A Novel Blockchain-based Anonymous Handover Authentication Scheme in Mobile Networks

ChenCheng Hu, Dong Zheng, Rui Guo, AXin Wu, Liang Wang, and ShiYao Gao
(Corresponding author: ChenCheng Hu)

School of Cyberspace Security, Xi'an University of Posts and Telecommunications
National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications
Xi'an 710121, China
(Email: 13772485758@163.com)

(Received Apr. 23, 2019; Revised and Accepted Nov. 16, 2019; First Online Jan. 29, 2020)

Abstract

In the wireless mobile network (WMN), the handover authentication scheme is the key to ensure fast and secure handoff of mobile nodes among several access points. However, it is difficult to design an appropriate handover authentication protocol for the inherent drawbacks in WMN. For example, the resources of the MN are limited and the mobile nodes have low capability in computing. Therefore, the traditional authentication schemes are unsuited to be applied in WMN for the reason that they have low efficiency. To construct a fast handover authentication protocol, in this paper, we design an anonymous handover authentication protocol with high efficiency by considering the distributed storage, collective maintenance and tamper-resistance. Then, the security and efficiency of the proposal is analyzed, and it is concluded that ours uses chameleon hash with blockchain to achieve robust security and high efficiency. Meanwhile, our scheme satisfies the property of user anonymity, conditional privacy protection and robust key agreement as well.

Keywords: Anonymity; Blockchain; Chameleon Hash; Handover Authentication; Wireless Mobile Network

1 Introduction

With the rapid development of wireless mobile network (WMN), various mobile Internet applications have been utilized in the different fields of life. Due to the portability and mobility of mobile devices, the demand for multimedia services by mobile nodes has exploded. Therefore, providing secure and fast real-time services for mobile users will become an inevitable trend in the future. When a service provider offers these real-time services to mobile terminals in the wireless network, the mobile users often need a handoff in the different access points (or base stations) for the limited signal range. In detail, a new connection is established between the mobile terminal and the new access point depending on the handover authentication.

The handover authentication technology realizes the interconnection, intercommunication and mutual confidence between the mobile node and access points, which provides a guarantee for the secure communication in the mobile internet. As shown in Figure 1, a typical handover authentication scenario consists of three entities: The mobile nodes (MNs), access points (APs) and authentication server (AS). For a secure handover authentication, when the MN moves from the current node (AP1) to the new node (AP2), the AP2 needs to authenticate the MN to prevent the illegal users, and the MN also needs to authenticate the AP2 to prevent an attacker from disguising the AP2. In addition, the MN should also establish a session key with the AP2 to protect the security of user's data. Based on this framework, the handover authentication is employed in the mobile communication and real-time services such as 5G, Voice over Internet Phone(VoIP), VideoPhone, mobile TV, Video Conference, and online games. However, the time-delay in these services affects user experience seriously. Thus, it is crucial to reduce the time-delay and the energy consumption in the process of handover authentication that improves the service quality.

To design an efficient and secure handover authentication protocol, there are two issues should be considered. First, for the limited computing power of the MN, the protocol should be lightweight in computation and communication costs. Second, because of the openness of wireless network, the protocol should have robust security to protect the privacy of MN and prevent the system from various attacks. In order to achieve the requirements above, many handover authentication protocols have been put forward in the last several years.

1.1 Related Works

In IEEE 802.11i [3], it proposed a four-way handshake to create a Pairwise Transient Key (PTK) and then distributed a Group Transient Key (GTK) for broadcast

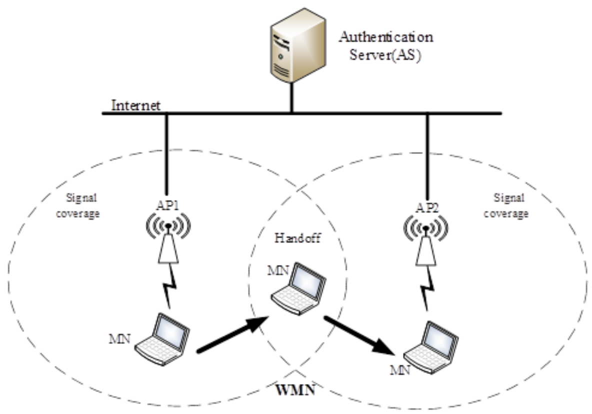

Figure 1: Handover authentication overview

communication. However, the time cost of full handover authentication is unacceptable for real-time traffic in nowadays. In order to improve the performance of handover authentication scheme, the authentication, authorization, and accounting (AAA) based schemes [21,22] were proposed. These schemes use AAA servers to ensure security handovers, and they adopt pre-authentication and proactive key distribution methods to increase the efficiency of authentication. However, they need to establish trust relationship and generate a large amount of authentication traffic between network nodes, which increases the complexity of the entire system. Different from the AAA scheme, there is an alternative protocol without communicating with the AAA server which is called the Security Context Transfer (SCT) schemes [4,27,30] were proposed. The SCT scheme need not to establish communication between AAA and AP. Nevertheless, these solutions are based on the assumption that the APs are mutually trustworthy. Thus, in actual application scenarios, the APs cannot be trusted totally, which brings some security risks to these schemes.

In order to solve the problems in handover authentication above, some works [2,12–15,18,19,28,29] were proposed. In [15], an identity-based handover authentication scheme was proposed, which can be implemented only by ID between the MN and AP. This scheme has better efficiency than AAA scheme because there is no need to make communication between the MN and AP, and it reduces the overall system complexity compared to the AAA-based and SCT-based schemes. Unfortunately, since there is a PKG to issue a private key, this solution has the problem of key escrow.

The study in [2] used low-cost functions to achieve security and efficiency, it also used nonce instead of timestamps to avoid the clock synchronization problem. However, Youn *et al.* [29] identified that the scheme of [2] cannot achieve the anonymity under four attack strategies, and it is not efficient in password authentication. Liao and Wang [19] presented a dynamic ID-based remote user authentication scheme for multi-server environment, the scheme of [19] uses simple hash function to enhance efficiency and it can preserve user's anonymity. Later on, Hsiang and Shih [14] showed that the scheme of [19] is vulnerable to insider's attack. He *et al.* [12] proposed a strong user authentication scheme with smart cards for wireless communications.

The scheme of [12] is suitable for the low-power and resource-limited mobile devices since it only performs a symmetric encryption/decryption operation. However, [18] showed that He *et al.*'s scheme is unfairness in key agreement. Then, He *et al.* [13] summarized the basic security requirements of handover authentication protocols and proposed a novel batch verification AHA protocol. However, their implementation calls for complex and time-consuming operation, such as bilinear pairing operations and point multiplication. After that, Xie *et al.* [28] proposed an improved AHA protocol using ECC. Unfortunately, this scheme does not support batch verification and are not suitable for practical applications.

Ramadan *et al.* [23] proposed a user-to-user mutual authentication and key agreement scheme, which is more compatible with the LTE security architecture. In recent years, the idea of proxy signature has been utilized to design handoff authentication schemes [7–9,20]. The essential idea of these schemes lies in that the authentication server issues its delegation power to the MN, which grants the MN the ability to generate a proxy signature on behalf of the authentication server. Then, the new AP trusts the MN due to the proxy signature on behalf of the authentication server. However, these schemes are vulnerable to various security issues.

Different from the above schemes, the schemes in [5,10,11] proposed a handover authentication scheme based on the chameleon hash function. These schemes used the collision of chameleon hash function for authentication to avoid certificate management problems. These protocols are lightweight authentication schemes with high efficiency, but there are still some shortcomings in them, such as key escrow, privacy preservation, redirection attack, high communication and computation overhead.

In the handover authentication, if the legal identity of the MN can be securely broadcast to all APs, the efficiency of authentication process can be greatly improved. In order to make this property can be applied in the handover authentication, we use blockchain technology to achieve our goals. Nowadays, blockchain technology has been applied in many fields [6,17,24,25]. Regarding the application of blockchain in the field of identity authentication. In the literature [6], based on the shortcomings of traditional authentication relying on third-party centers and vulnerable to man-in-the-middle attacks, a blockchain PKI scheme based on privacy protection was proposed. The scheme of [17] describes the concept of blockchain PKI and shows that it has significant advantages over traditional PKI and implements PKI authentication based on Ethereum. However, none of these schemes solves the handover authentication problem.

1.2 Our Contribution

For the above problems in the current handover authentication, we propose a secure anonymous handover authentication scheme based on chameleon hash function and blockchain technology, and design a blockchain certificate model. We summarize our main research contributions as follows:

1) In order to improve the efficiency of authentication process, our scheme uses the distributed and difficult-to-tamper features of the blockchain, and it does not require an extra interaction between the AP node and registration node.

2) We use a blockchain certificate and chameleon hash function to solve the problem of certificate management.

3) To achieve the robust security, we use pseudonyms to provide user anonymity, conditional privacy protection, and updatable key agreement.

4) Finally, we analyze the performance of our scheme and compare its performance with some existing schemes. From the analysis results, our scheme is more efficient than them.

1.3 Organization

The rest of the paper is organized as follows: The Section 2 introduces some preliminaries, such as the knowledge of blockchain techniques, chameleon hash functions and the requirements for an ideal handover authentication. The anonymous handover authentication based on blockchain scheme is presented in Section 3. The security and performance analysis of the related schemes is discussed in Section 4. Finally, Section 5 concludes the paper.

2 Preliminaries

2.1 Blockchain

Blockchain is a new application mode of computer technology such as distributed database, point-to-point transmission, consensus protocols, and encryption algorithm [24]. It records all transaction information occurring on the node. The process is highly transparent and the data is highly secure. The data structure of the blockchain can be described from three levels: Chain, block and transaction. All transactions in the same time period form a block, and the blocks are linked in chronological order to form a blockchain. When several transactions are packaged into a block, data in all nodes can be updated. Each block is composed of a block header and a block body.

Each block header contains the hash value of the previous block, the timestamp, the total hash value of the transaction data (Merkle root). In this way, the chain structure is formed by the interlocking of the hash values of each block. Because of these properties, blockchain has some important characteristics such as tamper resistance, data synchronization, traceability.

2.2 Chameleon Hash Function

The chameleon hash function was first proposed by Krawczyk and Rabin as a one-way hash function with trapdoors [16]. A chameleon hash function is associated with a set of public and private keys, which are also known as trapdoors. For the participants who do not grasp the trapdoor information, it is only a one-way function that is strongly collision-resistance. But for the users who have mastered the trapdoor information, he can easily calculate the collision of the chameleon hash function.

Definition 1. *A chameleon hash function based on the single trapdoor information) [1]*

Generation of public and private key pairs: Let p be a safe prime number of bitlength τ, and satisfies $p = 2q + 1$, where q is a sufficiently large prime number. Let Z_p^* be a group, g is the generator of Z_p^*, g has order q. The user chooses random number $x \in Z_q^*$ as a private key CK_R, and the corresponding public key HK_R is computed as $y = g^x modp$. Assume that the length of q is λ. Let H be a collision-resistant hash function, mapping arbitrary-length bitstrings to strings of fixed length λ, $H : \{0, 1\}^* \to H : \{0, 1\}^\lambda$.

Construction of chameleon hash function: To commit to a message m, and $m \in Z_q^*$. Define the chameleon hash function as: $CHAM - HASH(m, r, s) = r - (y^e g^s modp) modq$, the random values (r, s) are choose from $Z_q^* \times Z_q^*$, where $e = H(m||r)$.

Collision finding: Let C be the output of Chameleon hash function $C = CHAM - HASH(m, r, s)$, the user chooses a new random message m' and a random value $k \in Z_q^*$, then computes $r' = C + (g^k modp) modq$, $e' = h(m'||r')$, $s' = k - e'xmodq$. Then, we can get the equation:

$$\begin{aligned} C &= CHAM - HASH(m, r, s) \\ &= CHAM - HASH(m', r', s'). \end{aligned}$$

Computational Diffie-Hellman (CDH) problem: Given $x \cdot P, y \cdot P(g^x, g^y)$, the task of the CDH problem is computing $x \cdot y \cdot P(g^{x \cdot y})$, where $x, y \in Z_q^*$ are two unknown numbers.

2.3 Requirements of Handover Authentication

In wireless networks, an ideal handover authentication scheme should satisfy the following requirements:

1) **Mutual authentication:** The AP should authenticate the identity of the MN to determine that the MN is a legitimate user. At the same time, although the AP is trusted, the MN should also authenticate the AP, in order to prevent the attacker from impersonating the AP.

2) **Conditional privacy protection of user:** The identity of the user should not be made public, except for the initial registration node, even if the AP does not know the true identity of the user. However, in some special cases, the AP can send a request to the registration node to obtain the true identity of the MN.

3) **Key agreement:** After mutual authentication is completed, a session key should be established between the MN and the AP to ensure the security of communication afterwards.

4) **Robust security property:** The handover authentication protocols should provide robust security attributes to defend against various attacks on the wireless network (such as eavesdropping, replay attacks, man-in-the-middle attacks, *etc.*).

5) **Perfect forward secrecy:** To protect the security of the session key, a handover authentication protocol should be able to provide perfect forward secrecy, i.e., the adversary cannot extract the session key produced in previous session even he/she gets both private keys of the MN and the AP.

6) **Efficiency:** Since the computing power and storage capacity of mobile nodes in mobile networks are limited, the energy consumption of the authentication process should be as small as possible and the delay should be as low as possible.

The scheme we proposed in this paper satisfies the security attributes required for the above handover authentication.

3 Anonymous Handover Authentication Based on Blockchain

3.1 Blockchain Certificate

In this section, we designed a blockchain certificate based on the X.509 digital certificate and blockchain structure. When the MN completes registration at the registration node AS, the AS will generate a unique blockchain certificate and upload it to the blockchain for the next handover authentication. Our bolckchain certificate structure is shown in Figure 2.

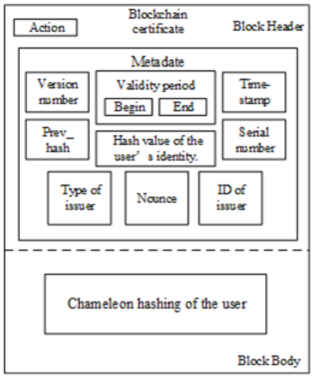

Figure 2: Blockchain certificate

According to [26], the write interface of the blockchain is defined as put(action, data), and the query interface of the blockchain is defined as get(condition). The registration node and the authentication server have the right to write and query. The valid users only have the right to query. The parameter action of the interface written here indicates the user's data processing intent, which can be the state of "issue" or "revoke". The parameter action of the interface written here indicates the user's data processing intent, which can be the state of "issue" or "revoke". Since the blockchain cannot change the data already stored in the blockchain, the issue and revoke here do not directly operate on the data, but record the operation of this data in the blockchain, and then generate a new block and add it to the blockchain. Our handover authentication model is shown in Figure 3.

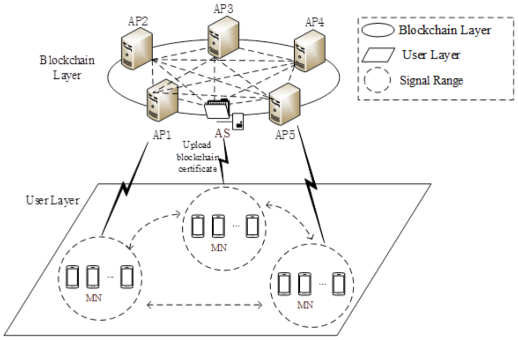

Figure 3: Our handover authentication system model

3.2 Our Handover Authentication Scheme

This section introduces our proposed anonymous handover authentication scheme based on blockchain technology. The notations used in the protocol are shown in Table 1.

Where i represents the different stages of the calculation, the specific process diagram of the protocol flow is shown in Figure 4 and Figure 5:

3.2.1 Initial Authentication Phase

The Initial authentication phase is shown as Figure 4. In the Initial Authentication phase, the mobile node MN needs to register to the AS node with his real identity. If the MN is valid, the AS generates a blockchain certificate

Table 1: The notations used in protocol

Notations	Meanings
$h_1() : \{0,1\}^* \rightarrow Z_q^*$ $h_2() : \{0,1\}^* \rightarrow \{0,1\}^\lambda$	One way and collision-resistance hash function
ID_x	The identity of x
N_i	Random number
$C()_x$	The blockchain certificate of x
T_{Exp}, T_{Curr}	Expiration and current time
(X_x, Y_x)	The chameleon hash trapdoor key pair of x
$CHAM(m,r,s)$	Chameleon hash function $CHAM(m,r,s) = r - (Y_x^e g^s modp) modq$
$r(i)_x$	The parameter of Chameleon hash function where $r(i)_x = CHAM(m,r,s) + (g^k modq)$
$s(i)_x$	The parameter of Chameleon hash function where $s(i)_x = k - eX_x modq$
m_x	A message choose by x where $m_x \in Z_q^*$
e	$e$is a required parameter to calculates$(i)_x$,where $e = h_2(m,r)$

of MN, and uploads it to the blockchain. Similarly, for each AP node, their own blockchain certificates are also recorded in the blockchain.

System Parameters: Our scheme specifies two random prime number p and q,q is a big prime number, where $p = 2q+1$.g is selected as a generator of order q from Z_q^*. $h_1() : \{0,1\}^* \rightarrow Z_q^*$ and $h_2() : \{0,1\}^* \rightarrow \{0,1\}^\lambda$ are two safe and collision-resistant hash functions.

1) MN → AS: $h_2(ID_{MN})$ The mobile node MN sends the hash value of his identity $h_2(ID_{MN})$ to the AS. Upon receiving the parameter from the MN. The AS verifies the validity of the MN identity based on the stored identity hash value. If the identity is invalid, the MN's access is denied, otherwise, the authentication proceed to the next step.

2) AS → MN: PID After confirming the identity of the MN, AS chooses a pseudo-name set $PID = pid_1, pid_2$...in which the elements are unlinkable, and sends it to the MN.

3) MN → AS: $CHAM(m_{MN}, r(0)_{MN}, s(0)_{MN})$ After the MN receives the feedback from the AS, the MN randomly chooses $X_{MN} \in Z_q^*$ as his private Chameleon hash key CK_R, and Y_{MN} is public Chameleon hash key. Then the MN chooses the random values $(r(0)_{MN}, s(0)_{MN})$ from $Z_q^* * Z_q^*$,and computes the value of Chameleon hash function:

$$\begin{aligned} C &= CHAM(m_{MN}, r(0)_{MN}, s(0)_{MN}) \\ &= r(0)_{MN} - (Y_{MN}^{e_{MN}} g^{s(0)_{MN}} \bmod p) \bmod q. \end{aligned}$$

Then, the MN sends the value to the AS, where $e_{MN} = h_2(m_{MN}, r(0)_{MN})$.

4) AS → Blockchain: $C(0)_{MN}$ Upon receiving the chameleon hash value sent by MN, the AS generates a blockchain certificate of the MN and uploads it to the blockchain.

5) AS → MN: T_{EXP} After the AS generates the blockchain certificate of the MN, it returns the time when the certificate expires to the MN. At the same time, the AS opens the query interface of the blockchain to the MN, so that the MN can query the data on the blockchain.

3.2.2 Handover Authentication Phase

The Handover Authentication phase is shown as Figure 5. When the MN arrives at the new AP2, the AP2 needs to

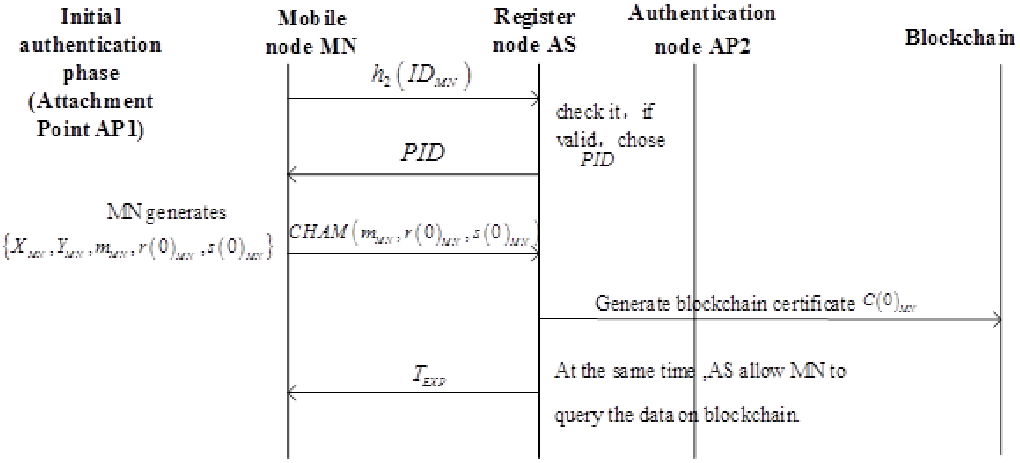
Initial authentication phase (Attachment Point AP1)
Mobile node MN
Register node AS
Authentication node AP2
Blockchain
$h_2(ID_{MN})$
check it，if valid，chose PID
PID
MN generates
$\{X_{MN}; Y_{MN}; m_{MN}; r(0)_{MN}; s(0)_{MN}\}$
$CHAM(m_{MN}, r(0)_{MN}, s(0)_{MN})$
Generate blockchain certificate $C(0)_{MN}$
T_{EXP}
At the same time ,AS allow MN to query the data on blockchain

Figure 4: Initial authentication phase

authenticate the legal identity of MN to decide whether to provide services for the MN. Similarly, the MN also needs to authenticates the AP2.

1) MN → AP2: $Cert_{MN} \parallel m'_{MN} \parallel r(1)_{MN} \parallel s(1)_{MN} \parallel g^{h_1(pid_j+N_1)} \parallel T_{Curr}$

   The MN chooses an unused pid_j from PID, a new random message m'_{MN}, and computes $g^{h_1(pid_j+N_1)}$, then the MN sends $Cert_{MN} \parallel m'_{MN} \parallel r(1)_{MN} \parallel s(1)_{MN} \parallel g^{h_1(pid_j+N_1)} \parallel T_{Curr}$ to AP2, where

$$\begin{aligned} Cert_{MN} &= (pid_j, g^{X_{MN}}) \\ r(1)_{MN} &= CHAM(m_{MN}, r(0)_{MN}, s(0)_{MN}) \\ &\quad +(g^{h_1(pid_j+N_1)} \bmod q) \\ s(1)_{MN} &= h_1(pid_j + N_1) - e'_{MN}X_{MN} \bmod q \\ e'_{MN} &= h_2(m'_{MN}, r(1)_{MN}). \end{aligned}$$

2) AP2 ← Blockchain: $C(0)_{MN}$ Upon receiving the parameters from the MN, the AP2 uses these parameters to find the MN's blockchain certificate. Then, the AP2 queries the status of the MN's blockchain certificate. If the certificate status is "revoke", the MN's access is denied. Otherwise, the AP2 computes:

$$\begin{aligned} & CHAM(m'_{MN}, r(1)_{MN}, s(1)_{MN}) \\ = \; & r(1)_{MN} - (Y_{MN}^{e'_{MN}} g^{s(1)_{MN}} \bmod p) \bmod q, \end{aligned}$$

   and compares with the Chameleon hash value of MN's blockchain certificate $C(0)_{MN}$ to verify whether

$$\begin{aligned} & CHAM(m_{MN}, r(0)_{MN}, s(0)_{MN}) \\ = \; & CHAM(m'_{MN}, r(1)_{MN}, s(1)_{MN}) \end{aligned}$$

   is established. If the equation does not hold. The MN is determined to be an illegal user, otherwise, the AP2 authenticates the MN as a legitimate user, and the AP2 sends its own parameters to the MN, so that the MN can authenticates the identity of the AP2.

3) AP2 → MN:

   $Cert_{AP2} \parallel m'_{AP2} \parallel r(1)_{AP2} \parallel s(1)_{AP2} \parallel g^{k'} \parallel T_{Curr}$

   $Cert_{AP2} = (ID_{AP2}, g^{X_{AP2}})$, $g^{X_{AP2}}$ is the public Chameleon hash key of AP2. The AP2 chooses random value $m'_{AP2} \in Z_q^*$ and $k' \in Z_q^*$, and computes $r(1)_{AP2}$, $s(1)_{AP2}$ and $g^{k'}$. Then the AP2 uses the value $g^{X_{MN}}$ and $g^{h_1(pid_j+N_1)}$ from the MN, together with his own parameters, to calculate the session K for communicating with MN. The AP2 can get:

$$K = (g^{h_1(pid_j+N_1)})^{X_{AP2}}(g^{X_{MN}})^{k'}.$$

4) MN ← Blockchain: $C(0)_{AP2}$

AP2 computes:

$$\begin{aligned} & CHAM(m'_{MN}, r(1)_{MN}, s(1)_{MN}) \\ = \; & r(1)_{AP2} - (Y_{AP2}^{e'_{AP2}} g^{s(1)_{AP2}} \bmod p) \bmod q \end{aligned}$$

and compares with the Chameleon hash value of AP2's blockchain certificate $C(0)_{AP2}$ to verify whether

$$\begin{aligned} & CHAM(m_{AP2}, r(0)_{AP2}, s(0)_{AP2}) \\ = \; & CHAM(m'_{AP2}, r(1)_{AP2}, s(1)_{AP2}) \end{aligned}$$

to authenticate the AP2. If the authentication is successful, the MN uses the parameters of the AP2 to calculate the session key for communicating with the AP2. The MN can get:

$$K = (g^{k'})^{X_{MN}}(g^{X_{AP2}})^{h_1(pid_j+N_1)}.$$

In the end, the session key shared between MN and AP2 is:

$$K = g^{h_1(pid_j+N_1)X_{AP2}} g^{k'X_{MN}}.$$

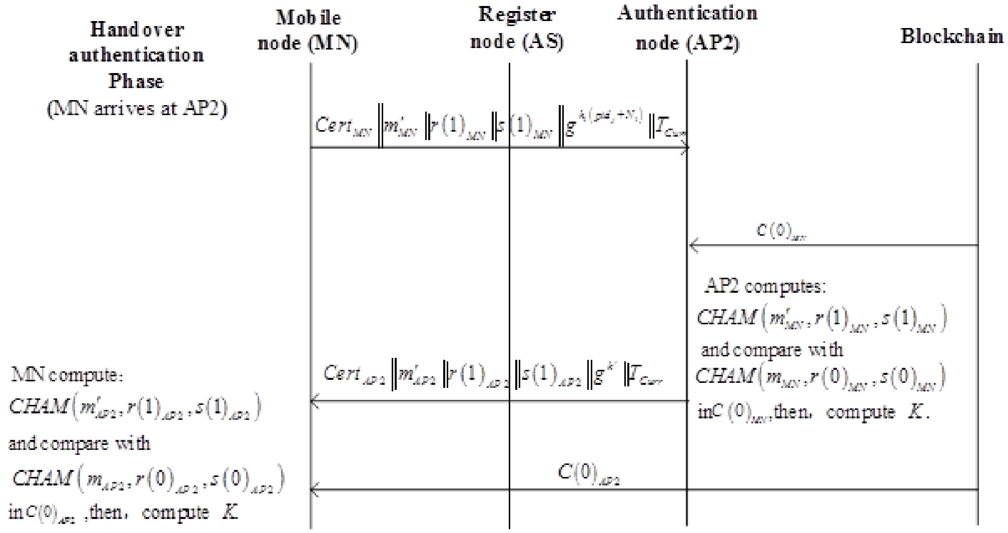
Handover authentication Phase (MN arrives at AP2)
Mobile node (MN)
Register node (AS)
Authentication node (AP2)
Blockchain
$Cert_{MN} \parallel m'_{MN} \parallel r(1)_{MN} \parallel s(1)_{MN} \parallel g^{h_1(pid_j+N_1)} \parallel T_{Curr}$
$C(0)_{MN}$
AP2 computes:
$CHAM(m'_{MN}, r(1)_{MN}, s(1)_{MN})$
and compare with
$CHAM(m_{MN}, r(0)_{MN}, s(0)_{MN})$
in $C(0)_{MN}$, then, compute K.
$Cert_{AP2} \parallel m'_{AP2} \parallel r(1)_{AP2} \parallel s(1)_{AP2} \parallel g^{k'} \parallel T_{Curr}$
MN compute:
$CHAM(m'_{AP2}, r(1)_{AP2}, s(1)_{AP2})$
and compare with
$CHAM(m_{AP2}, r(0)_{AP2}, s(0)_{AP2})$
in $C(0)_{AP2}$, then, compute K
$C(0)_{AP2}$

Figure 5: Handover authentication phase

Finally, when the user no longer has a handover authentication request or needs to quit the system, the current AP node generates the user's revocation block and uploads it to the blockchain. In this way, the revocation operation of the users' blockchain certificate is achieved.

4 Security Analysis and Performance Evaluation

4.1 Security Analysis

4.1.1 Mutual Authentication

Our scheme ensures only the legitimate user to access the wireless network. After the MN is successfully registered, the AS allows the MN to query the data on the blockchain. In a handover authentication phase, after the AP authenticates the identity of the MN, the MN calculates $CHAM(m'_{AP_i}, r(1)_{AP_i}, s(1)_{AP_i})$ by using the value$r(1)_{AP_i}$,$s(1)_{AP_i}$ and m'_{AP_i} provided by the AP, and then the MN authenticates the identity of the AP by querying the blockchain certificate $C(0)_{AP_i}$ on the blockchain. According to this, the mutual authentication between MN and AP is completed.

4.1.2 Conditional Privacy Preservation

The MN obtained the pseudonym set PID from the AS during the Initial Authentication phase. The MN uses different pid instead of the real identity during different handover authentication phase. Since the elements in the PID are unlinkable to each other, when the MN reaches the new AP and uses a new pseudonym, there is no way for APs to collude to trace the MN according to the connection between the pseudonyms. However, in some special cases, the AP can send a request with the pid provided by MN to AS. Upon receiving the request, the AS finds the pseudonym set to which it belongs according to the pid provided by the AP, and the true identity of the MN can be found. Based on this, the conditional privacy protection of user can be achieved.

4.1.3 Key Agreement

During the authentication process, the MN uses his own chameleon hash function public key $g^{X_{MN}}$ and the parameter $g^{h_1(pid_j+N_1)}$ generated by the random number and pid; the AP2 uses his own chameleon hash function public key $g^{X_{AP2}}$ and the parameter $g^{k'}$ generated by the newly selected element to establish a shared session key. In our construction,K can be shared by the MN and AP2, which satisfies $K = g^{h_1(pid_j+N_1)X_{AP2}} g^{k'X_{MN}}$. Moreover, whenever a new round of handover authentication is performed, the MN must choose a new pid to protect its privacy. At the same time, according to key agreement process, since the session key contains the parameter pid, the session key is updated with each new round of handover authentication.

4.1.4 Resistance to Replay Attack

In the process of handoff authentication, an adversary may record the message that the MN send to the AP and replay it. Our scheme uses timestamps, random numbers and PID to prevent replay of previous messages. Since the MN updates his own pid_j at every new round of handover authentication. When the MN performs a verification, the timestamp T_{Curr} will be sent, and the parameter $g^{h_1(pid_j+N_1)}$ also contains a random number N_1. Therefore, if an attacker replays a message to try to enter the system, the AP can detect the replay attack regardless of whether he detects the pid_j, the timestamp T_{Curr}, or the value of $g^{h_1(pid_j+N_1)}$. Accordingly, it is worthless for an adversary to replay messages.

4.1.5 Resistance to Man-in-the-Middle attack

In the process of key agreement between MN and AP2, an adversary may replace the parameters with his generated parameters to obtain information. The attack process implemented by the attacker can be described as Figure 6.

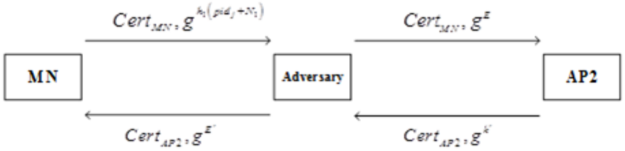

Figure 6: Man-in-the-Middle Attack model

As shown in Figure 6, the adversary E may replace the key parameters to get the session key between the MN and the AP. Upon receiving the parameters, the MN and the AP2 respectively calculate the session key. The key calculated by the MN is $K_1 = g^{h_1(pid_j+N_1)X_{AP2}+E'X_{MN}}$, and the key calculated by the AP2 is $K2 = g^{EX_{AP2}+k'X_{MN}}$. This is not the shared key value they expect, so the MN and the AP2 can not communicates with each other. The adversary will be discovered by the MN and AP2. However, since the attacker does not know the private indexes X_{MN} and X_{AP2} of the MN and the AP2, the attacker cannot calculate either of K_1 or K_2 . It ensures that the MN and the AP2 can be confident that only themselves can calculate the key value shared between them.

4.1.6 Resistance to Passive Eavesdropping Attack

During the process of the handoff authentication, the information that the attacker most desires is the identity of the MN and the the session key K. Firstly, the identity that the MN sends to the AS during the Initial Authentication phase is hashed, which is not available to the eavesdroppers. During the different handover authentication phases, the pid_j in the PID are unlinkable with each other, so the attacker cannot associate the user MN with different pid appearing in different handover authentications. As a result, obtaining the identity of the MN is

Table 2: Security comparisons

protocols	Mutual Authentication	Key Agreement	Conditional Privacy Preservation	Replay Attack	Man-in-the-Middle attack	Passive avesdropping Attack	Perfect forward secrecy
[15]	YES	YES	NO	YES	NO	NO	NO
[13]	YES	YES	YES	YES	YES	YES	YES
[28]	YES	YES	NO	YES	YES	YES	YES
[7]	YES	YES	NO	YES	YES	YES	YES
[11]	YES	YES	NO	YES	NO	NO	NO
Ours	YES	YES	YES	YES	YES	YES	YES

difficult for the attacker. Secondly, if the adversary wants to get the private key X_{MN} and X_{AP2}, then the problem of getting X_{MN} and X_{AP2} from $g^{X_{MN}}$ and $g^{X_{AP2}}$ can be reduced to solve the discrete logarithm problem, and it is difficult to be solved. Therefore, our construction can resist against passive eavesdropping.

4.1.7 Perfect Forward Secrecy

To get the session key $K = g^{h_1(pid_j+N_1)X_{AP2}} g^{k' X_{MN}}$ the adversary has to extract $g^{h_1(pid_j+N_1)X_{AP2}}$ from $g^{h_1(pid_j+N_1)}$ and $g^{X_{AP2}}$, the adversary has to address the CDH problem. Because the CDH problem is hard, the proposed protocol can support the perfect forward secrecy.

4.2 Security Comparisons

According to the requirements of handover authentication in section 2.3 and section 4.1, the comparisons of security properties are listed in Table 2.

4.3 Performance Analysis

In this section, the performance of the proposed protocol is analyzed with some existing schemes. Then, we obtained some conclusions about the efficiency of our scheme.

4.3.1 Computation Overhead

The notations we used in this section are shown in Table 3.

Table 3: The notations used in Efficiency calculation

T_E	Time for executing a modular exponentiation in G_T
T_P	Time for executing a bilinear map operation
T_{ECSM}	Time for executing a scalar multiplication operation
T_H	Time for executing a general hash function

Since the AS node only plays the role of registering and uploading the MN's blockchain certificate to the blockchain in our scheme, we only consider the operations and computational cost required by the MN and AP nodes in the efficiency analysis. In order to prove the efficiency of our scheme, we implement the above operations on a Laptop (Lenovo with Intel I5-3320M 2.60GHz processor, 4G bytes memory and the Windows 7 operating system) using the JPBC library. The time cost of the primitive cryptography operations shown in Table 4.

In the Handover authentication phase of our scheme, the MN and AP2 authenticates each other and negotiates a session key. During this phase, the computation cost of MN is: $5T_E+3T_H \approx 1.038ms$, the computation cost of AP is: $5T_E + T_H \approx 0.946ms$. Furthermore, the computation cost among schemes [7, 13, 15, 28] and ours is analyzed in Table 5 and is compared in Figure 9.

Table 4: Time cost of cryptography operations

	T_E	T_P	T_{ECSM}	T_H
Times(ms)	0.18	8.45	2.013	0.046

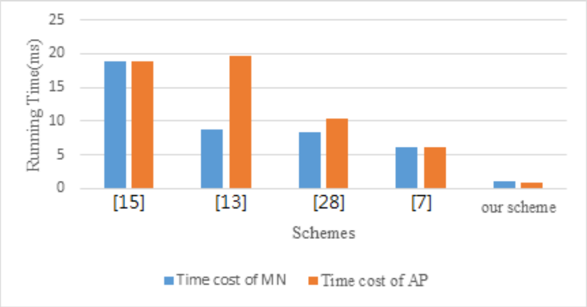

Figure 7: Comparison of the computation cost

And Table 6 shows the energy consumption at the MN (E_{MN}), the energy consumption can be calculated as $E = T_{MN} \times P$, where E is the energy consumption, T_{MN} is the total computation time for handover authentication of MN, and P is the CPU maximum power (35W).

Table 5: Comparison of the computation cost

	MN operations	AP operations
[15]	$T_{ECSM} + 2T_P \approx 18.913ms$	$T_{ECSM} + 2T_P \approx 18.913ms$
[13]	$4T_{ECSM} + 3T_E + 5T_H \approx 8.822ms$	$2T_P + T_{ECSM} + 3T_E + 5T_H \approx 19.683ms$
[28]	$4T_{ECSM} + 5T_H \approx 8.282ms$	$5T_{ECSM} + 5T_H \approx 10.295ms$
[7]	$3T_{ECSM} + 4T_H \approx 6.223ms$	$3T_{ECSM} + 4T_H \approx 6.223ms$
Ours	$5T_E + 3T_H \approx 1.038ms$	$5T_E + T_H \approx 0.946ms$

Table 6: Energy consumption of MN

	[15]	[13]	[28]	[7]	Ours
$E_{MN}(mJ)$	661.955	308.77	289.87	217.805	36.33

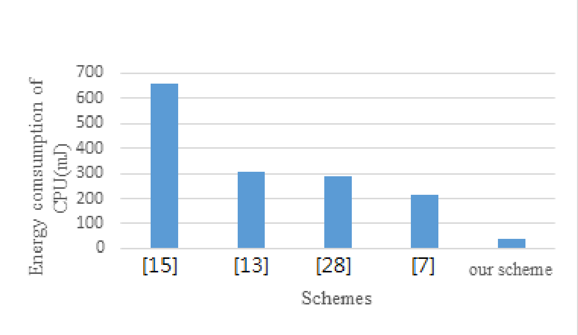

Figure 8: Energy consumption of CPU

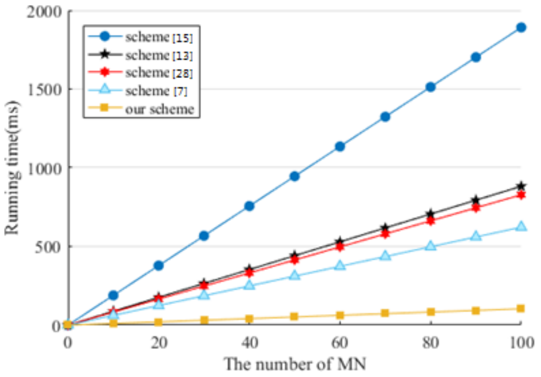

Figure 9: Comparison of handover authentication

4.3.2 Transmission Overhead

For the transmission overhead, it is assumed that the expected authentication message delivery cost between the AP2 and the AAA server is e unit and that between the MN and the AP2 is δ unit, respectively. In our scheme, since we only view the data on the blockchain and do not need it to send us data, we only consider the time consumption between the MN and the AP2. The comparison of the transmission overhead as shown in table 7.

Table 7: Comparison transmission overhead

	[15]	[13]	[9]	Ours
T_{MN-AP2}	3δ	2δ	3δ	2δ
$T_{AP1-AP2}$	0	0	0	0
$T_{AP2-AAA}$	0	0	0	0
T_{tot}	3δ	2δ	3δ	2δ

* T_{MN-AP2} :The transmission cost between the MN and the AP2.

* $T_{AP1-AP2}$:The transmission cost between APs, i.e., AP1 and AP2.

* $T_{AP2-AAA}$:The transmission cost between the AP2 and the AAA server.

* $T_{T_{tot}}$:The total transmission cost.

4.3.3 Communication Overhead

In the proposed handover protocol, two messages correspondence is required for obtaining the handover authentication. In the protocol, the MN transmits $Cert_{MN} \parallel m'_{MN} \parallel r(1)_{MN} \parallel s(1)_{MN} \parallel g^{h_1(pid_j+N_1)} \parallel T_{Curr}$ to the AP2. Hence, the communication overhead incurred from the MN is $(2|p| + 3|q| + l_{id} + l_{time})bits$. The AP2 transmits $Cert_{AP2} \parallel m'_{AP2} \parallel r(1)_{AP2} \parallel s(1)_{AP2} \parallel g^{k'} \parallel T_{Curr}$ to the MN. Hence the generated communication overhead from the AP2 is $(2|p| + 3|q| + l_{id} + l_{time})bits$. According to [13], we know that the proposed protocol increases the communication cost. The reason for the increases is that the MN and the AP2 send $g^{h_1(pid_j+N_1)}$ and $g^{k'}$ to each other for achieving the perfect forward secrecy. It is worthy to achieve the important security attribute at the cost of increasing computation cost only.

Based on the above comparative analysis, it can be seen that our scheme consumes less computation. Our scheme also provides user anonymity and conditional privacy protection. Therefore, our scheme is more suitable for practical application scenarios.

5 Conclusion

In the handover authentication of wireless networks, secure and efficient handover authentication has been the focus of widespread attention. In this paper, we propose a anonymous handover authentication scheme based on chameleon hash function and blockchain technology. The main idea of our scheme is to generate a blockchain certificate for the user by a registration node AS. When the handover authentication occurs, the AP compares the chameleon hash value provided by the user with the blockchain certificate to verify the legal identity of the user. Our scheme provides anonymity and conditional privacy protection.The AP can request the true identity of the MN from the AS when some accidents occurs during the handover authentication phase. When the user no longer has a handover authentication request or needs to log off, the current AP node generates the user's revocation block and uploads it to the blockchain. In this way, the revocation operation of the users' blockchain certificate is achieved. Finally, when the MN performs a new handover authentication to choose a new *pid*, the session key for the secure communication with AP is also updated at the same time. After the analysis of performance, our scheme has the ideal efficiency.

Acknowledgments

This work was supported by the Natural Science Foundation of China under Grants 61802303 and 61772418, the Innovation Ability Support Program in Shaanxi Province of China under Grant 2017KJXX-47, the Natural Science Basic Research Plan in Shaanxi Province of China under Grant 2016JM6033 and 2018JZ6001.

References

[1] G. Ateniese and B. D. Medeiros, "On the key exposure problem in chameleon hashes," in *International Conference on Security in Communication Networks*, pp. 165–179, Sep. 2004.

[2] C. C. Chang, C. Y. Lee, and Y. C. Chiu, "Enhanced authentication scheme with anonymity for roaming service in global mobility networks," *Computer Communications*, vol. 32, no. 4, pp. 611–618, 2009.

[3] C. Chaplin, E. Qi, H. Ptasinski, J. Walker, and S. Li, *802.11i overview, IEEE.802.11–04/0123r1*, 2005. (http://www.drizzle.com/~aboba/IEEE)

[4] J. Choi and S. Jung, "A secure and efficient handover authentication based on lightweight diffie-hellman on mobile node in FMIPv6," *IEICE Transactions on Communications*, vol. 91, no. 2, pp. 605–608, 2008.

[5] J. Choi and S. Jung, "A handover authentication using credentials based on chameleon hashing," *IEEE communications letters*, vol. 14, no. 1, pp. 54–56, 2009.

[6] C. Fromknecht, D. Velicanu, and S. Yakoubov, "Certcoin: A namecoin based decentralized authentication system 6.857 class project," *Unpublished Class Project*, 2014. (https://courses.csail.mit.edu/6.857/2014/files/19-fromknecht-velicann-yakoubov-certcoin.pdf)

[7] S. Gupta, B. L. Parne, and N. S. Chaudhari, "A lightweight handover authentication protocol based on proxy signature for wireless networks," in *The 14th IEEE India Council International Conference (INDICON'17)*, pp. 1–6, July 2017.

[8] S. Gupta, B. L. Parne, and N. S. Chaudhari, "A proxy signature based efficient and robust handover AKA protocol for LTE/LTE-A networks," *Wireless Personal Communications*, vol. 103, no. 3, pp. 2317–2352, 2018.

[9] S. Gupta, B. L. Parne, and N. S. Chaudhari, "Pseh: A provably secure and efficient handover AKA protocol in LTE/LTE-A network," *Peer-to-Peer Networking and Applications*, vol. 12, no. 4, pp. 989–1011, 2018.

[10] S. Gupta, B. L. Parne, and N. S. Chaudhari, "An efficient handover aka protocol for wireless network using chameleon hash function," in *The 4th International Conference on Recent Advances in Information Technology (RAIT'18)*, pp. 1–7, June 2018.

[11] Q. Han, Y. Zhang, X. Chen, H. Li, and J. Quan, "Efficient and robust Identity-Based handoff authentication in wireless networks," in *International Conference on Network and System Security*, pp. 180–191, 2012.

[12] D. He, M. Ma, Y. Zhang, C. Chen, and J. Bu, "A strong user authentication scheme with smart cards for wireless communications," *Computer Communications*, vol. 34, no. 3, pp. 367–374, 2011.

[13] D. He, D. Wang, Q. Xie, and K. F. Chen, "Anonymous handover authentication protocol for mobile wireless networks with conditional privacy preservation," *Science China Information Sciences*, vol. 60, no. 5, pp. 052104, 2017.

[14] H. C. Hsiang and W. K. Shih, "Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment," *Computer Standards & Interfaces*, vol. 31, no. 6, pp. 1118–1123, 2009.

[15] Y. Kim, W. Ren, J. Jo, M. Yang, Y. Jiang, and J. Zheng, "SFRIC: A secure fast roaming scheme in wireless lan using ID-based cryptography," in *IEEE International Conference on Communications*, pp. 1570–1575, June 2007.

[16] H. Krawczyk and T. Rabin, *Chameleon Hashing and Signatures*, Aug. 2000. US Patent 6,108,783.

[17] K. Lewison and F. Corella, *Backing Rich Credentials with a Blockchain PKI*, 2016. (https://pomcor.com/techreports/BlockchainPKI.pdf)

[18] C. T. Li and C. C. Lee, "A novel user authentication and privacy preserving scheme with smart cards for

wireless communications," *Mathematical and Computer Modelling*, vol. 55, no. 1-2, pp. 35–44, 2012.

[19] Y. P. Liao and S. S. Wang, "A secure dynamic ID based remote user authentication scheme for multi-server environment," *Computer Standards & Interfaces*, vol. 31, no. 1, pp. 24–29, 2009.

[20] C. Ma, K. Xue, and P. Hong, "A proxy signature based re-authentication scheme for secure fast handoff in wireless mesh networks," *International Journal Network Security*, vol. 15, no. 2, pp. 122–132, 2013.

[21] A. Mishra, M. H. Shin, and W. A. Arbaugh, "Proactive key distribution using neighbor graphs," *IEEE Wireless Communication Magazine*, vol. 11, no. 1, pp. 26–36, 2004.

[22] S. Pack and Y. Choi, "Fast handoff scheme based on mobility prediction in public wireless lan systems," *IEE Proceedings of Communications*, vol. 151, no. 5, pp. 489–495, 2004.

[23] M. Ramadan, F. Li, C. X. Xu, and A. Mohamed, "User-to-user mutual authentication and key agreement scheme for LTE cellular system," *International Journal Network Security*, vol. 18, no. 4, pp. 769–781, 2016.

[24] N. Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008. (`https://bitcoin.org/bitcoin.pdf`)

[25] C. Tang and L. Gao, "Multi-parties key agreement protocol in block chain," *Netinfo Security (in Chinese)*, vol. 12, no. 9, pp. 19, 2017.

[26] W. T. Tsai, L. Yu, and R. Wang, "Blockchain application development techniques," *Journal of Software (in Chinese)*, vol. 28, no. 6, pp. 1474–1487, 2017.

[27] H. Wang and A. R. Prasad, "Fast authentication for inter-domain handover," in *Telecommunications and Networking (ICT'04)*, pp. 973–982, Aug. 2004.

[28] Y. Xie, L. Wu, N. Kumar, and J. Shen, "Analysis and improvement of a privacy-aware handover authentication scheme for wireless network," *Wireless Personal Communications*, vol. 93, no. 2, pp. 523–541, 2017.

[29] T. Y. Youn, Y. H. Park, and J. Lim, "Weaknesses in an anonymous authentication scheme for roaming service in global mobility networks," *IEEE Communications Letters*, vol. 13, no. 7, pp. 471–473, 2009.

[30] C. Zhang, R. Lu, P. Ho, and A. Chen, "A location privacy preserving authentication scheme in vehicular networks," in *IEEE Wireless Communications and Networking Conference*, Apr. 2008. DOI: 10.1109/WCNC.2008.447.

Biography

ChenCheng Hu received the B.Eng. degree from the Xi'an University of Posts and Telecommunications, in 2016, where he is currently pursuing the M.S. degree. He is doing research at the National Engineering Laboratory for Wireless Security. His current research interests include blockchain technology, user authentication, and information security.

Dong Zheng received the Ph.D. degree from Xidian University, in 1999. He joined the School of Information Security Engineering, Shanghai Jiao Tong University. He is currently a Professor with the Xi'an University of Posts and Telecommunications, China. His research interests include information theory, cryptography, and information security. He is also a Senior Member of the Chinese Association for Cryptologic Research and a member of the Chinese Communication Society.

Rui Guo received the Ph.D. degree from the State Key Laboratory of Networking and Switch Technology, Beijing University of Posts and Telecommunications, China, in 2014. He is currently a Lecturer with the National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications. His current research interests include attribute-based cryptograph, cloud computing, and blockchain technology.

Axin Wu received B.S. degree from Zhengzhou University of Light Industry in 2016. Since 2016, he is currently in M.Eng program in Xi'an University of Post and Telecommunications, Xi'an, China. His research interests include cloud security and wireless network security.

Liang Wang received the B.S. degree from the Institute of Information Technology, GUET, in 2016. He is currently pursuing the M.S. degree with the National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, China. His research interests include anonymous authentication, vehicular ad hoc networks, and blockchain.

ShiYao Gao received the B.S. degree from the Xi'an University of Posts and Telecommunications, in 2017. She is currently pursuing the M.S. degree with the Xi'an University of Posts and Telecommunications, China. She is doing research at the National Engineering Laboratory for Wireless Security. Her research interests include blockchain technology, electronic voting, and information security.