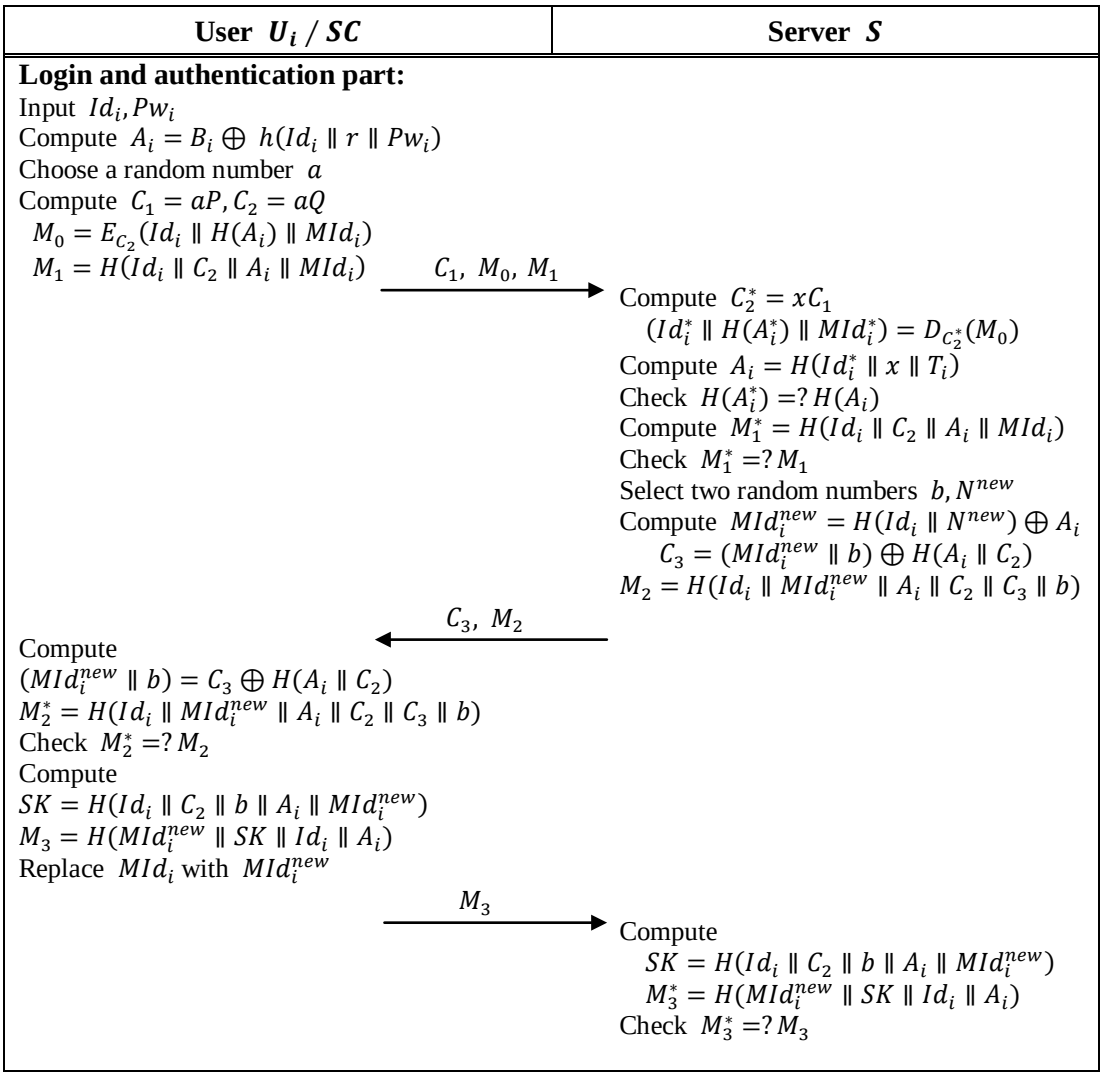

Fig. 2. Login and authentication part

(2) On receiving $\{C_1, M_0, M_1\}$, S computes $C_2^* = xC_1$, $(Id_i^* \| H(A_i^*) \| MId_i^*) = D_{C_2^*}(M_0)$, $A_i = H(Id_i^* \| x \| T_i)$ and verifies $H(A_i^*) =? H(A_i)$. If these are not equal, S terminates the login request. Otherwise, S computes $M_1^* = H(Id_i \| C_2 \| A_i \| MId_i)$ and checks $M_1^* =? M_1$. If these are not equal, S ends the next operation. Otherwise, S selects random numbers b, N^{new} and computes $MId_i^{new} = H(Id_i \| N^{new}) \oplus A_i$, $C_3 = (MId_i^{new} \| b) \oplus H(A_i \| C_2)$ and $M_2 = H(Id_i \| MId_i^{new} \| A_i \| C_2 \| C_3 \| b)$. Then, S sends $\{C_3, M_2\}$ to U_i via a public channel.

(3) After receiving $\{C_3, M_2\}$, SC figures out $(MId_i^{new} \| b) = C_3 \oplus H(A_i \| C_2)$, $M_2^* = H(Id_i \| MId_i^{new} \| A_i \| C_2 \| C_3 \| b)$ and checks $M_2^* =? M_2$. If these are not equal, SC terminates this session. Otherwise, SC compute $SK = H(Id_i \| C_2 \| b \| A_i \| MId_i^{new})$, $M_3 = H(MId_i^{new} \| SK \| Id_i \| A_i)$ and replaces MId_i with MId_i^{new}.

Finally, SC transmits M_3 to S via a public channel.

(4) Upon obtaining M_3, S calculates the session key $SK = H(Id_i \| C_2 \| b \| A_i \| MId_i^{new})$, then computes $M_3^* = H(MId_i^{new} \| SK \| Id_i \| A_i)$ and checks $M_3^* =? M_3$. If these are not equal, S ends this session. Otherwise, S accepts this session and the session key $SK = H(Id_i \| C_2 \| b \| A_i \| MId_i^{new})$.

5.4 Password updating part

After U_i and S have completed the authentication and the session key SK is established, U_i can renew his/her password at will. Firstly, U_i inputs his identity Id_i, old password Pw_i and new password Pw_i^{new}. Then, SC computes

$$B_i^{new} = B_i \oplus H(Id_i \| r \| Pw_i) \oplus H(Id_i \| r \| Pw_i^{new}).$$

Finally, SC replaces B_i with B_i^{new}.

***Remark*:** To eliminate the shortcomings of Kumari et al.'s and Nikooghadam et al.'s protocols and provide better security, in our protocol, 1. we adopt a pattern that the smart card does not check the correctness of the login, but the correctness of the login is verified by the server; 2. according to [53], in order to obtain perfect forward secrecy, the improved protocol uses elliptic curve cryptography (ECC); 3. in order to resist key-compromise user impersonation attack, the server store a secret element T_i in its database which cannot be leak to the adversary.

6. Heuristic security analysis

6.1 Preserve user anonymity & un-traceability

We suppose that the adversary $\mathcal{A}$ has stolen U_i's smart card and has obtained all datum $\{B_i, MId_i, P, Q, E_k(\cdot) / D_k(\cdot), H(\cdot)\}$. In the login process of U_i, $\mathcal{A}$ eavesdrops all transmitted message $\{C_1, M_0, M_1, C_3, M_2, M_3\}$. Since, these parameters are either protected by hash function or is computed by elliptic curve discrete logarithm cryptography, $\mathcal{A}$ is unable to derive the identity Id_i from them in polynomial time. Moreover, those transmitted message are variable in every time communication. Therefore, the presented protocol can provide user anonymity & un-traceability.

6.2 Resist privileged insider attack

During the registration phase, the user U_i sends $\{Id_i, h(Id_i \| r \| Pw_i)\}$ to S. The password Pw_i of U_i is protected by hash function and the secret element r, so the inside adversary cannot get the plaintext password of U_i. Accordingly, the proposed scheme is immune to such attack.

6.3 Resist replay attack

In our proposed scheme, all transmitted message $\{C_1, M_0, M_1, C_3, M_2, M_3\}$ in open channel are different for every communication. Once the adversary replays these message, the server or user can detect the problem. Therefore, it is impossible to perform the replay attack for the adversary in the improved protocol.

6.4 Resist stolen verifier attack

In our improved protocol, suppose that $\mathcal{A}$ steals the verifier table stored in S, however, $\mathcal{A}$ still cannot perform any attack. Thereupon, the improved protocol can resistance against stolen-verifier-attack.

6.5 Resist off-line password guessing attack

Suppose that $\mathcal{A}$ gets all elements stored in SC_i of U_i. On one hand, $\mathcal{A}$ is not able to guess the correct password Pw_i of U_i, since, there does not exist any verifying value in these parameters. On the other hand, if $\mathcal{A}$ not only gets these parameters in smart card, but also intercepts the login request message $\{C_1, M_0, M_1\}$, then $\mathcal{A}$ attempts to guess the password Pw_i of U_i. In the login request message, $\{M_0, M_1\}$ be used as verifying values. Afterwards, $\mathcal{A}$ can choose identity and password from dictionary space and computes $A_i^* = B_i \oplus h(Id_i^* \| r \| Pw_i^*)$. However, if $\mathcal{A}$ wants to calculate the corresponding verifier value $\{M_0, M_1\}$, he must know $C_2 = aQ = xC_1$, which is only known to the user and server. Accordingly, $\mathcal{A}$ cannot guess the correct password of U_i by computing the corresponding verifying values. Therefore, our proposed protocol is resistant to off-line dictionary attack.

6.6 Resist key-compromise user impersonation attack

Suppose that if the long-term private element x has been leaked to $\mathcal{A}$, and $\mathcal{A}$ can impersonate the legal user to server, then it infers that the analyzed protocol is vulnerable to key compromise impersonation attack. In proposed protocol, to impersonate the legal user U_i, $\mathcal{A}$ must be able to figure out the forged login request message. Since, the random number T_i of S hasn't been leaked to $\mathcal{A}$, it implies that $\mathcal{A}$ cannot get the correct value of $A_i = H(Id_i \| x \| T_i)$. Thereupon, $\mathcal{A}$ has no way to forge the legal value of $M_1 = H(Id_i \| C_2 \| A_i \| MId_i)$ and $M_3 = H(MId_i^{new} \| SK \| Id_i \| A_i)$. Thus, the proposed protocol is immune to key compromise user impersonation attack.

6.7 Resist server impersonation attack

If $\mathcal{A}$ wants to masquerade as S, then $\mathcal{A}$ must have to calculate a valid responding message $\{C_3, M_2\}$ for U_i. In proposed protocol, firstly, $\mathcal{A}$ captures the login request message $\{C_1, M_0, M_1\}$ and extracts the information $\{B_i, MId_i, P, r, Q, E_k(\cdot) / D_k(\cdot), H(\cdot)\}$ in smart card. Then, $\mathcal{A}$ selects two random numbers $b', N^{new\prime}$. To compute the valid message $\{C_3, M_2\}$, $\mathcal{A}$ must know the value of $\{A_i, C_2\}$ that can compute MId_i^{new}. However, $\mathcal{A}$ is unable to create C_2 without the long-term private key x of S. Thus, $\mathcal{A}$ cannot forge C_3 or even M_2. According to above discussion, it is inferred that the improved protocol can be protected against the server impersonation attack.

6.8 Provide mutual authentication

During the login & authentication part of the improved protocol, U_i is authenticated by S by using the equations $H(A_i^*) =? H(A_i)$ and $M_1^* =? M_1$. Subsequently, S by using the equation $M_2^* =? M_2$. According to the previous analysis, our improved protocol is immune to impersonation attack. Therefore, S and U_i can carry out authentication smoothly. That is to say, the proposed protocol addresses the requirements of mutual authentication.

6.9 Provide perfect forward security

Suppose the adversary can intercept any message over public channels and extracts the data in smart card by side-channel attack. In proposed protocol, though $\mathcal{A}$ knows password Pw_i of U_i and the long-term private key x of S, $\mathcal{A}$ still cannot calculate the session key $SK = H(Id_i \| C_2 \| b \| A_i \| MId_i^{new})$, because the key is protected by b, N^{new} and A_i. Accordingly, the improved protocol can preserve perfect forward secrecy.

7. Security simulation of proposed protocol using AVISPA software

AVISPA [38] is a pushbutton software tool for the automated validation of internet security-sensitive protocols and applications, can simulate the formal security verification for the improved protocol. Here, we give the simulation of the improved protocol by using *AVISPA* tool that estimates whether our protocol is safe under the Dolev-Yao model [31]. Since *AVISPA* tool accepts High Level Protocol Specification Language (*HLPSL*), we firstly provide the HLPSL codes, which are provided in **Figs. 3-5**, for U_i, S, the session, goal and the environment, respectively. The analysis results of the proposed protocol are displayed in **Figs. 6** and **7**. From the simulation results of OFMC and CL-AtSe, it is inferred that that the proposed protocol is SAFE against active and passive attacks including replay and man-in-the-middle attacks under Dolev-Yao model.

8. BNA-Logic Proof of Proposed Protocol

Here, we give the security proof of the improved protocol using BAN-Logic [39]. We prove that U_i can establish a session initial key with S in the proposed protocol. First, some BAN-Logic notations are listed in **Table 2**. Second, some BAN-logic postulates are listed in **Table 3**, and the idealized form, security goals and initiative premises of the improved protocol are formally provided.

(1) The idealized form of the proposed protocol is given as follows:

- **Message-1:** $U_i \longrightarrow S$: $C_1,\ (Id_i, C_2, MId_i)_{U_i \overset{A_i}{\leftrightarrow} S},\ \left(Id_i, MId_i^{new}, U_i \overset{SK}{\leftrightarrow} S\right)_{U_i \overset{A_i}{\leftrightarrow} S}$
- **Message-2:** $S \longrightarrow U_i$: $< MId_i^{new}, b >_{U_i \overset{H(A_i \| C_2)}{\longleftrightarrow} S},\ (Id_i, MId_i^{new}, C_2, C_3, b)_{U_i \overset{A_i}{\leftrightarrow} S}$

(2) Security goals of the proposed protocol are presented as follows:

- **Goal-1:** $U_i| \equiv S| \equiv U_i \overset{SK}{\leftrightarrow} S$
- **Goal-2:** $U_i| \equiv U_i \overset{SK}{\leftrightarrow} S$
- **Goal-3:** $S| \equiv U_i| \equiv U_i \overset{SK}{\leftrightarrow} S$
- **Goal-4:** $S| \equiv U_i \overset{SK}{\leftrightarrow} S$

(3) Initiative premises of the improved protocol are presented as follows:

- **I-1:** $U_i| \equiv \#a$
- **I-2:** $S| \equiv \#b$
- **I-3:** $U_i| \equiv \#MId_i^{new}$
- **I-4:** $S| \equiv \#MId_i^{new}$
- **I-5:** $U_i| \equiv U_i \overset{A_i}{\leftrightarrow} S$
- **I-6:** $S| \equiv U_i \overset{A_i}{\leftrightarrow} S$
- **I-7:** $U_i| \equiv S| \Rightarrow U_i \overset{SK}{\leftrightarrow} S$

- **I-8:** $S| \equiv U_i| \Rightarrow U_i \overset{SK}{\leftrightarrow} S$

(4) We conduct the BAN-Logic proof of the improved protocol as follows:

- **P-1:** According to Message-2, we have
$$U_i \lhd (Id_i, MId_i^{new}, C_2, C_3, b)_{U_i \overset{A_i}{\leftrightarrow} S}.$$
- **P-2:** From P-1, I-5, and Message-meaning rule, we deduce
$$U_i| \equiv S|\sim(Id_i, MId_i^{new}, C_2, C_3, b).$$
- **P-3:** By P-2, I-1, I-2, I-3, and Freshness-conjuncatenation rule, we infer
$$U_i| \equiv \#(Id_i, MId_i^{new}, C_2, C_3, b).$$
- **P-4:** By P-3, P-2, and Nonce-verification fule, we deduce
$$U_i| \equiv S| \equiv (Id_i, MId_i^{new}, C_2, C_3, b).$$
- **P-5:** From P-4 and Believe rule, we obtain
$$U_i| \equiv S| \equiv U_i \overset{SK}{\leftrightarrow} S \quad \text{-----} \quad \textbf{Goal-1}$$

```
role alice(Ui,S:agent, SKas:symmetric_key,
H, Mul: hash_func,
Snd, Rcv: channel(dy))
played_by Ui
def=
local State: nat,
IDi,PWi,R,X,Ti,VPWi,A,B,P,Q,N,C2,N0,MIdi0,SK:text,
Ai,Bi,MIdi,C1,C3,M0,M1,M2,M3:message,
Inc: hash_func
const alice_server_a,server_alice_b,subs1,subs2,subs3,
subs4,subs5:protocol_id
init State:=0
transition
%%%Registration phase
1.State=0/\Rcv(start)=|>
State':=1/\R':=new()
/\VPWi':=H(IDi.R'.PWi)
/\secret({PWi},subs1,Ui)
%%%Send the registration message to server
/\Snd({IDi.VPWi'}_SKas)
%%%Receive the responding registration message from server
2.State=1/\Rcv({Bi'.MIdi'.P.Q}_SKas)=|>
%%%Login and Authentication Phase
State':=3/\A':=new()
/\Ai':=xor(Bi,VPWi)
/\C1':=Mul(A'.P)
/\C2':=Mul(A'.Q)
/\M0':=xor(H(IDi.H(Ai').MIdi),C2')
/\M1':=H(IDi.C2'.Ai'.MIdi')
%%%Send the login request message to Server
/\Snd(C1'.M0'.M1')
/\witness(Ui,S,alice_server_a,C2')
/\request(Ui,S,alice_server_a,C2')
/\secret({C2'},subs2,{Ui,S})
%%%Receive the respond message from Server
3.State=3/\Rcv(C3'.M2')=|>
State':=5/\B':=new()
```

```
        /\MIdi0':=new()
        /\SK':=H(IDi.C2.B'.Ai.MIdi0')
        /\M3':=H(MIdi0'.SK'.IDi.Ai)
%%%Send the request message to Server
        /\Snd(M3')
/\request(S,Ui,server_alice_b,B)
end role
```

Fig. 3. Role specification of user U_i in *HLPSL*

- **P-6:** By I-7, P-5, and Jurisdiction rule, we get

$$U_i| \equiv U_i \overset{SK}{\leftrightarrow} S \quad \text{-----} \quad \textbf{Goal-2}$$

- **P-7:** According to Message-1, we have

$$S \lhd \left(Id_i, MId_i^{new}, U_i \overset{SK}{\leftrightarrow} S\right)_{U_i \overset{A_i}{\leftrightarrow} S}.$$

```
role server(S,Ui:agent,
SKas:symmetric_key,
H,Mul:hash_func,
Snd,Rcv:channel(dy))
played_by S
def=
local State:nat,
IDi,PWi,Ri,X,N,Ti,VPWi,A,B,P,Q,N0,MIdi0,C2,SK:text,
Ai,Bi,MIdi,C1,C3,M0,M1,M2,M3:message,
Inc:hash_func
const alice_server_a,server_alice_b,subs1,subs2,subs3,
subs4,subs5:protocol_id
init State:=0
transition
%%%Registration phase
%%%Receive the registration message from User
1.State=0/\Rcv({IDi.VPWi'}_SKas)=|>
State':=2/\X':=new()
        /\N':=new()
        /\Ti':=new()
        /\Ai':=H(IDi.X'.Ti')
        /\Bi':=xor(Ai',VPWi')
        /\MIdi':=xor(H(IDi.N'),Ai')
        /\secret({X',Ti',N'},subs5,S)
%%%Send the respond registration message to User
        /\Snd({Bi'.MIdi'.P.Q}_SKas)
%%%Login and Authentication Phase
%%%Receive the login request message from User
2.State=2/\Rcv({C1'.M0'.M1'}_SKas)=|>
State':=4/\B':=new()
/\N0':=new()
/\C2':=Mul(X.C1')
/\MIdi0':=xor(H(IDi.N0'),Ai)
/\C3':=xor((MIdi0'.B'),H(Ai.C2'))
/\M2':=H(IDi.MIdi0'.Ai.C2'.C3'.B')
%%%Send the respond message to User
/\Snd(C3'.M2')
```

```
/\witness(S,Ui,server_alice_b,B')
/\request(Ui,S,server_alice_b,B')
/\secret({B'},subs4,{S,Ui})
%%%Receive the respond message from User
3.State=4/\Rcv(M3')=|>
State':=6/\SK':=H(IDi.C2.B.Ai.MIdi0)
/\M3':=H(MIdi0.SK'.IDi.Ai)
end role
```

Fig. 4. Role specification of server S in *HLPSL*

- **P-8:** By P-7, I-5, and Message-meaning rule, we infer

$$S|\equiv U_i|\sim \left(Id_i, MId_i^{new}, U_i \overset{SK}{\leftrightarrow} S\right).$$

- **P-9:** From P-8, I-4, and Freshness-conjuncatenation rule, we have

$$S|\# \left(Id_i, MId_i^{new}, U_i \overset{SK}{\leftrightarrow} S\right).$$

```
role session(Ui, S: agent,
SKas : symmetric_key,
H, Mul: hash_func)
def=
local S1, S2, R1, R2: channel(dy)
composition
alice(Ui,S, SKas, H, Mul, S1, R1)
/\ server(Ui, S, SKas, H, Mul, S2, R2)
end role
role environment()
def=
const ui,s: agent,
skas : symmetric_key,
h, mul : hash_func,
idi,pwi,r,x,n,vpwi,bi,midi,a,b,p,q,n0,c1,c2,c3,m0,m1,m2,m3:text,

alice_server_a,server_alice_b, subs1,
subs2, subs3, subs4, subs5,subs6: protocol_id
intruder_knowledge = {ui,s, h, mul, bi, midi, r, p,q,c1,m0,
m1,c3, m2,m3}
composition
session(ui,s, skas, h, mul)
/\ session(s, ui, skas, h, mul)
end role
goal
secrecy_of subs1
secrecy_of subs2
secrecy_of subs3
secrecy_of subs4
secrecy_of subs5
authentication_on alice_server_a
authentication_on server_alice_b
end goal
environment()
```

Fig. 5. Roles for session, goal and environment in *HLPSL*.

- **P-10:** From P-8, P-9, and Nonce-verification fule, we deduce
$$S| \equiv U_i| \equiv \left(Id_i, MId_i^{new}, U_i \overset{SK}{\leftrightarrow} S\right).$$
- **P-11:** By P-10 and Believe rule, we get
$$S| \equiv U_i| \equiv U_i \overset{SK}{\leftrightarrow} S \quad \text{-----} \quad \textbf{Goal-3}$$
- **P-12:** From P-11, I-8, and Jurisdiction rule, we infer
$$S| \equiv U_i \overset{SK}{\leftrightarrow} S \quad \text{-----} \quad \textbf{Goal-4}$$

In summary, since Goals-1-2-3-4 are addressed, U_i and S are convinced that the session key is shared successfully between them.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/smq_KISS.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.02s
  visitedNodes: 4 nodes
  depth: 2 plies
```

Fig. 6. The experiment result using OFMC.

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  /home/span/span/testsuite/results/smq_KISS.if
GOAL
  As Specified
BACKEND
  CL-AtSe
STATISTICS
  Analysed    : 0 states
  Reachable   : 0 states
  Translation: 0.02 seconds
  Computation: 0.00 seconds
```

Fig. 7. The experiment result using CL-AtSe.

Table 2. BAN-Logic notations

Notations	Description
$X\&Y$	Statements
$A\&B$	Principals
K	Cryptographic encryption key
$A\mid\equiv X$	A believes on X
$A \lhd X$	A sees or receives X
$A\mid\sim X$	A once said X
$A\mid\Rightarrow X$	A controls X
$\#(X)$	X is fresh
$A \overset{K}{\leftrightarrow} B$	A and B communicate using shared key K
$(X,Y)_K$	Take hash of X and Y using K as key
$< X >_K$	X is xor-ed with the key K

Table 3. BAN-Logic rules

Rule	Description
Nonce-verification rule	$\dfrac{A\mid\equiv \#(X), A\mid\equiv B\mid\sim X}{A\mid\equiv B\mid\equiv X}$
Message meaning rule	$\dfrac{A\mid\equiv A \overset{K}{\leftrightarrow} B, A \lhd (X)_K}{A\mid\equiv B\mid\sim X}$
Freshness-conjuncatenation rule	$\dfrac{A\mid\equiv \#(X)}{A\mid\equiv \#(X,Y)}$
Believe rule	$\dfrac{A\mid\equiv B\mid\equiv (X,Y)}{A\mid\equiv B\mid\equiv X}$ or $\dfrac{A\mid\equiv X, A\mid\equiv Y}{A\mid\equiv (X,Y)}$
Jurisdiction rule	$\dfrac{A\mid\equiv B\mid\Rightarrow X, A\mid\equiv B\mid\equiv X}{A\mid\equiv X}$

9. Performance Analysis of improved Protocol with Related Literatures

In this part, we compare the performance of the improved protocol with some related protocols [26-30, 40-44, 54] in terms of computational cost and security performance. Usually, we neglect the lightweight operations such as exclusive-OR and string concatenation. However, the following cryptographic operations are considered: Th: the time for executing a hash operation, Ts: the time for performing symmetric key encryption/decryption, Tmm: an 160-bit modular multiplication, Tme: the computational time for an elliptic curve point multiplication, Tae: the computational cost for an elliptic curve point addition computation, Te: the computational time for an 1024-bit modular exponentiation. According to the experimental results of [45,46], Th, Ts, Tmm, Tme, Tae and Te approximately take $0.0023ms$, $0.0046ms$, $0.001855ms$, $2.226ms$, 0.0288ms, $3.85ms$, respectively.

Table 4. The computational cost in login-authentication phase

Cost / Protocols	User	Server	Total
Chang et al.[26]	$5Th$	$5Th$	$10Th \approx 0.023ms$
Kumari et al.[28]	$8Th$	$7Th$	$15Th \approx 0.0345ms$
Chaudhry et al.[29]	$8Th$	$6Th + 2Ts$	$14Th + 2Ts \approx 0.0414ms$
Nikooghadam et al.[30]	$3Th + 2Ts$	$3Th + 4Ts$	$6Th + 6Ts \approx 0.0414ms$
Chou et al.[40]	$10Th$	$11Th$	$21Th \approx 0.0483ms$
Wen et al.[41]	$9Th$	$8Th$	$17Th \approx 0.0391ms$
Wang et al.[27]	$3Te + 8Th$	$3Te + 6Th$	$6Te + 14Th \approx 23.1322ms$
Chen et al.[42]	$2Te + 2Tmm + 3Th$	$2TE + Tmm + 4Th$	$4Te + 3Tmm + 7Th \approx 15.4217ms$
Mishra et al.[43]	$2Te + 6Th$	$2Te + 5Th$	$4Te + 11Th \approx 15.4253ms$
Qu et al.[44]	$16Th + 2Tme$	$12Th + 2Tme$	$28Th + 4Tme \approx 8.9684ms$
Chaudhry et al.[54]	$8Th + 3Tme + Tae$	$6Th + 3Tme$	$14Th + 6Tme + Tae \approx 13.417ms$
Ours	$\mathbf{7Th + 2Tme + Ts}$	$\mathbf{8Th + Tme + Ts}$	$\mathbf{15Th + 3Tme + 2Ts \approx 6.7217ms}$

From **Table 4**, since the protocols of Chang et al.[26], Kumari et al. [28], Chaudhry et al. [29], Nikooghadam et al. [30], Chou et al. [40], Wen et al. [41] only use hash function and symmetric key cryptographic operations, the computational cost is quite small not exceeding $0.05ms$. In order to make the authentication protocol more secure, Wang et al. [27], Chen et al. [42], Mishra et al. [43], Qu et al. [44] and Chaudhry et al.[54] use public key cryptographic, such as: ECC, RSA and discrete logarithms on a general group. The computational cost of login-authentication phase in the protocols of Wang et al. [27], Chen et al. [42], Mishra et al. [43], Qu et al. [44] and Chaudhry et al.[54] are approximately $23.1322ms$, $15.4217ms$, $15.4253ms$, $8.9684ms$ and $13.417ms$ respectively. While the computational cost of the proposed protocol is approximately only $6.7217ms$. Therefore, it illustrates that the improved protocol is more efficient than [27,42-44] under the advantage of public key cryptography.

From **Table 5**, we observe that Chang et al.[26], Kumari et al. [28], Chaudhry et al. [29], Nikooghadam et al. [30], Chou et al. [40], Wen et al. [41]'s protocols are unable to provide perfect forward secrecy because of only using hash function and symmetric key cryptographic operations in their protocols. Among comparative literature, only our, Chaudhry et al. [29] and Mishra et al. [43]'s protocols can resist key-compromise impersonation attack. To summarize, all these compared literatures are more or less vulnerable to certain security vulnerabilities, except our and Mishra et al.'s protocol. According to **Table 4**, Mishra et al.'s protocol requires about $15.4253ms$ in login-authentication phase, while the proposed protocol executes only in $6.7217ms$. These illustrate that the improved protocol has better performance than the compared protocols.

Table 5. Comparison of security features

Features / Protocols	F1	F2	F3	F4	F5	F6	F7	F8	F9
Chang et al. [26]	No	No	Yes	Yes	No	No	No	Yes	No
Kumari et al. [28]	No	Yes	Yes	Yes	No	No	Yes	Yes	No
Chaudhry et al. [29]	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No
Nikooghadam et al. [30]	Yes	Yes	Yes	Yes	No	No	Yes	Yes	No
Chou et al. [40]	No	No	Yes	Yes	No	No	Yes	Yes	No
Wen et al. [41]	No	No	Yes	Yes	No	No	No	Yes	No
Wang et al. [27]	No	Yes	Yes	Yes	Yes	No	No	Yes	Yes
Chen et al. [42]	No	No	Yes	Yes	No	No	Yes	Yes	Yes
Mishra et al. [43]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Qu et al. [44]	No	Yes	Yes	Yes	No	No	Yes	Yes	Yes
Chaudhry et al.[54]	Yes	Yes	Yes	Yes	No	N/A	Yes	Yes	Yes
Ours	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**

F1: Preserve user anonymity & un-traceability, F2: Resist privileged-insider attack, F3: Resist replay attack, F4: Resist stolen verifier attack, F5: Resist off-line password guessing attack, F6: Resist (key-compromise) user impersonation attack, F7: Resist server impersonation attack, F8: Provide mutual authentication, F9: Provide perfect forward security. **N/A**: means the evaluation indicator is not considered.

10. Conclusion

In this paper, we proved that Kumari et al.'s protocol [28] is vulnerable to key-compromise impersonation attack and cannot provide perfect forward secrecy, while Nikooghadam et al.'s protocol [30] is vulnerable to key compromise impersonation attack, off-line password-guessing attack, and unable to provide perfect forward secrecy. In order to remedy these limitations, we design a new authentication and key agreement protocol based on Nikooghadam et al.'s protocol. By heuristic analysis, AVISPA software simulation and BAN-logic proof, we proved that the improved protocol is more secure than those relevant protocols. By comparison of computational cost, the improved protocol is also more efficient than comparative works under the category of public key cryptography. Therefore, through a comprehensive analysis and evaluation, it is inferred that the proposed protocol is more practical for real application scenarios because of its more secure and efficient features. In our future research, we will focus on exploring the more lightweight public key cryptography to design a practical authentication scheme. Moreover, according to [55-58], we will further explore the application of some cryptographic methods applied to image compression and digital watermarking.

Acknowledgment

The authors are thankful to the Editor and anonymous reviewers for the generous feedback and constructive comments. This research was supported by BUPT Excellent Ph.D. Students Foundation (No. CX2018312), the National Key Research and Development Program of China (No. 2018YFB0803600).

References

[1] J.Arkko, V. Torvinen, G. Camarillo, A. Niemi and T. Haukka, "Security mechanism agreement for SIP sessions," *IETF Internet Draft*, Jun. 2002.

[2] MK. Khan, "Fingerprint Biometric-based Self-Authentication and Deniable Authentication Schemes for the Electronic World," *Iete Technical Review*, vol. 26, no. 3, pp. 191–195, 2009. Article (CrossRef Link)

[3] TH. Chen, HL. Yeh, PC. Liu, HC. Hsiang and WK. Shih, "A secured authentication protocol for SIP using elliptic curves cryptography," *FGIT-FGCN*, vol. 119, no.1, pp. 46–55, 2010. Article (CrossRef Link).

[4] FW. Liu and H. Koenig, "Cryptanalysis of a SIP authentication scheme," *In: 12th IFIP TC6/TC11 International Conference, CMS, Lecture Notes in Computer Science*, vol. 7025, pp. 134–143, 2011. Article (CrossRef Link).

[5] DB. He, J. Chen and Chen Y, "A secure mutual authentication scheme for session initiation protocol using elliptic curve cryptography," *Secur Commun Netw*, vol.5, no.12, pp. 1423–1429, 2012. Article (CrossRef Link).

[6] R. Arshad and N. Ikram, "Elliptic curve cryptography based mutual authentication scheme for session initiation protocol," *Multimed Tools Appl*, vol.66, no.2, pp. 165–178, 2013. Article (CrossRef Link).

[7] MS. Farash and MA. Attari, "An Enhanced authenticated key agreement for session initiation protocol," *Inf Technol Control*, vol.42, no.4, pp. 333–342, 2013. Article (CrossRef Link).

[8] H. Tang and X. Liu, "Cryptanalysis of Arshad et al'.s ECC-based mutual authentication scheme for session initiation protocol," *Multimed Tools Appl*, vol. 65, no. 3, pp. 321–333, 2013. Article (CrossRef Link).

[9] XM. Wang, W. Guo, WF. Zhang, MK. Khan and K Alghathbar, "Cryptanalysis and improvement on a parallel keyed hash function based on chaotic neural network," *Telecommunication Systems*, vol. 52, no. 2, pp. 515–524, 2013. Article (CrossRef Link).

[10] S. Kumari and MK. Khan, "More secure smart card-based remote user password authentication scheme with user anonymity," *Security and Communication Networks*, vol.7, no.11, pp. 2039–2053, 2014. Article (CrossRef Link).

[11] S. Kumari, SA. Chaudhry, F. Wu, X. Li, MS. Farash and MK. Khan, "An improved smart card based authentication scheme for session initiation protocol," *Peer-to-Peer Networking and Applications*, 2015. Article (CrossRef Link).

[12] SA. Chaudhry, H. Naqvi, T. Shon, M. Sher and MS. Farash, "Cryptanalysis and Improvement of an Improved Two Factor Authentication Protocol for Telecare Medical Information Systems," *J. Medical Systems*, vol. 39, no.6, pp. 1–11, 2015. Article (CrossRef Link).

[13] S. Challa, AK. Das, S. Kumari, V. Odelu, F. Wu and X. Li, "Provably secure three-factor authentication and key agreement scheme for session initiation protocol," *Security and Communication Networks*, vol. 9, no.18, pp. 5412–5431, 2016. Article (CrossRef Link).

[14] SA. Chaudhry, I. Khan, A. Irshad, MU. Ashraf, MK. Khan and HF. Ahmad, "A provably secure anonymous authentication scheme for session initiation protocol," *Secur Commun Netw*, 2016. Article (CrossRef Link).

[15] AK. Sutrala, AK. Das, V. Odelu, M. Wazid and S. Kumari, "Secure anonymity-preserving password-based user authentication and session key agreement protocol for telecare medicine information systems," *Computer Methods and Programs in Biomedicine*, vol.135, pp. 167–185, 2016. Article (CrossRef Link).

[16] MS. Farash, SA. Chaudhry, M. Heydari, SMS. Sadough, S. Kumari and MK. Khan, "A lightweight anonymous authentication scheme for consumer roaming in ubiquitous networks with provable security," *Int. J. Communication Systems*, vol.30, no.4, 2017. Article (CrossRef Link).

[17] S. Kumari, M. Karuppiah, AK. Das, X. Li, F. Wu and V. Gupta, "Design of a secure anonymity-preserving authentication scheme for session initiation protocol using elliptic curve cryptography," *J Ambient Intell Human Comput*, 2017. Article (CrossRef Link).

[18] S. Kumari, "Design flaws of "an anonymous two-factor authenticated key agreement scheme for session initiation protocol using elliptic curve cryptography," *Multimed Tools Appl*, vol.76, pp. 13581, 2017. Article (CrossRef Link).
[19] SM. Qiu, GA. Xu, H. Ahmad and LC. Wang, "A Robust Mutual Authentication Scheme Based on Elliptic Curve Cryptography for Telecare Medical Information Systems," *IEEE Access*, 6, pp. 7452-7463, 2018. Article (CrossRef Link)
[20] SM. Qiu, GA. Xu, H. Ahmad and YH. Guo, "An enhanced password authentication scheme for session initiation protocol with perfect forward secrecy," *PLoS ONE*, vol. 13, no. 3, e0194072, 2018. Article (CrossRef Link).
[21] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leac and A. Luotonen, "HTTP Authentication: Basic and digest access authentication," *IETF RFC*, 2617, 1999.
[22] C. Yang, R. Wang and W. Liu, "Secure authentication scheme for session initiation protocol," *Comput Secur*, vol. 24, 381–386, 2015. Article (CrossRef Link).
[23] HF. Huang, WC. Wei and GE. Brown, "A new efficient authentication scheme for session initiation protocol," in *Proc. of 9th Joint Conference on Information Sciences*, 2006. Article (CrossRef Link)
[24] D. Denning, G. Sacco. "Timestamps in key distribution systems," *Commun ACM*, vol. 24, no.8, pp. 533–536, 1981. Article (CrossRef Link).
[25] A. Durlanik and I. Sogukpinar, "SIP authentication scheme using ECDH," *World Enformatika Soc Trans Eng Comput Technol*, 8, pp. 350–353, 2005.
[26] Y. Chang, W. Tai and H. Chang, "Untraceable dynamic-identity-based remote user authentication scheme with verifiable password update," *Int J Commun Syst*, 2015. Article (CrossRef Link).
[27] D. Wang, C. Ma, P. Wang and Z. Chen, "Robust smart card based password authentication scheme against smart card security breach," *IACR Cryptology ePrint Archive*, 2012. Retrieved from eprint.iacr.org/2012/439.pdf.
[28] S. Kumari, M. Khan and X. Li, "An improved remote user authentication scheme with key agreement," *Comput Electr Eng*, vol.40, no.6, pp. 1997–2012, 2014. Article (CrossRef Link)
[29] SA. Chaudhry, MS. Farash, H. Naqvi, S. Kumari and MK. Khan, "An enhanced privacy preserving remote user authentication scheme with provable security," *Secur Commun Netw*, vol.8, no.18, pp. 3782–3795, 2015. Article (CrossRef Link)
[30] Morteza. Nikooghadam, Reza. Jahantigh and Hamed. Arshad, "A lightweight authentication and key agreement protocol preserving user anonymity," *Multimedia Tools Appl*, Vol. 76, no.11, pp. 13401-13423, 2017. Article (CrossRef Link)
[31] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans Inf Theory*, vol. 29, no.2, pp. 198–208, 1983. Article (CrossRef Link).
[32] D. Wang and P. Wang, "Two birds with one stone: two-factor authentication with security beyond conventional bound," *IEEE Trans Depend Secur Comput*, 2016. Article (CrossRef Link).
[33] P. Kocher, J. Jaffe and B. Jun, "Differential power analysis," *Advances in Cryptology*, 1666, pp. 388–397, 1999. Article (CrossRef Link).
[34] TS. Messerges, EA. Dabbish and RH. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans Comput*, vol.51, no.5, pp. 541–552, 2002. Article (CrossRef Link).
[35] D. Wang, DB. He, P. Wang and C. Chu, "Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment," *IEEE Trans Depend Secur Comput*, vol. 12, no. 4, pp. 428–442, 2015. Article (CrossRef Link).
[36] DD. Wang, Z. Zhang, and P. Wang, ''Targeted online password guessing: An underestimated threat,'' in *Proc. of ACM CCS*, vol. 16, pp. 1242–1254, 2016. Article (CrossRef Link)
[37] D. Wang and P. Wang, "On the implications of Zipf's law in passwords," in *Proc. of ESORICS*, 2016, pp. 111–131. Article (CrossRef Link)
[38] AVISPA. "Automated validation of internet security protocols and applications," http://www.avispaproject.org/ (accessed on March 2018).

[39] M. Burrow, M. Abadi, and R. M. Needham, "A logic of authentication," *ACM Trans. Comput. Syst*, vol. 8, no. 1, pp. 18–36, 1990. Article (CrossRef Link)
[40] J. Chou, C. Huang, Y. Huang and Y. Chen, "Efficient two-pass anonymous identity authentication using smart card," *IACR Cryptology ePrint Archive*, 2013. Retrieved from eprint.iacr.org/2013/402.pdf.
[41] F. Wen and X. Li, "An improved dynamic id-based remote user authentication with key agreement scheme," *Comput Electr Eng*, vol. 38, no. 2, pp. 381–387, 2011. Article (CrossRef Link)
[42] BL. Chen, WC. Kuo and LC. Wuu, "Robust smart-card-based remote user password authentication scheme," *Int J Commun Syst*, 27, pp. 377–389, 2012. Article (CrossRef Link).
[43] D. Mishra, AK. Das, A. Chaturvedi and S. Mukhopadhyay, "A secure password-based authentication and key agreement scheme using smart cards," *J Inf Secur Appl*, 23, pp. 28–43, 2015. Article (CrossRef Link)
[44] Juan. Qu and Li-min. Zou, "An Improved Dynamic ID-Based Remote User Authentication with Key Agreement Scheme," *J. Electrical and Computer Engineering*, pp. 786587:1-786587:, 2013. Article (CrossRef Link)
[45] H. Kilinc and T. Yanik, "A survey of SIP authentication and key agreement schemes," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 2, pp. 1005–1023, 2014. Article (CrossRef Link).
[46] H. Arshad and M. Nikooghadam, "An efficient and secure authentication and key agreement scheme for session initiation protocol using ECC," *Multimedia Tools and Applications*, vol. 75, no. 1, pp. 181-197, 2016. Article (CrossRef Link)
[47] Chunguang. Ma, Dingwang. and Sendong. Zhao, "Security flaws in two improved remote user authentication schemes using smart cards," *Int. J. Communication Systems*, vol. 27, no. 10, pp. 2215-2227, 2014. Article (CrossRef Link)
[48] Xinyi. Huang, Xiaofeng. Chen, Jin. Li, Yang. Xiang and Li. Xu, "Further Observations on Smart-Card-Based Password-Authenticated Key Agreement in Distributed Systems," *IEEE Trans. Parallel Distrib. Syst*, vol. 25, no. 7, pp. 1767-1775, 2014. Article (CrossRef Link)
[49] Ding. Wang, Haibo. Cheng, Debiao. He and Ping. Wang, "On the Challenges in Designing Identity-Based Privacy-Preserving Authentication Schemes for Mobile Devices," *IEEE Systems Journal*, vol. 12, no. 1, pp. 916-925, 2018. Article (CrossRef Link)
[50] Ding. Wang and Ping. Wang, "On the anonymity of two-factor authentication schemes for wireless sensor networks: Attacks, principle and solutions," *Computer Networks*, 73, pp. 41-57, 2014. Article (CrossRef Link)
[51] Ding. Wang, Qianchen. Gu, Haibo. Cheng and Ping. Wang, "The Request for Better Measurement: A Comparative Evaluation of Two-Factor Authentication Schemes," *AsiaCCS*, pp. 475-486, 2016. Article (CrossRef Link)
[52] Mohammad. Wazid, Ashok Kumar. Das, Vanga. Odelu, Neeraj. Kumar, Mauro. Conti and Minho. Jo, "Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 269-282, 2018. Article (CrossRef Link)
[53] Ding. Wang, Nan, Wang, Ping. Wang and Sihan. Qing, "Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity," *Inf. Sci*, 321, pp. 162-178, 2015. Article (CrossRef Link)
[54] Shehzad Ashraf. Chaudhry, Husnain. Naqvi, Khalid. Mahmood, Hafiz. Farooq. Ahmad and Muhammad Khurram. Khan, "An Improved Remote User Authentication Scheme Using Elliptic Curve Cryptography," *Wireless Personal Communications*, vol. 96, no. 4, pp. 5355-5373, 2017. Article (CrossRef Link)
[55] Shuai. Liu, Zheng. Pan and Houbing. Song, "Digital image watermarking method based on DCT and fractal encoding," *IET Image Processing*, vol. 11, no. 10, pp. 815-821, 2017. Article (CrossRef Link)
[56] Shuai. Liu, Zheng. Pan and Xiaochun. Cheng, "A Novel Fast Fractal Image Compression Method based on Distance Clustering in High Dimensional Sphere Surface," *Fractals*, vol. 25, no. 4, 1740004, 2017. Article (CrossRef Link)

[57] Zheng. Pan, Shuai. Liu and Weina. Fu, "A review of visual moving target tracking," *Multimedia Tools Appl*, vol. 76, no. 16, pp. 16989-17018, 2017. Article (CrossRef Link)
[58] Shuai. Liu, Mengye. Lu, Gaocheng. Liu and Zheng. Pan, "A Novel Distance Metric: Generalized Relative Entropy," *Entropy*, vol. 19, no. 6, pp. 269, 2017. Article (CrossRef Link)

Shuming Qiu received the M.S. degree from Jiangxi Normal University in 2009. He is currently a Ph.D. student in Beijing University of Posts and Telecommunications, Beijing, China and a lecturer at Jiangxi Normal University, Nanchang, China. His research interests include algebra, information security and cryptography (in particular, cryptographic protocols, non-commutative cryptography), etc.

Guosheng Xu received the Ph.D. degree in Information Security from Beijing University of Posts and Telecommunications, China, in 2008. He is a lecturer in school of Cyberspace Security, Beijing University of Posts and Telecommunications. His research interest is in the areas of deep learning and mordern cryptography.

Haseeb Ahmad is serving as an Assistant Professor at Department of Computer Science, National Textile University, Faisalabad, Pakistan. He received the BS degree from G.C. University, Faisalabad, Pakistan in 2010 and the Masters degree from Virtual University of Pakistan in 2012. He has obtained his PhD degree from Beijing University of Posts and Telecommunications, Beijing, China in 2017. His current research interest includes data mining, information retrieval and information security.

Guoai Xu received the Ph.D. degree in signal and information processing from Beijing University of Posts and Telecommunications, China, in 2002. He was awarded the title of Professor in 2011. He is currently an associate director in the National Engineering Laboratory of Security Technology for Mobile Internet, School of Cyberspace Security, Beijing University of Posts and Telecommunications. His research interest is in the areas of software security and data analysis.

Xinping Qiu received the M.S. degree in applied mathematics in 2000 and the Ph.D. degree in management science and engineering in 2006 from Beijing University of Posts and Telecommunications，Beijing，China. He is a lecturer at Jiangxi University of Finance and Economics, Nanchang, Jiangxi. His research interests include network and e-commerce.

Hong Xu served in the High-Tech Research & Development Center (HTRDC) of the Ministry of Science & Technology, P.R.C. She had managed several “863” programs, e.g., network communication and information security. Now, she is the manager of the earth observation and navigation program which is included in the national key research and development plan. Ms. Hong Xu has published several papers, and her research areas focus on science management policy and system, innovation mechanism, network communication, information security, remote sensing and navigation technology, etc.