Hindawi
Security and Communication Networks
Volume 2020, Article ID 2637916, 19 pages
https://doi.org/10.1155/2020/2637916

Research Article

A Lattice-Based Authentication Scheme for Roaming Service in Ubiquitous Networks with Anonymity

Yousheng Zhou [1,2] and Longan Wang [2]

[1] *College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China*
[2] *School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing 400065, China*

Correspondence should be addressed to Yousheng Zhou; zhouys@cqupt.edu.cn

Received 22 October 2019; Revised 16 May 2020; Accepted 23 May 2020; Published 28 June 2020

Academic Editor: Mamoun Alazab

In the ubiquitous networks, mobile nodes can obtain roaming service that enables them to get access to the services extended by their home networks in the field of foreign network. To provide secure and anonymous communication for legal mobile users in roaming services, there should be a mutual authentication between mobile user and foreign agent with the help of home agent. There are many roaming authentication schemes which have been proposed; however, with the progress of quantum computation, quantum attack poses security threats to many traditional public key cryptography-based authentication schemes; thus, anti-quantum attack roaming authentication schemes need to be investigated. On account of the limitation of computational resources for mobile nodes, a lightweight anonymous and antiquantum authentication schemes need to be developed to enable mobile nodes to roam across multiple service domains securely and seamlessly. In consideration of the advantages of lattice in anti-quantum, an NTRU-based authentication scheme with provable security and conditional privacy preservation is proposed to remedy these security weaknesses. Compared with the existing scheme, the proposed scheme not only improves efficiency but also can resist the quantum attack.

1. Introduction

With the advance of the wireless Internet access technology [1] and the popularity of smart mobile devices, the ubiquitous network has been widely used in our daily life, providing people with a more convenient life. Ubiquitous network enables people to access network services, such as online shopping and mobile payment. However, the mobile device is prone to suffer from various security and privacy challenges in ubiquitous network environment due to its inherent openness and computation limitation. For instance, an attacker can intercept the transmission data, and then analyze or tamper these data, which would cause user data pollution and privacy leakage [2].

Authentication is an essential security technique to prevent attacker in roaming service of ubiquitous network, and great efforts have been made in this field in the past years. However, most of the existing authentication schemes [3–23] are built using conventional cryptographic approaches. It is widely believed that such primitives cannot resist to quantum attack. For instance, discrete logarithm problems and factorization problems can be resolved using the polynomial time algorithm proposed by Shor [24]. In addition, the computation cost or communication cost of the existing authentication scheme are relatively high, which makes many of these schemes not practical for the wireless network since most of them are equipped with resource-constrained devices [25–29]. Therefore, it is of great significance to design efficient and antiquantum roaming authentication schemes. However, the openness of ubiquitous network and dynamic nature makes it extremely challenging to design a secure and effective roaming authentication protocol.

1.1. Related Work. In recent years, many roaming authentication protocols [5–23, 30–36] have been proposed to achieve secure information acquisition for mobile users with smart card in the ubiquitous network. In 2004, a roaming authentication protocol for the ubiquitous network was proposed by Zhu and Ma [5], which aims to preserve the privacy of mobile users. However, Lee et al. [6] proved that Zhu and Ma [5] fails to provide backward security and cannot resist forgery attack. To eliminate these defects, an improved roaming authentication protocol was proposed by Lee et al. [6]. Later, Wu et al. [7] pointed out that the anonymity of users cannot be preserved in the protocols of Zhu and Ma [5] and Lee et al. [6], while the latter also fails to guarantee backward security. In addition, to remedy the shortcomings the abovementioned, Wu et al. [7] proposed an improved scheme. In 2012, Mun et al. [8] demonstrated that the user anonymity and perfect forward security have not been achieved in Wu et al. [7], and then they proposed an enhanced authentication protocol to remedy these weaknesses. Unfortunately, Kim and Kwak [9] found that Mun et al. [8] is vulnerable to replay attacks and man-in-middle attacks. In addition, Zhao et al. [10] also pointed out that Mun et al. [8] is vulnerable to various attacks.

In 2011, a lightweight anonymous authentication protocol was proposed by He et al. [11] for roaming service. However, in 2013, Jiang et al. [12] showed that He et al. [11] cannot resist various attacks such as offline password guessing and replay attacks. To address these problems, they proposed an enhanced anonymous authentication scheme. Wen et al. [13] subsequent study shows that Jiang et al. [12] is vulnerable to replay attacks and cannot provide forward security. In 2014, an authentication scheme based on elliptic curve was proposed by Kuo et al. [14] to achieve anonymity. However, Lu et al. [15] proved that the protocol of Kuo et al. [14] has many security problems, such as the vulnerability from internal attacks, and Zhang et al. [21] also found that Kuo et al. [14] may cause the leakage of the secret value of mobile terminal MU. Subsequently, Xu et al. [22] and Srinivas [23] pointed out that Zhang et al. [21] is vulnerable to offline guessing attacks and replay attacks and cannot guarantee the anonymity of users.

In 2015, Farash et al. [16] pointed out that the scheme of Wen et al. [13] is vulnerable to offline guessing attack and forgery attack. And then, Farash et al. [16] and Gope and Hwang [17], respectively, proposed enhanced anonymous roaming authentication schemes to resist various attacks in ubiquitous networks. However, Wu et al. [18] showed that there are many security defects in Farash et al. [16] and Gope and Hwang [17], and the session keys of their schemes can be exposed to HA. In addition, Chaudhry et al. [19] also pointed out some security risks in Farash et al. [16], such as the inability to guarantee user anonymity and the leakage of mobile user session key. In 2017, Xie et al. [35] designed a first roaming authentication scheme which takes the advantage of the chaotic maps for key agreement in ubiquitous network. Subsequently, in 2019, Ostad-Sharif et al. [33] found that Xie et al. [35] cannot resist the known session-specific information attack. In 2018, Lee et al. [20] claimed that Chaudhry et al. [19] is vulnerable to many attacks such as user forgery attacks and device theft attacks [37–40]. Then, Lee et al. [20] proposed an improved biometric-based [40, 41] authentication scheme for roaming in ubiquitous networks. They claimed that their scheme is secure against the various known attacks with conditional anonymous [37, 39, 42–46] and is lightweight compared with the earlier scheme. In 2019, Lu et al. [34] found some weaknesses in Gope and Hwang [36] authentication scheme for roaming users and proposed a new roaming user authentication scheme using ECC and claimed that their proposal extends required security features and resists known attacks. Very recently, in 2020, Alzahrani et al. [31] show that the roaming scheme in Lu et al. [34] cannot protect the remote user against Stolen Verifier and Traceability attacks. Then, Alzahrani et al. [31] proposed an improved scheme based on ECC which is designed under the proposal of Lu et al. [34]. However, in the same year, Khatoon and Singh Thakur [32] found that Lee et al. [20] is vulnerable offline dictionary attack, replay attack, etc.

Lattice is a promising tool to develop various post-quantum cryptography schemes, which has been put forward for a long time. In 1997, the first lattice-based cryptosystem constructed by Ajtai and Dwork [47] appeared, followed by the NTRU cryptosystem constructed by Hoffstein [48] in 1998. In 2009, Gentry [49] constructed the first fully homomorphic cryptography scheme based on lattice cryptography. In 2015, the postquantum cryptography report [30] released by the national institute of standards and technology of the United States pointed out that, owing to the rapid development of quantum computing technology, the existing public key cryptography standard will no longer be safe under quantum computing. As early as 1997, Shor [24] proposed a quantum algorithm to solve the large number factorization problem in polynomial time; therefore, many conventional cryptosystems, for instance, those based on large integer factorization and discrete logarithm assumption, would face great security challenges with the advance of quantum computation.

In recent years, many authentication protocols from lattices have been developed [28, 47–62]. Specially, many lattice-based key exchange protocols have been proposed [53–57] and some of them have been used by Microsoft and Google [62] as alternatives to the prequantum key agreements in the TLS handshake protocol, which means that lattice-based key exchange protocols can be practical in many contexts and offer credible alternatives to schemes such as ECDH.

However, these existing lattice-based key exchange protocols [47, 63–66] are unsuitable to wireless environment with limited resources since they are built from LWE or RLWE. NTRU, first proposed by Hoffstein [48], is a lightweight public key encryption algorithm. When compared with other public key encryption mechanism, NTRU possesses more distinct advantages such as cheap memory and computation consumption, fast speed of encryption/decryption [48], and signature/verification [59]. NTRU has been widely used in wireless environment such as wireless sensor networks [28], cellular networks [60, 61], and opportunistic networks [58] due to its low computational cost.

Therefore, it is a desirable tool to construct roaming authentication scheme for ubiquitous network.

1.2. Motivation and Contributions. Although many authentication schemes have been proposed, a promotion in security and performance remains a challenge to develop a practical authentication for roaming services in ubiquitous networks. Furthermore, the potential threat of quantum attack makes it necessary to develop efficient antiquantum attack roaming authentication protocols. Motivated by this, a novel roaming authentication scheme based on NTRU is proposed in this paper. Our contributions are as follows:

(1) We put forward an NTRU-based authentication scheme with conditional anonymity for mobile users to roaming securely in ubiquitous network, the most significant merit of which is antiquantum attack

(2) Formal and informal security analysis is conducted for the proposed scheme to demonstrate that it can meet all security requirements

(3) Furthermore, we perform the comparisons in terms of the computational and communication cost to show the feasibility and efficiency of the proposed scheme

1.3. Organization. The rest of this paper is organized as follows. Section 2 introduces the basic knowledge of lattice and the NTRU public key encryption algorithm. Section 3 illustrates the scheme in detail. Section 4 presents the formal security proof for the proposed scheme. The comparison of performance and security characteristics of the proposed scheme are given in Section 5, and the paper is concluded in Section 6.

2. Preliminaries

In Section 2, we will briefly introduce the basic knowledge of lattice cryptography [50] and NTRU public key encryption algorithm [48].

2.1. Lattice

Definition 1. Given n linearly independent vectors $b_1, b_2, \ldots, b_n \in R^m$, the lattice generated by them is defined as follows:

$$\mathscr{L}(b_1, b_2, \ldots, b_n) = \left\{\sum x_i b_i \mid x_i \in \mathbb{Z}\right\}. \tag{1}$$

We say that the rank of the lattice is n and its dimension is m and $b_1, b_2, \ldots, b_n$ as a basis of the lattice. If we define B as $m \times n$ matrix whose columns are $b_1, b_2, \ldots, b_n$, then the lattice generated by B is

$$\mathscr{L}(B) = \left\{\sum Bx \mid x_i \in \mathbb{Z}^n\right\}. \tag{2}$$

(1) In equation (2), Bx stands for ordinary matrix multiplication.

(2) Lattice is a discrete additive group of R^m, closed under addition operation, and there is space between points.

Definition 2 (the shortest vector problem (SVP)). Given a lattice basis $B \in Z^{m\times n}$, to find a nonzero lattice vector $Bx\,(x \in Z^n\{0\})$, so for all $y \in Z^n\backslash\{0\}$ such that $\|Bx\| \le \|By\|$.

Definition 3 (the closest vector problem (CVP)). Given a lattice basis $B \in Z^{m\times n}$ and a target vector $t \in Z^m$, to find a lattice vector Bx that close to the target vector t, so for all $y \in Z^n$ such that $\|Bx - t\| \le \|By - t\|$.

Both the CVP and the SVP are difficult computational problems; the two are interchangeable with the same difficulty, and there is no effective algorithm to solve these two problems.

2.2. NTRU

2.2.1. Definition of Algorithm

Definition 4 (polynomial ring). A polynomial with respect to x over a ring R has a form, $a_0 + a_1x + a_2x^2 + \cdots + a_{N-1}x^{N-1}$, $a_i \in R$. A ring formed by a set of these polynomials is called a polynomial ring, denoted as $R[x]$, simply R for short.

The parameters of NTRU mainly include three integers (N, p, q) and four integer coefficient polynomial sets $\mathscr{L}_f$, $\mathscr{L}_g$, $\mathscr{L}_r$, and $\mathscr{L}_m$ with $n-1$ dimension, p and q are not required as prime numbers, while they should satisfy the equation $\gcd(p, q) = 1$, and q is greater than p. Definite polynomial $R = Z[X]/(X^N - 1)$, if $f \in R, f$ can be denoted as $f = \sum_{i=0}^{N-1} f_i x^i = [f_0, f_1, \ldots, f_{N-1}]$. Definite $\odot$ is multiplication operation over polynomial ring; if $f \in R$, $g \in R$, and $f \odot g = h$, then

$$h_k = \sum_{i=0}^{k} f_i g_{k-i} + \sum_{i=k+1}^{n-1} f_i g_{n+k-i} = \sum_{i+j\equiv k \bmod n} f_i g_j. \tag{3}$$

Definition 5 (truncated polynomial ring). The system $(R, +, \odot)$ consists of the convolution operations defined above, and the addition operations in ordinary polynomial rings are called the truncated polynomial ring.

The polynomial ring used in NTRU is truncated polynomial ring, denoted as R, and R_q is polynomial ring of modular q. When performing the product result $\bmod\, q$, we reduce all the polynomial coefficients by $\bmod\, q$, so the result is in the ring $Z[X]/(q, X^N - 1)$.

2.2.2. Key Creation. The two communication parties are Bob and Alice. To generate a key, Bob randomly chooses two polynomials $f \in \mathscr{L}_f$ and $g \in \mathscr{L}_g$; the polynomial f should have inverses modulo and modulo p, and we will write these inverses as f_q^{-1} and f_p^{-1}:

$$\begin{aligned} f_q^{-1} \odot f &\equiv 1 \bmod q, \\ F_p^{-1} \odot f &\equiv 1 \bmod p. \end{aligned} \tag{4}$$

Then, Bob computes the public key $h \equiv p f_q^{-1} \odot g \bmod q$, and the private key pair of Bob is (f, f_p^{-1}).

2.2.3. Encryption. Alice chooses her plaintext m from the set $\mathscr{L}_m$ and a random polynomial r from $\mathscr{L}_r$; then, she uses Bob's public key h to encrypt the message $e \equiv r \odot h + m \bmod q$ and sends it to Bob. In addition, in order to strengthen the feasibility and security of the scheme, this scheme adopts the encryption security enhancement variant proposed by Hoffstein and Silverman [51].

2.2.4. Decryption. Bob uses his private key f to decrypt the encrypted message e from Alice. Firstly, Bob computes the intermediate polynomial a by

$$\begin{aligned} a &= f \odot e \bmod q, \\ &= f \odot r \odot h + f \odot m \bmod q, \\ &= pr \odot g + f \odot m \bmod q. \end{aligned} \tag{5}$$

The coefficients of a are in the interval $[-q/2, q/2]$. Then, a is used for modulus p operation. Finally, Bob uses his private key f_p^{-1} multiply polynomial to recover the plaintext:

$$m = f_p^{-1} \odot a \bmod p. \tag{6}$$

In order to reduce the decryption time and speed up the decryption operation [51, 52], we set $f = 1 + pF$. Then, Bob can decrypt plaintext m successfully after computing $m = a \bmod p$.

2.2.5. Parameter Choices. Message space $\mathscr{L}_m$ is composed of polynomial of modular p, where $m = m_0 + m_1 x + \cdots + m_{N-1} x^{N-1} \bmod p$ and

$$\mathscr{L}_m = \left\{ m \in R\colon m_i \subseteq \left[-\frac{p-1}{2}, \frac{p-1}{2} \right] \right\}. \tag{7}$$

Similarly, other sample spaces can be described in the following way:

$$\begin{aligned} \mathscr{L}_{(d_1,d_2)} = \{ f \in R\colon\ & f \text{ has } d_1 \text{ coeffcients equal } 1, \\ & d_2 \text{ coefficients equal } -1, \text{ the rest } 0 \}. \end{aligned} \tag{8}$$

We choose three positive integers d_f, d_r, and d_g and then we use these symbols to denote polynomial f, g, r: $\mathscr{L}_f = \mathscr{L}(d_f, d_f - 1)$, $\mathscr{L}_g = \mathscr{L}(d_g, d_g)$, and $\mathscr{L}_r = \mathscr{L}(d_r, d_r)$

Since f is expected to be invertible, the number of -1 should not equal the number of 1.

3. Concrete Construction

3.1. System Model. This section illustrates the concrete construction of the proposed authentication scheme for mobile user roaming in ubiquitous network. Ubiquitous network provides roaming services for mobile users, enabling them to obtain extended services of home agents whenever they enter into a foreign agent field, no matter where they are [8–10]. In the proposed scheme, there are three types of entities:

(1) MU (mobile user): uses mobile phone with smart card to get services in ubiquitous network

(2) FA (foreign agent): provides roaming services for mobile users

(3) HA (home agent): provides authentication for MU and FA

When a mobile user (MU) enters the foreign agent area, MU should be authenticated under the collaboration between the home agent and the foreign agent. A general framework of roaming service is shown in Figure 1. MU has to register itself during the initialization of the system. Afterwards, with the help of HA, MU and FA can perform mutual authentication when necessary. Only when MU and FA confirm each other's identities can they communicate with each other. In order to ensure the identity legitimacy of the involved entities and the message validity, a mutual authentication mechanism is designed to achieve authorization when realizing roaming service, and the message security is satisfied through key agreement protocol [3, 4, 25].

We describe the proposed protocol in ubiquitous networks as follows. Please refer to Table 1 for notation guide.

3.2. Registration. Home agent (HA) mainly authenticates the real identity of roaming mobile user (MU) and the identity of foreign agent (FA) and then sends the authentication results to FA and MU, respectively. Therefore, a mobile phone user must register himself with his home agent before roaming. Figure 2 shows the registration stage of the proposed scheme, and the main steps of registration are as follows:

(1) HA broadcasts public parameters $\{p, q, n, h_{\mathrm{HA}}\}$ and then calculates and sends his public key to registered MU, where h_{HA} is HA's public key

(2) MU randomly selects a random number λ and a legal login password $\mathrm{PW}_{\mathrm{MU}}$; then, MU computes $H_{\mathrm{MU}} = H_1(\mathrm{ID}_{\mathrm{MU}} \| \mathrm{PW}_{\mathrm{MU}} \| \lambda)$ and $f_{\mathrm{MU}.q}^{-1} \cdot g_{\mathrm{MU}} = h_{\mathrm{MU}}$ and then sends $\{\mathrm{ID}_{\mathrm{MU}}, H_{\mathrm{MU}}, h_{\mathrm{MU}}, \lambda\}$ to HA through a secure channel

(3) After receiving the registration request from MU, HA verifies the user identity $\mathrm{ID}_{\mathrm{MU}}$ first; if the verification holds, then compute the identification of MU $\mathrm{IM} = H_1(H_{\mathrm{MU}} \| f_{\mathrm{HA}} \| t_{\mathrm{HA}})$, t_{HA} is the timestamp of MU registration, and no one except HA can forge or calculate IM. Then, HA stores parameters $\{H_{\mathrm{MU}}, \lambda, \mathrm{IM}, h_{\mathrm{MU}}, p, q, n, H(\cdot)\}$ into the smart card and assigns the smart card to MU.

Assume that a symmetric key has been previously shared between the home agent and the foreign agent, and each home agent has a list of public keys corresponding to ID. Home agent (HA) has a list of public and private keys for relative roaming user (MU), see Table 2. Home agent (HA)

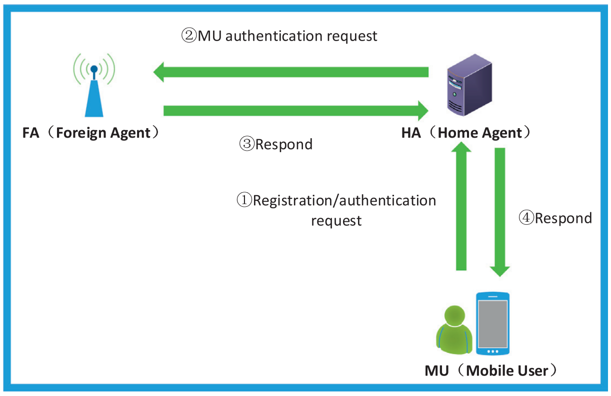

②MU authentication request
FA（Foreign Agent）
③Respond
HA（Home Agent）
①Registration/authentication request
④Respond
MU（Mobile User）

Figure 1: The scenario of roaming authentication in ubiquitous networks.

Table 1: Notations and definition.

Notation	Definition
n	Dimensions of polynomial rings in NTRU
p	A small positive prime integer, usually 2 or 3
q	A positive integer used to reduce the coefficients of polynomial
$H_1, 1 \in 1.2, 3, 4$	One-way hash function
ID_i	The true identity of communication entity i
SID	The anonymous identity of MU
IM	The identification of MU
$\mathscr{L}_f$	Set of polynomials f over $\mathbb{Z}[X]/x^{n-1}$
$\mathscr{L}_g$	Set of polynomials g over $\mathbb{Z}[X]/x^{n-1}$
$\mathscr{L}_r$	Set of polynomials z over $\mathbb{Z}[X]/x^{n-1}$
$f_{i,q}^{-1}$	Inverse of polynomial $f_{i,q}$
$f_{i,p}^{-1}$	Inverse of polynomial $f_{i,p}$
h_i	The public key of communication entity i
$f_{i,q}$	The polynomial over $\mathbb{Z}[X]/(q, x^{n-1})$
$f_{i,p}$	The polynomial over $\mathbb{Z}[X]/(p, x^{n-1})$
r_i	The random polynomial chosen from $\mathscr{L}_r$
SK_{ij}	The session key of communication entity i and j

has a list of public and private keys for foreign agent (FA), see Table 3.

3.3. Login and Authentication Phase. As shown in Figure 3, when the mobile terminal completes the registration, it can perform the login and authentication process. In this process, the mobile terminal completes the negotiation of the session key and authentication with the foreign agent with the help of the local agent:

(1) MU $\longrightarrow$ FA: $m_1 = \{\mathrm{SID}, h_0, V_1, V_2, t_{\mathrm{MU}}, \mathrm{ID}_{\mathrm{HA}}\}$

The mobile user MU first enters its real identity $\mathrm{ID}_{\mathrm{MU}}$ and password $\mathrm{PW}_{\mathrm{MU}}$ into the smart card; then, the smart card computes and verifies $H'_{\mathrm{MU}} = H_1(\mathrm{ID}_{\mathrm{MU}} \| \mathrm{PW}_{\mathrm{MU}} \| \lambda)$; if the verification holds, then the ID of MU is valid; smart card allows user to login in; otherwise, the smart card denies the user login request. MU selects two random polynomials r_{MU} and x_{MU}, computes $\mathrm{SID} = H_4(\mathrm{ID}_{\mathrm{MU}} \| x_{\mathrm{MU}} \| \mathrm{IM} \| t_{\mathrm{MU}})$, then encrypts $\mathrm{ID}_{\mathrm{MU}}$ and x_{MU}, $V_1 = p \cdot h_{\mathrm{HA}} \cdot r_{\mathrm{MU}} + \mathrm{ID}_{\mathrm{MU}}$, $V_2 = V_1 \cdot \mathrm{ID}_{\mathrm{MU}} + x_{\mathrm{MU}}$, and $h_0 = H_2(\mathrm{ID}_{\mathrm{MU}} \| \mathrm{IM} \| t_{\mathrm{MU}} \| x_{\mathrm{MU}})$, computes $h_0 = H_2(\mathrm{ID}_{\mathrm{MU}} \| \mathrm{IM} \| t_{\mathrm{MU}} \| x_{\mathrm{MU}})$, and then sends $\{\mathrm{SID}, h_0, V_1, V_2, t_{\mathrm{MU}}, \mathrm{ID}_{\mathrm{HA}}\}$ to FA.

(2) FA $\longrightarrow$ HA: $m_2 = \{m_1, \mathrm{ID}_{\mathrm{FA}}, \mathrm{MAC}, t_{\mathrm{FA}}\}$

When FA receives m_1, it first verifies whether the timestamp is valid. If so, it saves SID first and retrieves the locally stored shared secret key $\mathrm{SK}_{\mathrm{FH}}$ with HA according to $\mathrm{ID}_{\mathrm{HA}}$, then computes $\mathrm{MAC} = H_2(\mathrm{ID}_{\mathrm{FA}} \| V_1 \| V_2 \| \mathrm{SK}_{\mathrm{HF}})$, and sends $m_2 = \{m_1, \mathrm{ID}_{\mathrm{FA}}, \mathrm{MAC}, t_{\mathrm{FA}}\}$ to HA.

(3) HA $\longrightarrow$ FA: $m_3 = \{h_2, V_3, V_4, h_{\mathrm{MU}}\}$

When HA receives the message m_2 from FA, HA verifies the timestamp first and then verifies the validity of $\mathrm{ID}_{\mathrm{FA}}$ and SID:

(1) HA calculates the message verification code $\mathrm{MAC}' = H_2(\mathrm{ID}_{\mathrm{FA}} \| V_1 \| V_2 \| K_{\mathrm{HF}} \| t_{\mathrm{FA}})? = \mathrm{MAC}$ according to $\mathrm{SK}_{\mathrm{HF}}$ stored in HA and verifies if the equation holds or not; if it holds then HA believes $\mathrm{ID}_{\mathrm{FA}}$ is legal.

(2) HA uses his private key to decrypt V_1 and V_2 to obtain x_{MU} and $\mathrm{ID}_{\mathrm{MU}}$, then uses $\mathrm{ID}_{\mathrm{MU}}$ to find IM stored in HA, and verifies $h'_0 = H_2(\mathrm{ID}_{\mathrm{MU}} \| \mathrm{IM} \| t_{\mathrm{MU}} \| x_{\mathrm{MU}})? = h_0$ and $\mathrm{SID}' = H_4(\mathrm{ID}_{\mathrm{MU}} \| x_{\mathrm{MU}} \| \mathrm{IM} \| t_{\mathrm{MU}})$; if all equation hold, then HA believes SID is valid.

(3) HA selects a random polynomial $r_{\mathrm{HA}} \in \mathscr{L}_r$, computes $h_1 = H_1(\mathrm{IM} \| x_{\mathrm{MU}} \| \mathrm{ID}_{\mathrm{FA}})$, $V_3 = p \cdot h_{\mathrm{FA}} \cdot r_{\mathrm{HA}} + h_1$, $V_4 = V_3 \cdot h_1 + x_{\mathrm{MU}}$, and then sends $m_3 = \{h_2 = H_2(h_1 \| \mathrm{SID} \| h_{\mathrm{MU}} \| \mathrm{SK}_{\mathrm{HF}}), V_3, V_4\}$ to FA.

(4) FA $\longrightarrow$ MU: $m_4 = \{h_3, V_5, V_6\}$

After receiving m_3 from HA, FA decrypts V_3 and V_4 and computes $h'_2 = H_2(h_1 \| \mathrm{SID} \| h_{\mathrm{MU}} \| \mathrm{SK}_{\mathrm{HF}})? = h_2$ to verify whether the anonymous identity SID of MU received from HA is equal to SID received in step 1. If it holds, FA believes MU's anonymous identity SID is legitimate. FA selects two random polynomials, then computes $K_{\mathrm{FM}} = x_{\mathrm{FA}} \cdot x_{\mathrm{MU}}$, computes session key $\mathrm{SK}_{\mathrm{FM}} = H_3(\mathrm{SID} \| K_{\mathrm{FM}} \| \mathrm{ID}_{\mathrm{FA}})$, then encrypts h_1 and x_{FA} uses equation $V_5 = p \cdot h_{\mathrm{MU}} \cdot r_{\mathrm{FA}} + h_1$, $V_6 = h_1 \cdot V_5 + x_{\mathrm{FA}}$, and finally sends $m_4 = \{h_3 = H_2(\mathrm{SID} \| h_1 \| \mathrm{SK}_{\mathrm{FM}} \| x_{\mathrm{FA}}), V_5, V_6\}$ to MU.

(5) After receiving m_4 from FA, MU obtains h_1 and x_{FA} from decrypting V_5 and V_6 and verifies $h'_1 = H_1(\mathrm{IM} \| x_{\mathrm{MU}} \| \mathrm{ID}_{\mathrm{FA}})? = h_1$; if it holds, MU trusts the legitimacy of FA. Then, computes $K_{\mathrm{MF}} = x_{\mathrm{MU}} \cdot x_{\mathrm{FA}}$ and the session key $\mathrm{SK}_{\mathrm{MF}} = H_3(\mathrm{SID} \| K_{\mathrm{MF}} \| \mathrm{ID}_{\mathrm{FA}})$. MU verifies $h'_3 = H_2$ in the end; if the equation holds, then the session key negotiation is successful.

To facilitate the understanding of the proposed protocol, the following three steps will describe the calculation process of public key generation, decryption, and key agreement in detail.

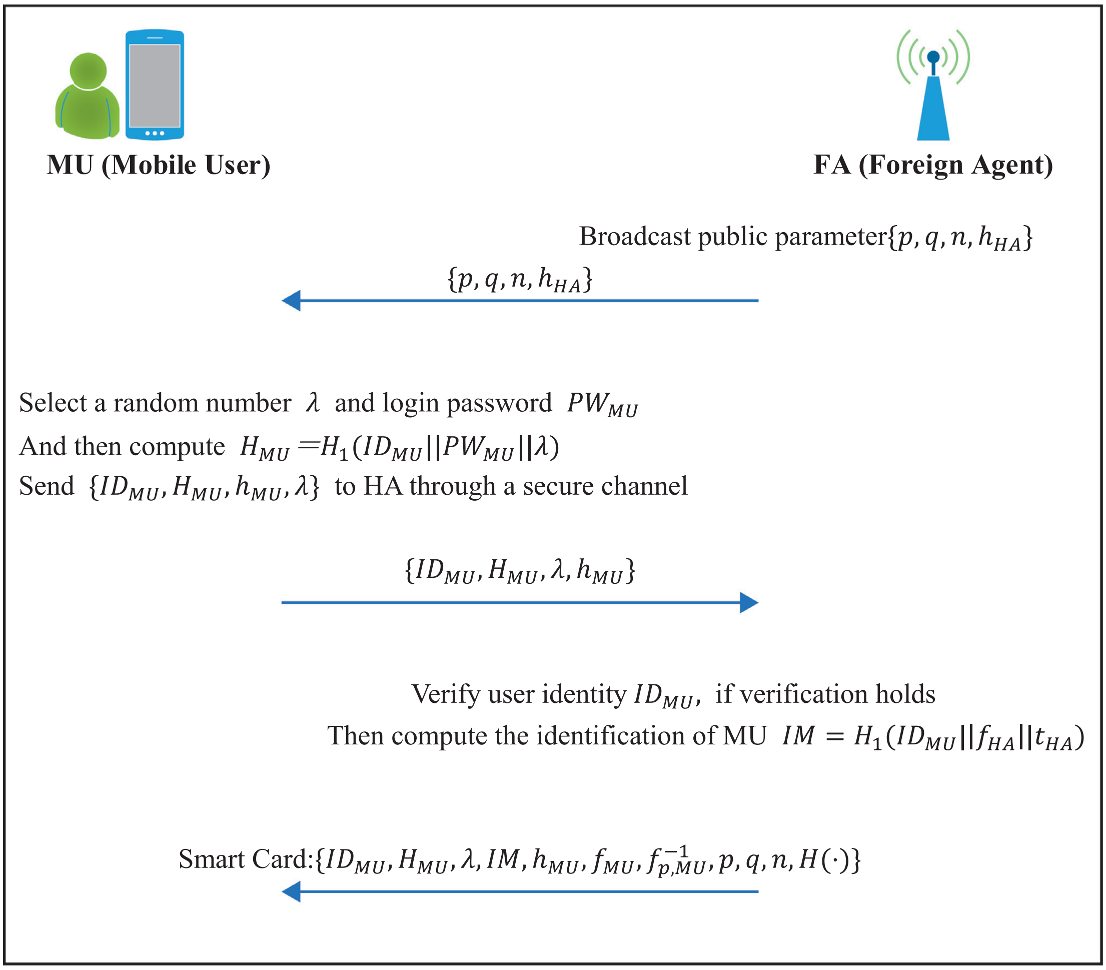

MU (Mobile User)
FA (Foreign Agent)
Broadcast public parameter$\{p, q, n, h_{HA}\}$
$\{p, q, n, h_{HA}\}$
Select a random number λ and login password PW_{MU}
And then compute $H_{MU} = H_1(ID_{MU}||PW_{MU}||\lambda)$
Send $\{ID_{MU}, H_{MU}, h_{MU}, \lambda\}$ to HA through a secure channel
$\{ID_{MU}, H_{MU}, \lambda, h_{MU}\}$
Verify user identity ID_{MU}, if verification holds
Then compute the identification of MU $IM = H_1(ID_{MU}||f_{HA}||t_{HA})$
Smart Card:$\{ID_{MU}, H_{MU}, \lambda, IM, h_{MU}, f_{MU}, f^{-1}_{p,MU}, p, q, n, H(\cdot)\}$

Figure 2: Registration stage.

Table 2: Information table of MU.

ID	Public key	*IM*
$\mathrm{ID}_{\mathrm{MU}}$	h_{MU}	$H_1(H_{\mathrm{MU}}\|f_{\mathrm{HA}}\|t_{\mathrm{HA}})$

Table 3: Information table of FA.

ID	Public key	Symmetric key
$\mathrm{ID}_{\mathrm{FA}}$	h_{FA}	$\mathrm{SK}_{\mathrm{HF}}$

(1) Public key generation: according to the key generation algorithm in Definition 2, three entities generate their own public keys with the following way, respectively:

$$\begin{aligned} h_{\mathrm{HA}} &= p \cdot f^{-1}_{\mathrm{HA},q} \cdot g_{\mathrm{HA}}, \\ h_{\mathrm{MU}} &= p \cdot f^{-1}_{\mathrm{MU},q} \cdot g_{\mathrm{MU}}, \\ h_{\mathrm{FA}} &= p \cdot f^{-1}_{\mathrm{FA},q} \cdot g_{\mathrm{FA}}. \end{aligned} \tag{9}$$

(2) Decryption: with the encrypted message according to Definition 3, the entities can decrypt the message according to Definition 4. Here, we take V_1 and V_2 as examples to explain the decryption process.

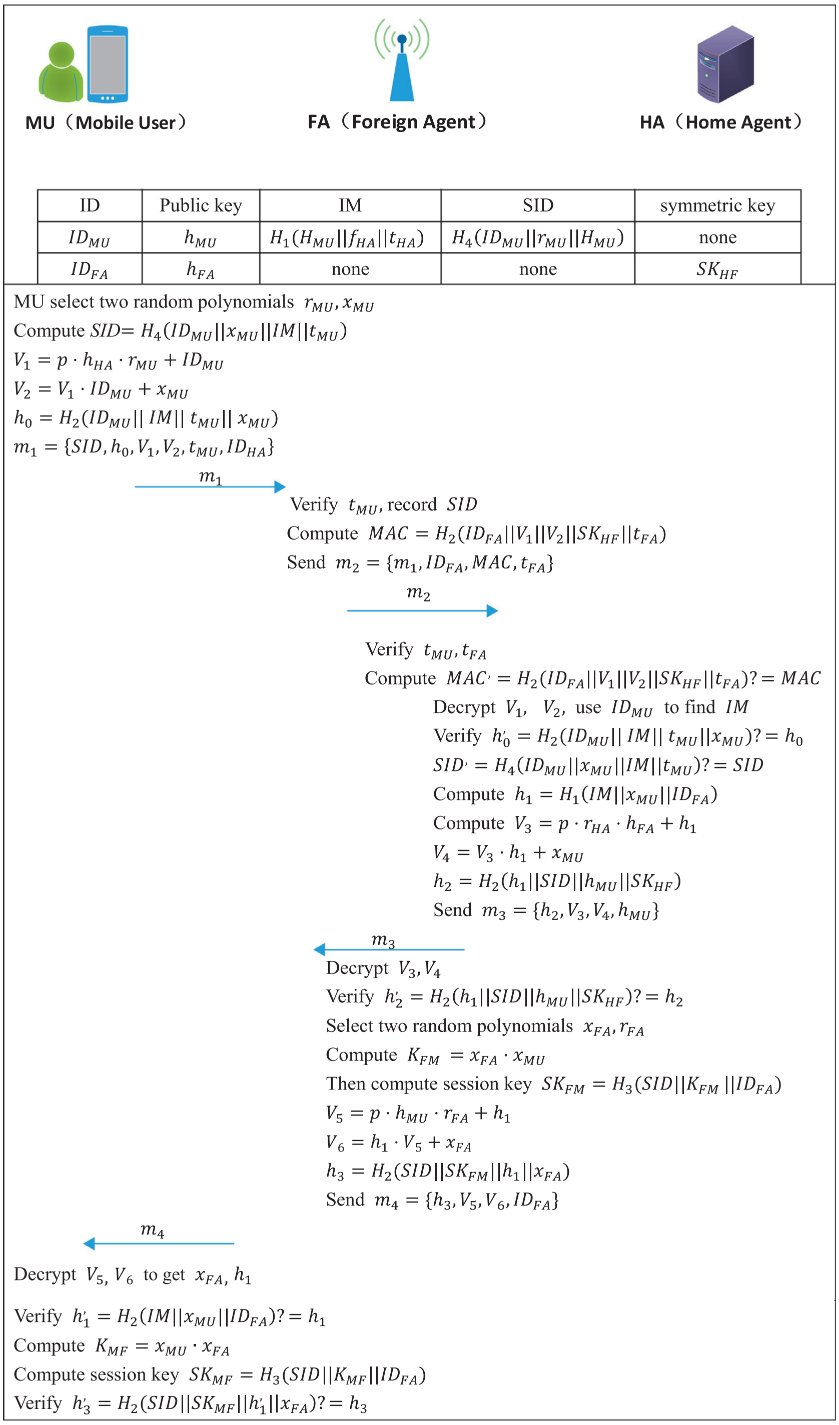
① When HA receives V_1, it first computes a temporary polynomial $T_{V_1} = f_{\mathrm{HA}} \cdot V_1 \pmod{q}$.

② Then, performs modular p operation on T_{V_1} to obtain $\mathrm{ID}_{\mathrm{MU}}$.

③ Afterwards, it computes $r_{\mathrm{MU}} = ((V_1 - \mathrm{ID}_{\mathrm{MU}})/p) \cdot h^{-1}_{\mathrm{HA}}$ and $x_{\mathrm{MU}} = V_2 - V_1 \cdot \mathrm{ID}_{\mathrm{MU}}$ to obtain r_{MU} and x_{MU}.

(3) Session key generation: with the help of HA, MU and FA trust each other; then, they will exchange secret parameters to compute the shared session key. Because $K_{\mathrm{FM}} = x_{\mathrm{FA}} \cdot x_{\mathrm{MU}} = K_{\mathrm{MF}}$, no one can compute or obtain K_{FM} and K_{MF} except MU and HA. Therefore, only MU and FA can generate the shared session key:

$$\begin{aligned} \mathrm{SK}_{\mathrm{FM}} &= H_3\left(\mathrm{SID}\|K_{\mathrm{FM}}\|\mathrm{ID}_{\mathrm{FA}}\right) \\ &= H_3\left(\mathrm{SID}\|K_{\mathrm{MF}}\|\mathrm{ID}_{\mathrm{FA}}\right) \\ &= \mathrm{SK}_{\mathrm{MF}}. \end{aligned} \tag{10}$$



ID	Public key	IM	SID	symmetric key
ID_{MU}	h_{MU}	$H_1(H_{MU}\|\|f_{HA}\|\|t_{HA})$	$H_4(ID_{MU}\|\|r_{MU}\|\|H_{MU})$	none
ID_{FA}	h_{FA}	none	none	SK_{HF}

MU select two random polynomials r_{MU}, x_{MU}
Compute $SID = H_4(ID_{MU}||x_{MU}||IM||t_{MU})$
$V_1 = p \cdot h_{HA} \cdot r_{MU} + ID_{MU}$
$V_2 = V_1 \cdot ID_{MU} + x_{MU}$
$h_0 = H_2(ID_{MU}|| IM|| t_{MU}|| x_{MU})$
$m_1 = \{SID, h_0, V_1, V_2, t_{MU}, ID_{HA}\}$

Verify t_{MU}, record SID
Compute $MAC = H_2(ID_{FA}||V_1||V_2||SK_{HF}||t_{FA})$
Send $m_2 = \{m_1, ID_{FA}, MAC, t_{FA}\}$

Verify t_{MU}, t_{FA}
Compute $MAC' = H_2(ID_{FA}||V_1||V_2||SK_{HF}||t_{FA})? = MAC$
Decrypt V_1, V_2, use ID_{MU} to find IM
Verify $h_0' = H_2(ID_{MU}|| IM|| t_{MU}||x_{MU})? = h_0$
$SID' = H_4(ID_{MU}||x_{MU}||IM||t_{MU})? = SID$
Compute $h_1 = H_1(IM||x_{MU}||ID_{FA})$
Compute $V_3 = p \cdot r_{HA} \cdot h_{FA} + h_1$
$V_4 = V_3 \cdot h_1 + x_{MU}$
$h_2 = H_2(h_1||SID||h_{MU}||SK_{HF})$
Send $m_3 = \{h_2, V_3, V_4, h_{MU}\}$

Decrypt V_3, V_4
Verify $h_2' = H_2(h_1||SID||h_{MU}||SK_{HF})? = h_2$
Select two random polynomials x_{FA}, r_{FA}
Compute $K_{FM} = x_{FA} \cdot x_{MU}$
Then compute session key $SK_{FM} = H_3(SID||K_{FM}||ID_{FA})$
$V_5 = p \cdot h_{MU} \cdot r_{FA} + h_1$
$V_6 = h_1 \cdot V_5 + x_{FA}$
$h_3 = H_2(SID||SK_{FM}||h_1||x_{FA})$
Send $m_4 = \{h_3, V_5, V_6, ID_{FA}\}$

Decrypt V_5, V_6 to get x_{FA}, h_1

Verify $h_1' = H_2(IM||x_{MU}||ID_{FA})? = h_1$
Compute $K_{MF} = x_{MU} \cdot x_{FA}$
Compute session key $SK_{MF} = H_3(SID||K_{MF}||ID_{FA})$
Verify $h_3' = H_2(SID||SK_{MF}||h_1'||x_{FA})? = h_3$

Figure 3: Authentication phase.

3.4. Password Update. In order to prevent password cracking, this scheme provides the operation of updating user password, and the password change phase is invoked by the mobile terminal, and the user performs the following steps on the smart card:

(1) Mobile user inputs his $\mathrm{ID}_{\mathrm{MU}}$ and $\mathrm{PW}_{\mathrm{MU}}$; smart card computes $H'_{\mathrm{MU}} = H_1(\mathrm{ID}_{\mathrm{MU}} \| \mathrm{PW}_{\mathrm{MU}} \| \lambda)$ and verifies whether $H'_{\mathrm{MU}} = H_{\mathrm{MU}}$; if the equation holds, user login in successful; otherwise, the smart card terminates the login process.

(2) The user sends the operation request of updating login password according to the system prompt, and the smart card will send the prompt of updating password to the user after receiving the request.

(3) User selects a new password $\mathrm{PW}_{\mathrm{MU}}^{\mathrm{NEW}}$ and new random number λ^{NEW}, then computes

$H_{\mathrm{MU}}^{\mathrm{NEW}} = H_1(\mathrm{ID}_{\mathrm{MU}} \| \mathrm{PW}_{\mathrm{MU}}^{\mathrm{NEW}} \| \lambda^{\mathrm{NEW}})$, and replaces H_{MU} by $H_{\mathrm{MU}}^{\mathrm{NEW}}$.

3.5. Session Key Update. MU and FA need to renew session key for security reasons if user is always within the same FA. However, initializing a new session to execute key exchange protocol is time consuming. For the sake of security and efficiency, we provide the update operation of the session key. If the roaming mobile user needs to update the session key established with the foreign agent before, as shown in Figure 4, the following steps should be performed.

MU randomly selects a polynomial r'_{MU} from $\mathscr{L}_r$, then MU computes and sends $m_i = \{E_{\mathrm{SK}_{\mathrm{FM}}}(\mathrm{SID} \| t_{\mathrm{MU}} \| r'_{\mathrm{MU}}), \mathrm{SID}, t_{\mathrm{MU}}, \mathrm{Ch}\}$ to FA. $\mathrm{SK}_{\mathrm{FM}}$ is the session key established with foreign agent before, t_{MU} is a timestamp. Ch is a flag for request of updating session key.

When the foreign agent FA receives the message m_i from the roaming user MU, FA performs the following steps:

(1) Verifies $|T_i - t_{\mathrm{MU}}| < \Delta T$, T_i is a timestamp

(2) If the equation above holds, uses $\mathrm{SK}_{\mathrm{FM}}$ to decrypt m_i and then verifies the legitimacy of SID

(3) If SID is valid, FA selects a random polynomial r'_{FA} from $\mathscr{L}_r$ and then computes $\mathrm{SK}'_{\mathrm{FM}} = H_3(\mathrm{SK}_{\mathrm{FM}} \| r'_{\mathrm{FA}} \| r'_{\mathrm{MU}})$, $\mathrm{SK}'_{\mathrm{FM}}$ is the new session key

(4) FA computes and sends $m_{i+1} = \{E_{\mathrm{SK}_{\mathrm{FM}}}(H_1(\mathrm{SK}'_{\mathrm{FM}} \| \mathrm{SK}_{\mathrm{FM}}), r'_{\mathrm{FA}}, t_{\mathrm{FA}}, \mathrm{ID}_{\mathrm{FA}}), \mathrm{ID}_{\mathrm{FA}}, t_{\mathrm{FA}}\}$ to MU

When MU receives the message m_{i+1}, MU verifies t_{FA} and $\mathrm{ID}_{\mathrm{FA}}$, if they are valid then computes $\mathrm{SK}'_{\mathrm{FM}} = H_3(\mathrm{SK}_{\mathrm{FM}} \| r'_{\mathrm{FA}} \| r'_{\mathrm{MU}})$, and verifies $H'_1(\mathrm{SK}'_{\mathrm{FM}} \| \mathrm{SK}_{\mathrm{FM}})? = H_1(\mathrm{SK}'_{\mathrm{FM}} \| \mathrm{SK}_{\mathrm{FM}})$; if this equation holds, then the new session key is updated.

4. Analysis

4.1. Correctness. BAN logic model was first proposed by Burrows et al. [67] in 1990, which is a simple and powerful tool for analyzing the correctness of authentication schemes. In this section, we first describe the basic knowledge of the BAN logic model. Then, we will use the BAN logic model to analyze the correctness of the proposed protocol.

4.1.1. Definition of BAN Logic Model. (1) Notations and Semantics. In the following, we briefly describe the BAN logic model from notations and semantics:

(1) P and Q denote the communication entity

(2) K_{ab} denotes the shared session key of communication entity

(3) K_a and K_b denote the public key of communication entity

(4) K_a^{-1} and K_b^{-1} denote the secret key of communication entity

(5) X and Y denote the message passed in the protocol

(6) $P| \equiv X$: P believes message X is true

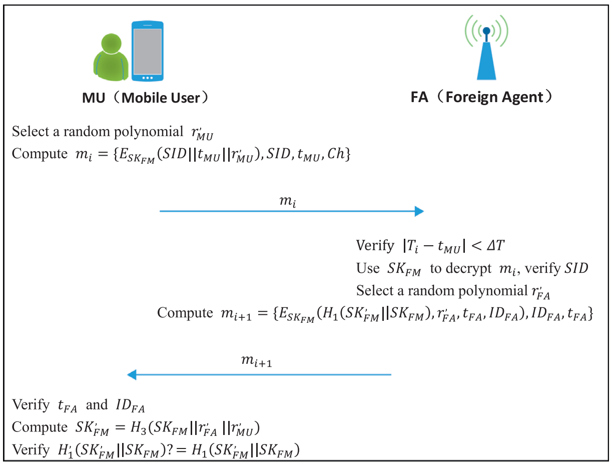

MU（Mobile User）
FA（Foreign Agent）
Select a random polynomial r'_{MU}
Compute $m_i = \{E_{SK_{FM}}(SID||t_{MU}||r'_{MU}), SID, t_{MU}, Ch\}$
m_i
Verify $|T_i - t_{MU}| < \Delta T$
Use SK_{FM} to decrypt m_i, verify SID
Select a random polynomial r'_{FA}
Compute $m_{i+1} = \{E_{SK_{FM}}(H_1(SK'_{FM}||SK_{FM}), r'_{FA}, t_{FA}, ID_{FA}), ID_{FA}, t_{FA}\}$
m_{i+1}
Verify t_{FA} and ID_{FA}
Compute $SK'_{FM} = H_3(SK_{FM}||r'_{FA}||r'_{MU})$
Verify $H'_1(SK'_{FM}||SK_{FM})? = H_1(SK'_{FM}||SK_{FM})$

Figure 4: Session key update phase.

(7) $P \triangleleft X$: P once received a message containing X

(8) $P| \sim X$: P once sent a message including X

(9) $P| \Rightarrow X$: P controls X

(10) $\#(X)$ denotes that the message X is fresh

(11) $P \overset{K}{\longleftrightarrow} Q$: P and Q use the shared symmetric K to communicate with each other

(12) $\{X\}_K$ represents the ciphertext obtained by encrypting message X with secret key K

(13) $\langle X \rangle_Y$ denotes the combination of X and Y, that is, Y is a secret value, whose presence represents the identity of the owner of $\langle X \rangle_Y$

(14) (X, Y) denotes the connection between X and Y

(15) $\mathrm{rule}_1/\mathrm{rule}_2$ means that rule_2 can be derived from rule_1

(2) Inference Rules. In order to use BAN logic for correctness analysis, we will describe some related inference rules of BAN logic model as follows:

(1) Message-meaning rule:

$$\frac{P| \equiv Q \overset{K}{\longleftrightarrow} P, P \triangleleft \{X\}_K}{P| \equiv Q| \sim X}. \tag{11}$$

If P believes the shared session key K between P and Q and P receives a message $\{X\}_K$ encrypted by K, then P believes that Q once sent the message X.

(2) Nonce verification rule:

$$\frac{P| \equiv \#(X), P| \equiv Q| \sim X}{P| \equiv Q| \equiv X}. \tag{12}$$

If P believes the message X is fresh, also P believes Q has said message X, then P believes X.

(3) Jurisdiction rule:

$$\frac{P| \equiv Q \Longrightarrow X, P| \equiv Q| \equiv X}{P| \equiv X}. \tag{13}$$

If P believes Q has jurisdiction over X, and P believes that Q believes X, then P believes message.

(4) Freshness rule:

$$\frac{P \mid \equiv \#(X)}{P \mid \equiv \#(X, Y)}. \tag{14}$$

If P believes X is fresh, then P believes (X, Y) is fresh.

(5) Belief rule:

$$\frac{P \mid \equiv (X, Y)}{P \mid \equiv X}, \qquad \frac{P \mid \equiv X, P \mid \equiv Y}{P \mid \equiv (X, Y)}. \tag{15}$$

If P believes message (X, Y) collection of X and Y, then P believes in each individual message.

(6) Session key rule:

$$\frac{P \mid \equiv \#(K), P \mid \equiv Q \mid \equiv X}{P \mid \equiv P \overset{K}{\longleftrightarrow} Q}. \tag{16}$$

If P believes the shared key K is fresh, and P also believes that Q believes message X, then P believes $P \overset{K}{\longleftrightarrow} Q$.

(7) Seeing rule:

$$\frac{P \lhd (X, Y)}{P \lhd X}, \qquad \frac{P \mid \equiv P \overset{K}{\longleftrightarrow} Q, P \lhd \{X\}_K}{P \lhd X}. \tag{17}$$

If P receives a message and P knows the related key about the message, then P receives component of the message.

4.1.2. Correctness Analysis. The correctness of the scheme can be proved as follows:

(1) Idealized protocol model:

(1) MU $\longrightarrow$ FA: $m_1 = \{\mathrm{SID}, h_0 = H_2(\mathrm{ID}_{\mathrm{MU}} \| \mathrm{IM} \| t_{\mathrm{MU}} \| x_{\mathrm{MU}}), \{\mathrm{ID}_{\mathrm{MU}}, x_{\mathrm{MU}}\}_{K_{HA}}, t_{\mathrm{MU}}, \mathrm{ID}_{\mathrm{HA}}\}$

(2) FA $\longrightarrow$ HA: $m_2 = \{m_1, \mathrm{ID}_{\mathrm{FA}}, H_2(\mathrm{ID}_{\mathrm{FA}} \| \{\mathrm{ID}_{\mathrm{MU}}, x_{\mathrm{MU}}\}_{K_{\mathrm{HA}}} \| \mathrm{FA} \overset{K_{\mathrm{HF}}}{\longleftrightarrow} \mathrm{HA}), t_{\mathrm{FA}}\}$

(3) HA $\longrightarrow$ FA: $m_3 = \{h_2 = H_2(h_1 \| \mathrm{SID} \| h_{\mathrm{MU}} \| \mathrm{HA} \overset{K_{\mathrm{HF}}}{\longleftrightarrow} \mathrm{FA}), \{h_1 = H_1(\mathrm{IM} \quad \| x_{\mathrm{MU}} \| \mathrm{ID}_{\mathrm{FA}}), \quad x_{\mathrm{MU}}\}_{K_{\mathrm{FA}}}, h_{\mathrm{MU}}\}$

(4) FA $\longrightarrow$ MU: $m_4 = \left\{h_3 = H_2(\mathrm{SID} \| h_1 \| \mathrm{FA} \overset{K_{FM}}{\longleftrightarrow} \mathrm{MU} \| x_{\mathrm{FA}}), \{h_1 = H_1(\mathrm{IM} \| x_{\mathrm{MU}} \| \mathrm{ID}_{\mathrm{FA}}), x_{\mathrm{FA}}\}_{K_{\mathrm{MU}}}\right\}$

(2) Initial assumptions:

There are three communication entities in the proposed scheme: MU (mobile user), HA (home agent), and FA (foreign agent). The three entities generate all the authentication messages of the proposed scheme, so we need to make initial assumptions through three aspects.

(1) MU:

$$\begin{gathered} \mathrm{A1}: \mathrm{MU} \lhd \mathrm{ID}_{\mathrm{MU}}, \\ \mathrm{A2}: \mathrm{MU} \mid \equiv \mathrm{SID}, \\ \mathrm{A3}: \mathrm{MU} \mid \equiv \mathrm{ID}_{\mathrm{HA}}, \\ \mathrm{A4}: \mathrm{MU} \mid \equiv x_{\mathrm{MU}}, \\ \mathrm{A5}: \mathrm{MU} \lhd h_{\mathrm{HA}}, \\ \mathrm{A6}: \mathrm{MU} \lhd \mathrm{IM}. \end{gathered} \tag{18}$$

The above formula A1~A6 means the following:

A1: MU believes and own its own real identity

A2: MU believes the anonymous its own identity

A3: because MU registered to HA before authentication phase, so MU believes the real identity of HA

A4: MU believes the random number x_{MU} it chooses

A5: MU knows the public key of HA

A6: MU owns its identity certificate IM because HA has computed and sent it to MU in the registration phase

(2) HA:

$$\begin{gathered} \mathrm{B1}: \mathrm{HA} \lhd \mathrm{ID}_{\mathrm{HA}}, \\ \mathrm{B2}: \mathrm{HA} \mid \equiv \mathrm{HA} \overset{K_{\mathrm{HF}}}{\longleftrightarrow} \mathrm{FA}, \\ \mathrm{B3}: \mathrm{HA} \lhd \mathrm{ID}_{\mathrm{MU}}, \\ \mathrm{B4}: \mathrm{HA} \lhd h_{\mathrm{MU}}, \\ \mathrm{B5}: \mathrm{HA} \lhd \mathrm{IM}, \\ \mathrm{B6}: \mathrm{HA} \lhd \mathrm{ID}_{\mathrm{FA}}. \end{gathered} \tag{19}$$

The above formula B1~B8 means the following:

B1: HA believes and owns its own real identity

B2: HA believes the key shared with FA

B3: because MU has sent $\mathrm{ID}_{\mathrm{MU}}$ to HA in the registration phase, so HA owns the real identity of MU

B4: HA owns the public key of MU because MU once sent it to HA in the registration phase

B5: HA owns identity certificate IM of MU because HA has computed in the registration phase

B6: HA owns the real identity of FA

(3) FA:

$$\begin{gathered} \mathrm{C1}: \mathrm{FA} \lhd \mathrm{ID}_{\mathrm{FA}}, \\ \mathrm{C2}: \mathrm{FA} \lhd \mathrm{ID}_{\mathrm{HA}}, \\ \mathrm{C3}: \mathrm{FA} \mid \equiv x_{\mathrm{FA}}, \\ \mathrm{C4}: \mathrm{FA} \mid \equiv \mathrm{FA} \overset{K_{\mathrm{HF}}}{\longleftrightarrow} \mathrm{HA}. \end{gathered} \tag{20}$$

The above formula C1~C6 means the following:

C1: FA believes and owns its own real identity

C2: FA owns the real identity of HA

C3: FA believes the random number x_{FA} it chooses

C4: FA believes the key shared with HA

(3) Goals to be achieved:

$$\begin{aligned}
&\text{G1: HA}| \equiv \text{ID}_{\text{FA}},\\
&\text{G2: HA}| \equiv \text{SID},\\
&\text{G3: FA}| \equiv \text{HA}| \equiv \text{SID},\\
&\text{G4: MU}| \equiv \text{HA}| \equiv \text{ID}_{\text{FA}},\\
&\text{G5: MU}| \equiv \text{MU} \overset{\text{SK}_{\text{MF}}}{\longleftrightarrow} \text{FA},\\
&\text{G6: FA}| \equiv \text{FA} \overset{\text{SK}_{\text{FM}}}{\longleftrightarrow} \text{MU}.
\end{aligned} \tag{21}$$

To provide secure and anonymous communication for legal mobile users in roaming services, there is a mutual authentication between the mobile user and foreign agent with the help of the home agent in the proposed protocol. Then, MU and FA generate a shared session key for the safety of subsequent communication. This means that the proposed scheme can achieve the goals listed above. In the following, we will give explanations for the goals listed above:

G1: HA believes the real identity of FA

G2: HA believes the anonymous identity of MU

G3: FA believes that HA believes the anonymous identity of MU

G4: MU believes that HA believes the real identity of FA

G5: MU believes the shared session key between MU and FA, which means MU and FA generated the shared session key successfully

G6: FA believes the shared session key between FA and MU, which means FA and MU generated the shared session key successfully

5. Correctness Verification

In this section, we analyze the proposed protocol using the BAN logic model to validate the security and correctness claim of the proposed protocol. The following are the detailed steps to prove that the proposed protocol can reach the goals shown above.

From the message m_2, on verifying the timestamp of FA and applying Seeing rule $P \lhd (X, Y)/P \lhd X$, we obtain the following:

$$\begin{aligned}
&\text{V1: HA} \lhd m_1,\\
&\text{V2: HA} \lhd \text{MAC},\\
&\text{V3: HA}| \equiv \#(m_2),\\
&\text{V4: HA}| \equiv \#(t_{\text{FA}}).
\end{aligned} \tag{22}$$

From V2 and B2, on applying Message-meaning rule $(P| \equiv Q \overset{K}{\longleftrightarrow} P, P \lhd \{X\}_K)/(P| \equiv Q| \sim X)$, we obtain

$$\text{V5: HA}| \equiv \text{FA}| \sim \text{MAC}. \tag{23}$$

From V4, on applying Freshness rule $(P| \equiv \#(X))/(P| \equiv \#(X, Y))$, we obtain

$$\text{V6: HA}| \equiv \#(\text{MAC}). \tag{24}$$

From V5 and V6, on applying Nonce verification rule $(P| \equiv \#(X), P| \equiv Q| \sim X)/(P| \equiv Q| \equiv X)$, we obtain

$$\text{V7: HA}| \equiv \text{FA}| \equiv \text{MAC}. \tag{25}$$

From V7, on applying Belief rule $(P| \equiv (X, Y))/(P| \equiv X)$, we obtain

$$\text{V8: HA}| \equiv \text{ID}_{\text{FA}}. \tag{26}$$

From V1, on verifying the timestamp of MU and applying Seeing rule $(P \lhd (X, Y))/(P \lhd X)$, we obtain

$$\begin{aligned}
&\text{V9: HA} \lhd \text{SID},\\
&\text{V10: HA}| \equiv \#(t_{\text{MU}}),\\
&\text{V11: HA} \lhd V_1,\\
&\text{V12: HA} \lhd V_2,\\
&\text{V13: HA} \lhd h_0.
\end{aligned} \tag{27}$$

From B3, V11, V12, and V13, on verifying $h_0' = H_2(\text{ID}_{\text{MU}} \| \text{IM} \| t_{\text{MU}} \| x_{\text{MU}})? = h_0$ and applying Seeing rule $(P| \equiv P \overset{K}{\longleftrightarrow} Q, P \lhd \{X\}_K)/(P \lhd X)$, we can say

$$\begin{aligned}
&\text{V14: HA}| \equiv \text{ID}_{\text{MU}},\\
&\text{V15: HA}| \equiv x_{\text{MU}},\\
&\text{V16: HA}| \equiv h_0,\\
&\text{V17: HA}| \equiv \text{IM}.
\end{aligned} \tag{28}$$

From V14, V15, and V17 Belief rule $(P| \equiv X, P| \equiv Y)/(P| \equiv (X, Y))$, we obtain

$$\text{V18: HA}| \equiv \text{SID}. \tag{29}$$

From message m_1, on verifying the timestamp of MU applying Seeing rule $(P \lhd (X, Y))/P \lhd X$, we obtain

$$\begin{aligned}
&\text{V19: FA} \lhd \text{SID},\\
&\text{V20: FA}| \equiv \#(t_{\text{MU}}).
\end{aligned} \tag{30}$$

From message m_3, on applying Seeing rule $(P \lhd (X, Y))/P \lhd X$ and $(P| \equiv P \overset{K}{\longleftrightarrow} Q, P \lhd \{X\}_K)/P \lhd X$, we obtain

$$\begin{aligned}
&\text{V21: FA} \lhd h_{\text{MU}},\\
&\text{V22: FA} \lhd h_1,\\
&\text{V23: FA} \lhd x_{\text{MU}},\\
&\text{V24: FA} \lhd h_2.
\end{aligned} \tag{31}$$

From C4, V19, and V24, on verifying $h_2' = H_2(h_1 \| \text{SID} \| h_{\text{MU}} \| \text{SK}_{\text{HF}})? = h_2$ and applying Message-meaning rule $(P| \equiv Q \overset{K}{\longleftrightarrow} P, P \lhd \{X\}_K)/(P| \equiv Q| \sim X)$, we obtain

$$\begin{aligned}
&\text{V25: FA}| \equiv \text{HA}| \sim \text{SID},\\
&\text{V26: FA}| \equiv h_2,\\
&\text{V27: FA}| \equiv h_1,\\
&\text{V28: FA}| \equiv x_{\text{MU}}.
\end{aligned} \tag{32}$$

From V20, on applying Freshness rule $(P| \equiv \#(X))/(P| \equiv \#(X,Y))$, we obtain

$$\text{V29: FA}| \equiv \#(\text{SID}). \tag{33}$$

From V25 and V29, on applying Nonce verification rule $(P| \equiv \#(X), P| \equiv Q| \sim X)/(P| \equiv Q| \equiv X)$, we obtain

$$\text{V30: FA}| \equiv \text{HA}| \equiv \text{SID}. \tag{34}$$

From message m_4, on applying Seeing rule $(P \lhd (X,Y))/P \lhd X$ and $(P| \equiv P\overset{K}{\longleftrightarrow}Q, P \lhd \{X\}_K)/P \lhd X$, we obtain

$$\begin{aligned}&\text{V31: MU} \lhd h_1,\\&\text{V32: MU} \lhd h_3,\\&\text{V33: MU} \lhd x_{\text{FA}},\\&\text{V34: MU} \lhd \text{ID}_{\text{FA}}.\end{aligned} \tag{35}$$

From A4 and A6, MU verifies $h_1' = H_2(\text{IM}\|x_{\text{MU}}\|\text{ID}_{\text{FA}})? = h_1$, and on applying Belief rule $(P| \equiv Q| \equiv (X,Y))/(P| \equiv Q| \equiv X)$, we can obtain

$$\begin{aligned}&\text{V35: MU}| \equiv \text{ID}_{\text{FA}},\\&\text{V36: MU}| \equiv \text{HA}| \equiv \text{ID}_{\text{FA}}.\end{aligned} \tag{36}$$

Because t_{MU} is a random timestamp selected by MU, so we can say

$$\text{V37: MU}| \equiv \#(t_{\text{MU}}). \tag{37}$$

From V37, on applying Freshness rule $(P| \equiv \#(X))/(P| \equiv \#(X,Y))$, we obtain

$$\begin{aligned}&\text{V38: MU}| \equiv \#(\text{SID}),\\&\text{V39: MU}| \equiv \#(\text{SK}_{\text{MF}}).\end{aligned} \tag{38}$$

From V31, V32, and V33, on verifying $h_3' = H_2(\text{SID}\|\text{SK}_{\text{MF}}\|h_1'\|x_{\text{FA}})? = h_3$ and applying Belief rule $(P| \equiv Q| \equiv (X,Y))/(P| \equiv Q| \equiv X)$, we can conclude

$$\begin{aligned}&\text{V40: MU}| \equiv \text{FA}| \equiv K_{\text{MF}},\\&\text{V41: MU}| \equiv x_{\text{FA}}.\end{aligned} \tag{39}$$

From V39 and V40, on applying Session key rule $(P| \equiv \#(K), P| \equiv Q| \equiv X)/(P| \equiv P\overset{K}{\longleftrightarrow}Q)$, we obtain

$$\text{V42: MU}| \equiv \text{MU}\overset{\text{SK}_{\text{MF}}}{\longleftrightarrow}\text{FA}. \tag{40}$$

From V29, on applying Freshness rule $(P| \equiv \#(X))/(P| \equiv \#(X,Y))$, we obtain

$$\text{V42: FA}| \equiv \#(\text{SK}_{\text{MF}}). \tag{41}$$

From V28 and both FA, compute $K_{\text{FM}} = x_{\text{FA}} \cdot x_{\text{MU}}$ in the same way:

$$\text{V43: FA}| \equiv \text{MU}| \equiv K_{\text{MF}}. \tag{42}$$

From V42 and V43, on applying Session key rule $(P| \equiv \#(K), P| \equiv Q| \equiv X)/(P| \equiv P\overset{K}{\longleftrightarrow}Q)$, we obtain

$$\text{V44: FA}| \equiv \text{FA}\overset{\text{SK}_{\text{FM}}}{\longleftrightarrow}\text{MU}. \tag{43}$$

Thus, the proposed can reach the goals G1~G6 through the analysis of the above steps, and it can be concluded that the proposed protocol provides mutual authentication and session key establishment.

5.1. Security

5.1.1. Formal Security Proof

(1) Security Model. This section defines the security model of lattice-based authentication protocol, which is based on the security model proposed by Bellare et al. [63–65]. The attack capability of the adversary $\mathscr{A}$ is defined by a series of oracle queries and security assumptions. $\mathscr{A}$ proceeds an interaction experiment by performing a series of oracle queries with any participant instances in the protocol $\prod_U^i$. In the course of interaction, $\mathscr{A}$ is given the ability to attack protocols. The security of the key exchange means that any adversary $\mathscr{A}$ cannot distinguish between session keys and random strings generated by honest protocol participant polynomial time random prediction queries. An honest protocol participant U has different instances $\prod_U^i$, and it can execute the protocol concurrently. The adversary $\mathscr{A}$ can use the following predictors to interact with different instances of honest players:

(i) Hash(m): $\mathscr{A}$ queries the random oracle for the hash result. The random oracle returns the result which is existing in the list; else, it chooses a random number r, records (m, r) in a hash table and then returns r.

(ii) Execute$(\prod_U^i)$: this query models the adversary's ability to eavesdrop passively on the protocol, $\mathscr{A}$ can eavesdrop on the honest protocol execution process. The output consists of messages exchanged during protocol execution.

(iii) Send$(\prod_U^i, m)$: this query models the adversary's ability to actively attack a protocol, $\mathscr{A}$ can intercept a message and change it, or simply forward it to a target instance. The input is the message m sent by the adversary to P^i, and the output is the corresponding message generated by P^i based on the message m.

(iv) Corrupt$(\prod_U^i)$: this query models the ability of adversary $\mathscr{A}$ to corrupt the protocol participant U and returns the user's password.

(v) Reveal$(\prod_U^i)$: $\mathscr{A}$ obtains the session key possessed by $\prod_U^i$. This query models a session key leak.

(vi) Test$(\prod_U^i)$: this query relates to the semantic security of the session key SK. This query was made after many other queries had been made by $\mathscr{A}$. The random oracle selects a random bit $b \in 0, 1$. If $b = 0$, the oracle returns a random value of the same length as the session key, and if $b = 1$, the oracle returns the real session key held by $\prod_U^i$.

Semantic security: considering $\mathscr{A}$ executes the key exchange protocol P, $\mathscr{A}$ interacts with Execute, Send, Reveal, and Test oracles, and finally outputs the bit value b' as a guess of b. If $b = b'$, the adversary is considered successful. Let Succ denote the event that the adversary is successful. Then, the advantage of the adversary successfully breaking the protocol P is defined as follows:

$$\mathrm{Adv}_P^{\mathrm{AKE}}(\mathscr{A}) = \left|\Pr\left[\mathrm{Succ}_P^{\mathrm{AKE}}(\mathscr{A})\right] - \frac{1}{2}\right|. \tag{44}$$

This authenticated key exchange protocol is considered secure if $\mathrm{Adv}_P^{\mathrm{AKE}}(\mathscr{A})$ is negligible.

(2) Security Proof.

Theorem 1. *An adversary $\mathscr{A}$ makes q_{se}, q_{exe}, q_{re}, and q_{co} queries of type Send, Execute, Reval, and Curropt in time t, respectively, and q_{ro} queries to the random oracles:*

$$\begin{aligned}\mathrm{Adv}_P^{\mathrm{AKE}}(\mathscr{A}) = {} & \frac{q_{H_1}^2 + (q_{\mathrm{se}} + q_{\mathrm{ex}})^2}{p^n} \\ & + \frac{q_{H_2}^2 + q_{H_4}^2 + 2(q_{\mathrm{se}} + q_{\mathrm{ex}})^2}{q^k} \\ & + \frac{q_{H_3}^2 + (q_{\mathrm{se}} + q_{\mathrm{ex}})^2}{q^n} + \frac{q_{\mathrm{se}}}{|D|}.\end{aligned} \tag{45}$$

Proof. We use seven experiments $\mathrm{Game}_0, \mathrm{Game}_1, \ldots, \mathrm{Game}_5$, Game_6 to prove the security of the protocol, which has $\mathrm{Adv}_{\mathrm{Game}_0}^{\mathrm{ake}}(\mathscr{A}) \leq \mathrm{Adv}_{\mathrm{Game}_1}^{\mathrm{ake}}(\mathscr{A}) + \mathrm{negl}(n) \leq \cdots \leq \mathrm{Adv}_{\mathrm{Game}_6}^{\mathrm{ake}}(\mathscr{A}) + \mathrm{negl}(n)$, and $\mathrm{negl}(n)$ is negligible values in n. □

Game_0. This experiment represents an original protocol execution.

Game_1. In this experiment, we simulated Send, *Reveal*, *Test*, and *Execute* queries as Tables 4 and 5 show, and H_1, H_2, H_3, and H_4 are also simulated by maintaining hash list $\wedge H_1$, $\wedge H_2$, $\wedge H_3$, and $\wedge H_4$:

$$\mathrm{Adv}_{\mathrm{Game}_0}^{\mathrm{ake}}(\mathscr{A}) \leq \mathrm{Adv}_{\mathrm{Game}_1}^{\mathrm{ake}}(\mathscr{A}) + \mathrm{negl}(n). \tag{46}$$

Proof. In the proposed protocol, H_1, H_2, H_3, and H_4 act as random oracles, so $\mathscr{A}$ cannot distinguish random values and the output of hash function:

$H_1(m)$: if there is a record (m, r) in the list $\wedge H_1$, returns r. If not, choose a random string $r \in R_p$, add (m, r) to the list $\wedge H_1$, and then return r.

$H_2(m)$: if there is a record (m, r) in the list $\wedge H_2$, returns r. If not, choose a random string $r \in z_q^*$, add (m, r) to the list $\wedge H_2$, and then return r.

$H_3(m)$: if there is a record (m, r) in the list $\wedge H_3$, return r. If not, choose a random string $r \in R_q$, add (m, r) to the list $\wedge H_3$, and then return r.

$H_4(m)$: if there is a record (m, r) in the list $\wedge H_4$, return r. If not, choose a random string $r \in z_q^*$, add (m, r) to the list $\wedge H_4$, and then return. □

Game_2. This game simulates all oracles as $Game_1$ expects the cancelation of the game when $\mathscr{A}$ guesses the password correctly. This modification increases the adversary's chances at breaking the game, but the adversary's advantage is still negligible:

$$\mathrm{Adv}_{\mathrm{Game}_1}^{\mathrm{ake}}(\mathscr{A}) \leq \mathrm{Adv}_{\mathrm{Game}_2}^{\mathrm{ake}}(\mathscr{A}) + \mathrm{negl}(n). \tag{47}$$

Proof.

(1) Since $\mathrm{ID}_{\mathrm{MU}}$ is invisible to the adversary $\mathscr{A}$, the adversary can only log in by guessing $\mathrm{ID}_{\mathrm{MU}}$, and this probability is q_{se}/p^n

(2) $\mathscr{A}$ needs to query random oracles to distinguish Game_2 from Game_1, and this probability is q_{ro}/p^n

If event.1 and event.2 do not happen, and Game_2 and Game_1 are indistinguishable, so

$$\Pr_{\mathrm{Game}_1}^{\mathrm{ake}}(\mathscr{A}) \leq \Pr_{\mathrm{Game}_2}^{\mathrm{ake}}(\mathscr{A}) + \frac{q_{\mathrm{se}} + q_{\mathrm{ro}}}{p^n}. \tag{48}$$

□

Game_3. Game_2 is almost identical to Game_3, but once honest parties choose random SID seen previously in the execution, this game will be forcefully ceased:

$$\mathrm{Adv}_{\mathrm{Game}_2}^{\mathrm{ake}}(\mathscr{A}) \leq \mathrm{Adv}_{\mathrm{Game}_3}^{\mathrm{ake}}(\mathscr{A}) + \frac{(q_{\mathrm{se}} + q_{\mathrm{ex}} + q_{\mathrm{ro}})(q_{\mathrm{se}} + q_{\mathrm{ex}})}{q^k}. \tag{49}$$

Proof. SID is a string of length k generated by H_4, which cardinal is q^k. SID is generated after Send, ro, and Execute queries. The probability of generating this value in previous *Send*, *Execute*, or random oracle query is $(q_{\mathrm{se}} + q_{\mathrm{ex}} + q_{\mathrm{ro}})/q^k$; therefore, the probability of *SID* being not unique is $(q_{se} + q_{ex} + q_{ro})(q_{se} + q_{ex})/q^k$. □

Game_4. making the following changes to the Send queries, replace $(x_{\mathrm{MU}}, x_{\mathrm{FA}})$ with random values $(x_{\mathrm{MU}}^*, x_{\mathrm{FA}}^*)$ to compute K_{MF}. For the messages that contain $(x_{\mathrm{MU}}, x_{\mathrm{FA}})$, use random values $(x_{\mathrm{MU}}^*, x_{\mathrm{FA}}^*)$ computes then responds to $\mathscr{A}$. Since the two values are randomly selected in the polynomial space and the secret values are transmitted through encryption and are invisible to the $\mathscr{A}$, this modification does not increase the probability of the $\mathscr{A}$ in violating protocol:

$$\mathrm{Adv}_{\mathrm{Game}_3}^{\mathrm{ake}}(\mathscr{A}) \leq \mathrm{Adv}_{\mathrm{Game}_4}^{\mathrm{ake}}(\mathscr{A}) + \mathrm{negl}(n). \tag{50}$$

Proof. $(x_{\mathrm{MU}}, x_{\mathrm{FA}})$ is encrypted and decrypted by NTRU algorithm. The related information about plaintext cannot be obtained by adversary who only holds public key and ciphertext without private key. Construct an algorithm $\mathscr{M}$ to run adversary $\mathscr{A}$ to break the encryption scheme.

$\mathscr{A}$ sends $(x_{\mathrm{MU}}^*, x_{\mathrm{FA}}^*)$ and $(x_{\mathrm{MU}}, x_{\mathrm{FA}})$ to algorithm $\mathscr{M}.\mathscr{M}$ selects one of them to execute encryption and then sends ciphertext to adversary. $\mathscr{A}$ guesses the encryption result and outputs a bit b. If parameters are selected properly, the advantage of the adversary is negligible. □

Game_5. In order to increase the adversary's chances at winning the game, we simulate all oracles nearly identical to $Game_4$ except that there are collision events happen on the

Table 4: Simulation of Reveal, Test, and Execute query.

Reveal$(\prod_U^i)$: return the session key of MU^i and FA^i
Test$(\prod_U^i)$: on a query Test(MU^i/FA^i), oracle selects a random bit $b \in \{0, 1\}$; if $b = 1$, return a session key; if $b = 0$, return a random value with the same length
Execute$(\prod_U^i)$: on a query Execute(MU^i, FA^i, HA^i), return the protocol message exchanged between three entities m_1, m_2, m_3, m_4

Table 5: Simulation of Send query.

(1) On a query Send(MU^i, start), which denotes the start of protocol, assuming MU^i runs correctly, then MU^i performs the first step operation of the authentication process; then, the query is answered with $m_1 = \{\mathrm{SID}, h_0, V_1, V_2, t_{\mathrm{MU}}, \mathrm{ID}_{\mathrm{HA}}\}$
(2) On a query Send(FA^i, m_1), assuming MU^i runs correctly, then FA^i performs the second step operation of the authentication process; then, the query is answered with $m_2 = \{m_1, \mathrm{ID}_{\mathrm{FA}}, \mathrm{MAC}, t_{\mathrm{FA}}\}$
(3) On a query Send(HA^i, m_2), assuming HA^i runs correctly, then HA^i performs the third step operation of the authentication process; then, the query is answered with $m_3 = \{h_1, h_2, V_3, V_4, V_5, h_{\mathrm{MU}}\}$
(4) On a query Send(FA^i, m_3), assuming FA^i runs correctly, then FA^i performs the fourth step operation of the authentication process; then, the query is answered with $m_4 = \{h_3, h_1, V_5, V_6\}$
(5) On a query Send(MU^i, m_4), assuming MU^i runs correctly, then MU^i executes the fifth step operation of the authentication process; then, the query is answered with $m_5 = H_2(\mathrm{SK}_{\mathrm{MF}} \Vert h_{\mathrm{FA}} \Vert K_{\mathrm{MF}})$

transcript $\{m_1, m_2, m_3, m_4\}$ in the output of hash queries during the execution of protocol. The adversary perform a polynomial number queries of H_1, H_2, H_3, and H_4 to catch collision:

$$\mathrm{Adv}^{\mathrm{ake}}_{\mathrm{Game}_0}(A) \le \mathrm{Adv}^{\mathrm{ake}}_{\mathrm{Game}_1}(A) + \frac{q_{H_1}^2 + (q_{\mathrm{se}} + q_{\mathrm{ex}})^2}{p^n} + \frac{q_{H_4}^2 + q_{H_2}^2 + (q_{\mathrm{se}} + q_{\mathrm{ex}})^2}{q^k} + \frac{q_{H_3}^2 + (q_{\mathrm{se}} + q_{\mathrm{ex}})^2}{q^n}. \tag{51}$$

Proof. Since authentication messages are generated with random numbers, so authentication messages are different at every authentication phase. If the are collision events happen, the adversary succeeds. According to Gardy et al. [66] birthday attack, Game$_4$ and Game$_5$ are distinguishable when collisions occur, and the probability of collisions happened is $((q_{H_1}^2 + (q_{\mathrm{se}} + q_{\mathrm{ex}})^2)/2|H_1|) + ((q_{H_2}^2 + (q_{\mathrm{se}} + q_{\mathrm{ex}})^2)/2|H_2|) + ((q_{H_3}^2 + (q_{\mathrm{se}} + q_{\mathrm{ex}})^2)/2|H_3|) + ((q_{H_4}^2 + (q_{\mathrm{se}} + q_{\mathrm{ex}})^2)/2|H_4|)$. $|\mathrm{H}_1|$, $|H_2|$, $|H_3|$, and $|H_4|$ are the size of the dictionary space corresponding to the hash function show above, and $|H_1| = p^n$, $|H_2| = q^k$, $|H_3| = q^n$, and $|H_4| = q^k$. □

Game$_6$. All passwords in the protocol are saved by an internal password oracle, and it accepts queries to test the given password for MU is correct or not. The internal password oracle is invisible to the adversary and generates all passwords during initialization:

$$\mathrm{Adv}^{\mathrm{ake}}_{\mathrm{Game}_5}(\mathscr{A}) \le \mathrm{Adv}^{\mathrm{ake}}_{\mathrm{Game}_6}(\mathscr{A}) + \mathrm{negl}(n). \tag{52}$$

Proof. The adversary cannot obtain their corresponding private keys by attacking the public keys of MU and FA, so the private key of MU and FA are invisible to the adversary, and in previous games, K_{MF} is calculated with randomly selected values. The session key is a random value at this time, and the information held by the adversary is irrelevant to the session key, so the can only attack the protocol by guessing the bit b or attack the protocol by attacking the user's password online. We denote the event that adversary succeeding in Game$_6$ by $\mathrm{SUCC}^{\mathrm{ake}}_{\mathrm{Game}_6}(\mathscr{A})$; E_{Guss} represents the event that adversary attack protocol by guessing the password. We can easily bound the probability of success in Game$_6$ created by adversary $\mathscr{A}$ as the following equation:

$$\begin{aligned}\Pr\left(\mathrm{SUCC}^{\mathrm{ake}}_{\mathrm{Game}_6}(\mathscr{A})\right) \le{}& \Pr\left(\mathrm{Guss}E_{\mathrm{Guss}}\right) \\ &+ \Pr\left(\mathrm{SUCC}^{\mathrm{ake}}_{\mathrm{Game}_6}(\mathscr{A}) \mid \neg E_{\mathrm{Guss}}\right) \\ &\cdot \Pr\left(\neg E_{\mathrm{Guss}}\right).\end{aligned} \tag{53}$$

Note that $\Pr(E_{\mathrm{Guss}}) \le (q_{\mathrm{se}}/|D|)$, if these passwords are chosen randomly from a dictionary of $|D|$ and the event E_{Guss} does not happen, and the only way for adversary to succeed is to guess bit b through Test query. Therefore, $\Pr(\mathrm{SUCC}^{\mathrm{ake}}_{\mathrm{Game}_6}(\mathscr{A}) \mid \neg\mathrm{Guss}) = (1/2)$.

$$\begin{aligned}\Pr\left(\mathrm{SUCC}^{\mathrm{ake}}_{\mathrm{Game}_6}(\mathscr{A})\right) &\le \Pr(\mathrm{Guss}) + \Pr\left(\mathrm{SUCC}^{\mathrm{ake}}_{\mathrm{Game}_6}(\mathscr{A}) \,\middle|\, \neg\mathrm{Guss}\right) \\ &\quad \cdot \Pr(\neg\mathrm{Guss}) \\ &\le \Pr(\mathrm{Guss}) + \Pr\left(\mathrm{SUCC}^{\mathrm{ake}}_{\mathrm{Game}_6}(\mathscr{A}) \,\middle|\, \neg\mathrm{Guss}\right) \\ &\quad \cdot (1 - \Pr(\mathrm{Guss})) \\ &\le \frac{q_{\mathrm{se}}}{|D|} + \frac{1}{2}\left(1 - \frac{q_{\mathrm{se}}}{|D|}\right) \\ &\le \frac{1}{2} + \frac{q_{\mathrm{se}}}{2|D|}.\end{aligned} \tag{54}$$

By the above calculation, we conclude that

$$\mathrm{Adv}^{\mathrm{ake}}_{\mathrm{Game}_6}(\mathscr{A}) = \left|2\Pr\left(\mathrm{SUCC}^{\mathrm{ake}}_{\mathrm{Game}_6}(\mathscr{A})\right) - 1\right| \le \frac{q_{\mathrm{se}}}{|D|}. \tag{55}$$

Finally, it can be computed that the advantage of the adversary is ignorable by analyzing Game_0, Game_1, ..., Game_5, Game_6. Hereby, Theorem 1 is concluded. □

5.1.2. Informal Security Analysis. Security analysis:

(i) Conditional anonymity: the identity information of the roaming terminal MU is invisible to the foreign agent FA. MU only communicates with the field agent FA through the pseudorandom SID, and SID will vary every one authenticated process. Therefore, the roaming terminal MU is strongly anonymous to the foreign agent FA. If there is a malicious roaming terminal MU in the system, it is necessary to find out its real identity information in time. Since each authentication process requires participation of the home agent HA, and the home agent HA establishes the association between SID and ID_{MU} before. Hence, HA can reveal the user's real identity ID_{MU} through SID.

(ii) Forward security: forward security means that even though an attacker obtains the private keys of roaming mobile user MU and home agent FA through some means, he cannot calculate the previous session key successfully negotiated between MU and FA. Since $\text{SK}_{\text{FM}} = H_3(\text{SID}\|K_{\text{FM}}\|\text{ID}_{\text{FA}})$, where SID is related to randomly selected r_{MU}. SID value is different in each authentication process.

(iii) Untraceability: even if the adversary can intercept all the information exchanged between protocol participants, it cannot track the behavior information of the roaming terminal MU. All exchanged messages and SID generated by the roaming terminal MU during each interaction are all random values, so untraceable properties are satisfied in the proposed scheme.

(iv) Mutual authentication: in this scheme, the adversary cannot participate in the generation and response of protocol authentication messages. The scheme participants are the roaming terminal MU, the foreign agent FA, and the home agent HA, respectively, where the authentication messages generated by MU and FA can only be decrypted by the legitimate home agent HA. Then, the legitimate home agent HA helps them perform the authentication process and generate the session key correctly only if the three parties trust each other.

(v) User login authentication: in order to improve the security of scheme, the smart card should verify the validity of user when login. In the proposed scheme, the user enters the identity ID_{MU} and password ID_{MU} when logging in. The smart card SC calculates $H_{\text{MU}}' = H_1(\text{ID}_{\text{MU}}\|\text{PW}_{\text{MU}}\|\lambda)$ and verifies its validity. If the equation holds, the identity of MU ID_{MU} is valid and SC allow user to login in; otherwise, SC denies the login request.

(vi) Resistance to replay attacks: in the proposed scheme, the messages for authentication that are sent by mobile user MU and foreign agent contain timestamps; when FA and HA execute authentication process, each entity firstly verifies the validity of timestamp contained in messages, and then proceeds subsequent operations. Furthermore, the random numbers r_{MU} ensures that the authentication information is varies in every authentication process so that the adversary cannot perform the replay attacks with the exchanged messages sent before.

(vii) Resistance to man-in-the-middle attack: in the proposed scheme, suppose that an attacker exists in a communication channel who attempts to execute man-in-the-middle attack by intercepting and tampering with communication messages. If he or she tries to tamper with the message m_1, he or she must first tamper with the encrypted messages V_1 and V_2, which are encrypted by NTRU encryption mechanism. Due to SVP and CVP, the attacker cannot get the private key to decrypt the message, so the adversary cannot tamper with the message m_1 successfully. While other messages contain information generated by One-way Hash functions, the attacker needs to solve the anti-collision problem of Hash functions to tamper with the message, so the attacker will also fail.

(viii) Resistance to device-stealing attacks: even if adversaries get user's mobile device, he cannot recover user's password and identity information from the user's smart card, and he can only log in the device by guessing the user's password and identity, so our scheme can resist device-stealing attacks.

(ix) Resistance to privileged-inside attack: in the registration stage, MU sends HA the registration information ID_{MU}, H_{MU}, λ. HA cannot extract MU's password information from the registration information. In addition, MU can also update passwords on smart card without the participation of HA. Finally, the session key negotiated by MU and FA is not visible to HA, so this scheme is resistant to privileged-inside attacks.

(x) Secure user password change: mobile user executes password change phase when the mobile user wants to change the password for the purpose of security. After passing the authentication of smart card, the old password will be replaced by a new password selected by user only in password change phase, FA and HA will not participate in this phase. Therefore, our password change phase is reasonable and security.

Based on the analysis of the security of the proposed scheme, we conduct security comparison with related scheme as in Table 6. The results show that only the proposed scheme provides all the required features and resists known

Table 6: Security comparison of the scheme.

	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	Security
Wu et al. [18]	√	√	√	√	√	√	×	√	×	√	8
Grope and Hwang [17]	×	×	√	√	√	√	√	×	√	√	7
Wen et al. [13]	×	×	√	×	×	√	√	×	×	√	4
Jiang et al. [12]	×	√	√	√	×	√	×	√	×	√	6
Farash et al. [16]	×	×	√	×	×	×	√	×	×	×	2
Alzahrani et al. [31]	√	√	√	√	√	√	√	√	√	×	9
Lu et al. [34]	×	√	×	√	√	√	√	√	×	√	7
Lee et al. [20]	√	√	×	√	×	√	√	√	×	√	8
Ostad-Sharif et al. [33]	√	√	√	√	√	√	×	√	√	√	9
Khatoon and Singh Thakur [32]	√	√	√	√	√	√	√	×	√	√	9
Ours	√	√	√	√	√	√	√	√	√	√	10

S1: conditional anonymity, S2: forward security, S3: untraceability, S4: mutual authentication, S5: resistance to replay attacks, S6: resistance to man-in-the-middle attack, S7: user login authentication, S8: resistance to device-stealing attacks, S9: resistance to privileged-inside attack, S10: secure user password change.

Table 7: Running time of single operation.

Notation	Definition	≈ Time (ms)
T_H	Execution time for one-way hash function	0.004
T_{NE}	Execution time for NTRU encryption	0.13
T_{ND}	Execution time for NTRU decryption	0.086
T_{NM}	Execution time for NTRU modulus multiplication	0.0138
T_S	Execution time for symmetrical encryption/decryption	0.075
T_E	Execution time for ECC-based encryption/decryption	3.85
T_M	Execution time for modular exponent operation	3.85
T_P	Execution time for elliptic curve point multiplication	2.226
T_A	Execution time for elliptic curve point addition	0.025
T_C	Execution time for Chebyshev polynomial computation	2.226

Configuration of experiment CPU: i7-6700, 4 core 8 threads, 3.4GHZ, OS: Windows10, Software: IntelliJ IDEA2019 library: libntru https://github.com/tbuktu/ntru

attacks, whereas competing schemes lack either some features or ensuring against some known attack. In addition, the proposed scheme can also resist to quantum attack, while the related schemes lack this feature.

5.2. Performance. In this section, the proposed scheme of this paper is compared with the presented authentication schemes in related studies [12, 13, 16–18, 20, 31–34] in terms of both communication cost and computational complexity. Since the related schemes are the most recent or influential works in this field that improved either the security or efficiency of their previous schemes, therefore, we will compare our scheme with them.

Due to the external impact on message transmission time, this section only considers the message processing time of the client and server in the authentication phase. The proposed scheme includes four operations: hash operation, NTRU encryption and decryption operation, polynomial modulus, and multiplication operation, which are represented by T_H, T_{NE}, T_{ND}, and T_{NM}, respectively. Based on the hardware and software shown in Table 7, these four operations running time of proposed scheme are evaluated. We recorded the operation time of NTRU and the single operation time of elliptic curve obtained by analyzing the related scheme [10, 20, 23, 30–34] in Table 7.

Table 8 shows the authentication time comparison of the proposed scheme with the related scheme. Due to the high performance of NTRU encryption mechanism, the computation time of three entities in proposed scheme is relatively low. As shown in Figure 5, schemes [16, 20] have better execution time; however, they are susceptible to several known attacks and cannot provide the perfect forward secrecy and untraceability respectively. Consequently, for the ubiquitous network environment, our proposed scheme is more practical.

Table 9 and Figure 6 provide comparison of communication overhead between the proposed scheme and related scheme during the authentication phase. The total communication cost of our protocol is 3903 bits, only lower than that of Wu et al. [18]. However, the communication cost of MU is only 974 bits which is lower than that of Grope and Hwang [17], Wen et al. [13], Jiang et al. [12], Alzahrani et al. [31], and Lu et al. [34]. Therefore, the proposed scheme is more friendly to mobile devices with limited resources. With comprehensive consideration from the performance (computational cost and communication cost) and security attributes, the proposed scheme makes a better tradeoff and makes it more suitable to ubiquitous networks.

Table 8: Computational cost of the client and server.

	MU	FA	HA	Times (ms)
Wu et al. [18]	$8T_H + 2T_E$	$4T_H + T_S + 2T_E$	$8T_H + 3T_S$	8.08
Grope and Hwang [17]	$4T_H + T_M$	$4T_H$	$4T_H + T_M$	7.748
Wen et al. [13]	$4T_H + T_M$	$4T_H + T_M$	$5T_H + 2T_M$	11.602
Jiang et al. [12]	$3T_H + T_M$	$4T_H$	$5T_H + T_M$	7.748
Farash et al. [16]	$6T_H$	$T_H + 2T_S$	$5T_H + 2T_S$	0.348
Alzahrani et al. [31]	$9T_H + 5T_P + 2T_A$	$6T_H + 4T_P + 2T_A$	$8T_H + 5T_P + 3T_A$	31.431
Lu et al. [34]	$10T_H + 5T_P + 3T_A + 2T_S$	$6T_H + 4T_P + 2T_A$	$9T_H + 6T_P + 5T_A + T_S$	33.965
Lee et al. [20]	$7T_H$	$4T_H$	$9T_H + 2T_S$	0.23
Ostad-Sharif et al. [33]	$9T_H + 2T_C$	$3T_H + 2T_C$	$9T_H$	8.988
Khatoon et al. [32]	$9T_H + 3T_P$	$5T_H + 2T_P$	$6T_H + T_P$	13.436
Ours	$5T_H + T_{NE}+T_{ND} + T_{NM}$	$4T_H + T_{NE} + T_{ND} + T_{NM}$	$5T_H + T_{NE} + T_{ND}$	0.7276

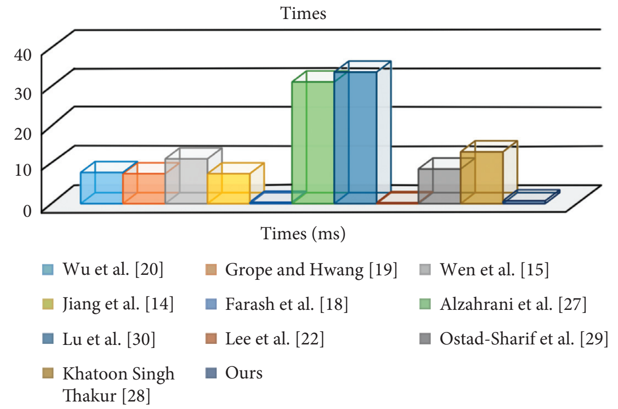


Figure 5: Computational cost of schemes.

Table 9: Comparison of communication overhead.

	MU	FA	HA	Overhead (bits)
Wu et al. [18]	864	2336	736	3936
Grope and Hwang [17]	1152	1600	320	3072
Wen et al. [13]	1152	1600	320	3072
Jiang et al. [12]	1152	1728	320	3200
Farash et al. [16]	608	832	256	1696
Alzahrani et al. [31]	1024	1216	992	3232
Lu et al. [34]	1088	1216	992	3296
Lee et al. [20]	704	1696	576	2976
Ostad-Sharif et al. [33]	960	1568	480	3008
Khatoon and Singh Thakur [32]	864	1312	480	3264
Ours	974	1980	949	3903

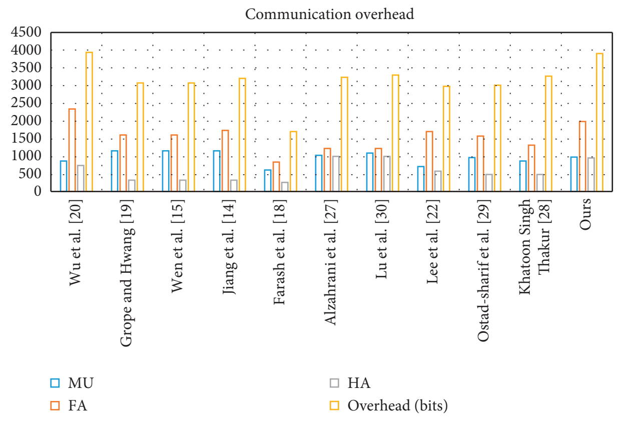


Figure 6: Comparison of computational cost.

6. Conclusion

We put forward a lattice-based roaming authentication scheme. We use formal security proofs and informal analysis to prove the security of our scheme. In addition, BAN logic analysis demonstrates that the proposed scheme is correct and mutual authentication is achieved. Through rigorous theoretical analysis and simulation experiments, we prove that the proposed scheme has better performance and feasibility, which can meet the security requirements of the roaming authentication scheme. We concluded that our lattice-based roaming authentication provides fully secured mutual authentication and conditional anonymity, which can also resist different security attacks such as tractability, replay attack, privileged-inside attack, and especially quantum attack. Security and performance results show that the proposed scheme outperforms the existing authentication schemes, but there are still some limitations on the proposed scheme.

The public key encryption algorithm involved in this paper is NTRU encryption algorithm. The designer of NTRU mainly chooses reasonable parameters to avoid decryption errors and does not carry out quantitative theoretical analysis on the decryption errors. This limits the range of parameter selection and affects the wide use of NTRU algorithm.

6.1. Future Work. In our future work, proposing a revised NTRU algorithm would be learned to solve the inherent decryption failure problem of NTRU algorithm. Then, we can extend the proposed authentication schemes in other scenarios based on revised NTRU algorithm, such as opportunistic networks and wireless sensor networks. And simultaneously, lattice-based multifactor authentication schemes for ubiquitous network would be investigated to accommodate to advanced communication and computation technology, for example, 5G and edge computing.

Data Availability

The source code and data used to support the findings of this study have been deposited in the (1) Github repository (https://github.com/tbuktu/ntru), (2) Springer repository (DOI 10.1007/s11277-012-0535-4, DOI 10.1007/s11277-013-1243-4, DOI 10.1007/s11277-015-2344-z, and DOI 10.1007/s12243-016-0547-2), (3) ScienceDirect repository (https://doi.org/10.1016/j.comcom.2007.12.005), (4) Plos one repository (https://doi.org/10.1371/journal.pone.0193366), (5) Symmetry repository (https://www.mdpi.com/2073-8994/12/2/287), (6) CRYPTOLOGIA repository (https://www.tandfonline.com/doi/full/10.1080/01611194.2019.1706061), (7) International Journal of Communication Systems repository ([https://onlinelibrary.wiley.com/doi/abs/10.1002/dac.3904]), and (8) IEEE SYSTEMS JOURNAL repository (DOI 10.1109/JSYST.2018.2883349).

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.

Acknowledgments

This work was supported by the Venture & Innovation Support Program for Chongqing Overseas Returnees (No. cx2018122).

References

[1] S. Bhattacharya, S. R. Krishnan S., P. K. R. Maddikunta et al., "A novel PCA-firefly based XGBoost classification model for intrusion detection in networks using GPU," *Electronics*, vol. 9, no. 2, p. 219, 2020.

[2] C. Iwendi, Z. Jalil, A. R. Javed et al., "KeySplitWatermark: zero watermarking algorithm for software protection against cyber-attacks," *IEEE Access*, vol. 8, pp. 72650–72660, 2020.

[3] M. Alizadeh, S. Abolfazli, M. Zamani, S. Baharun, and K. Sakurai, "Authentication in mobile cloud computing: a survey," *Journal of Network and Computer Applications*, vol. 61, pp. 59–80, 2016.

[4] J. Srinivas, D. Mishra, and S. Mukhopadhyay, "A mutual authentication framework for wireless medical sensor networks," *Journal of Medical Systems*, vol. 41, no. 5, pp. 1–19, 2017.

[5] J. Zhu and J. Ma, "A new authentication scheme with anonymity for wireless environments," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, pp. 233–235, 2004.

[6] C.-C. Lee, M.-S. Hwang, and I.-E. Liao, "Security enhancement on a new authentication scheme with anonymity for wireless environments," *IEEE Transactions on Industrial Electronics*, vol. 53, no. 5, pp. 1683–1687, 2006.

[7] C. C. Wu, W. B. Lee, and W. J. Tsaur, "A secure authentication scheme with anonymity for wireless communications," *IEEE Communications Letters*, vol. 12, no. 10, pp. 722-723, 2008.

[8] H. Mun, K. Han, Y. S. Lee, C. Y. Yeun, and H. H. Choi, "Enhanced secure anonymous authentication scheme for roaming service in global mobility networks," *Mathematical and Computer Modelling*, vol. 55, no. 1-2, pp. 214–222, 2012.

[9] J. S. Kim and J. Kwak, "Improved secure anonymous authentication scheme for roaming service in global mobility networks," *International Journal of Security and Its Applications*, vol. 6, no. 3, pp. 45–54, 2013.

[10] D. Zhao, H. Peng, L. Li, and Y. Yang, "A secure and effective anonymous authentication scheme for roaming service in global mobility networks," *Wireless Personal Communications*, vol. 78, no. 1, pp. 247–269, 2014.

[11] D. He, S. Chan, C. Chen, J. Bu, and R. Fan, "Design and validation of an efficient authentication scheme with anonymity for roaming service in global mobility networks," *Wireless Personal Communications*, vol. 61, no. 2, pp. 465–476, 2011.

[12] Q. Jiang, J. Ma, G. Li, and L. Yang, "An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks," *Wireless Personal Communications*, vol. 68, no. 4, pp. 1477–1491, 2013.

[13] F. Wen, W. Susilo, and G. Yang, "A secure and effective anonymous user authentication scheme for roaming service in global mobility networks," *Wireless Personal Communications*, vol. 73, no. 3, pp. 993–1004, 2013.

[14] W.-C. Kuo, H.-J. Wei, and J.-C. Cheng, "An efficient and secure anonymous mobility network authentication scheme," *Journal of Information Security and Applications*, vol. 19, no. 1, pp. 18–24, 2014.

[15] Y. R. Lu, X. B. Wu, and X. D. Yang, "A secure anonymous authentication scheme for wireless communications using smart cards," *International Journal of Network Security*, vol. 17, no. 3, pp. 237–245, 2015.

[16] M. S. Farash, S. A. Chaudhry, M. Heydari et al., "A lightweight anonymous authentication scheme for consumer roaming in ubiquitous networks with provable security," *International Journal of Communication Systems*, vol. 30, no. 4, p. e3019, 2017.

[17] P. Gope and T. Hwang, "Enhanced secure mutual authentication and key agreement scheme preserving user anonymity in global mobile networks," *Wireless Personal Communications*, vol. 82, no. 4, pp. 2231–2245, 2015.

[18] F. Wu, L. Xu, S. Kumari et al., "An enhanced mutual authentication and key agreement scheme for mobile user roaming service in global mobility networks," *Annals of Telecommunications*, vol. 72, no. 3-4, pp. 1–14, 2016.

[19] S. A. Chaudhry, A. Albeshri, N. Xiong, C. Lee, and T. Shon, "A privacy preserving authentication scheme for roaming in ubiquitous networks," *Cluster Computing*, vol. 20, no. 2, pp. 1223–1236, 2017.

[20] H. Lee, D. Lee, J. Moon et al., "An improved anonymous authentication scheme for roaming in ubiquitous networks," *PLoS One*, vol. 13, no. 3, Article ID e0193366, 2018.

[21] G. Zhang, D. Fan, Y. Zhang, X. Li, and X. Liu, "A privacy preserving authentication scheme for roaming services in global mobility networks," *Security and Communication Networks*, vol. 8, no. 16, pp. 2850–2859, 2015.

[22] F. Wu, L. Xu, S. Kumari et al., "A novel and provably secure authentication and key agreement scheme with user anonymity for global mobility networks," *Security and Communication Networks*, vol. 9, no. 16, pp. 3527–3542, 2016.

[23] J. Srinivas, D. Mishra, S. Mukhopadhyay et al., "An authentication framework for roaming service in global mobility networks," *Information Technology and Control*, vol. 48, no. 1, pp. 129–145, 2019.

[24] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Review*, vol. 41, no. 2, pp. 303–332, 1999.

[25] M. Numan, F. Subhan, W. Z. Khan et al., "A systematic review on clone node detection in static wireless sensor networks," *IEEE Access*, vol. 8, pp. 65450–65461, 2020.

[26] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Systems Journal*, vol. 11, no. 4, pp. 2590–2601, 2016.

[27] J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun, "A lightweight multi-layer authentication protocol for wireless body area networks," *Future Generation Computer Systems*, vol. 78, pp. 956–963, 2018.

[28] H. Zhu, Y.-A. Tan, L. Zhu, X. Wang, Q. Zhang, and Y. Li, "An identity-based anti-quantum privacy-preserving blind authentication in wireless sensor networks," *Sensors*, vol. 18, no. 5, p. 1663, 2018.

[29] D. He and S. Zeadally, "An analysis of RFID authentication schemes for Internet of Things in healthcare environment using elliptic curve cryptography," *IEEE Internet of Things Journal*, vol. 2, no. 1, pp. 72–83, 2015.

[30] P. Zhang, H. Jiang, J. Cai et al., "Recent research progress of lattice cryptography," *Computer Research and Development*, vol. 54, no. 10, pp. 2121–2129, 2017.

[31] B. A. Alzahrani, S. A. Chaudhry, A. Barnawi, A. Al-Barakati, and M. H. Alsharif, "A privacy preserving authentication scheme for roaming in IoT-based wireless mobile networks," *Symmetry*, vol. 12, no. 2, p. 287, 2020.

[32] S. Khatoon and B. Singh Thakur, "Cryptanalysis and improvement of authentication scheme for roaming service in ubiquitous network," *Cryptologia*, pp. 1–26, 2020.

[33] A. Ostad-Sharif, A. Babamohammadi, D. Abbasinezhad-Mood et al., "Efficient privacy-preserving authentication scheme for roaming consumer in global mobility networks," *International Journal of Communication Systems*, vol. 32, no. 5, p. e3904, 2019.

[34] Y. Lu, G. Xu, L. Li et al., "Robust privacy-preserving mutual authenticated key agreement scheme in roaming service for global mobility networks," *IEEE Systems Journal*, vol. 13, no. 2, pp. 1454–1465, 2019.

[35] Q. Xie, B. Hu, X. Tan, and D. S. Wong, "Chaotic maps-based strong anonymous authentication scheme for roaming services in global mobility networks," *Wireless Personal Communications*, vol. 96, no. 4, pp. 5881–5896, 2017.

[36] P. Gope and T. Hwang, "Lightweight and energy-efficient mutual authentication and key agreement scheme with user anonymity for secure communication in global mobility networks," *IEEE Systems Journal*, vol. 10, no. 4, pp. 1370–1379, 2016.

[37] X. Li, J. Ma, W. Wang, Y. Xiong, and J. Zhang, "A novel smart card and dynamic ID based remote user authentication scheme for multi-server environments," *Mathematical & Computer Modelling*, vol. 58, no. 1-2, pp. 85–95, 2013.

[38] X. Li, J. Niu, M. Khurram Khan, and J. Liao, "An enhanced smart card based remote user password authentication scheme," *Journal of Network and Computer Applications*, vol. 36, no. 5, pp. 1365–1371, 2013.

[39] X. Li, Y. Xiong, J. Ma, and W. Wang, "An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards," *Journal of Network and Computer Applications*, vol. 35, no. 2, pp. 763–769, 2012.

[40] X. Li, J.-W. Niu, J. Ma, W.-D. Wang, and C.-L. Liu, "Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 73–79, 2011.

[41] D. He and D. Wang, "Robust biometrics-based authentication scheme for multiserver environment," *IEEE Systems Journal*, vol. 9, no. 3, pp. 816–823, 2015.

[42] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 9, pp. 2467–2476, 2017.

[43] P. Vijayakumar, V. Chang, L. Jegatha Deborah, B. Balusamy, and P. G. Shynu, "Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks," *Future Generation Computer Systems*, vol. 78, pp. 943–955, 2018.

[44] S. H. Islam, M. S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li, and M. K. C. Reddy, "A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs," *Future Generation Computer Systems*, vol. 84, pp. 216–227, 2018.

[45] P. Vijayakumar, M. Azees, V. Chang, J. Deborah, and B. Balusamy, "Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks," *Cluster Computing*, vol. 20, no. 3, pp. 2439–2450, 2017.

[46] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad-hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, 2015.

[47] M. Ajtai and C. Dwork, "A public-key cryptosystem with worst-case/average-case equivalence," in *Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing—STOC'97*, pp. 284–293, Seattle, WA, USA, May 1997.

[48] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: a ring-based public key cryptosystem," *Lecture Notes in Computer Science*, pp. 267–288, Springer, Berlin, Heidelberg, 1998.

[49] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proceedings of the 41st Annual ACM Symposium on Symposium on Theory of Computing—STOC'09*, pp. 169–178, Bethesda, MD, USA, May 2009.

[50] D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems: A Cryptographic Perspective*, Springer Science & Business Media, Berlin, Heidelberg, 2012.

[51] J. Hoffstein and J. H. Silverman, "Implementation notes for NTRU PKCS multiple transmissions," NTRU Cryptosystems Technical report, 1998.

[52] J. Hoffstein and J. Silverman, "Optimizations for NTRU," *Public-Key Cryptography and Computational Number Theory*, pp. 77–88, De Gruyter, Berlin, Germany, 2001.

[53] E. Alkim, L. Ducas, T. Pöppelmann et al., "Post-quantum key exchange—a new hope," in *Proceedings of the 25th USENIX Security Symposium ({USENIX} Security 16)*, pp. 327–343, Austin, TX, USA, August 2016.

[54] J. Bos, C. Costello, L. Ducas et al., "Frodo: take off the ring! practical, quantum-secure key exchange from LWE," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ACM, Vienna Austria, pp. 1006–1018, October 2016.

[55] J. W. Bos, C. Costello, M. Naehrig et al., "Post-quantum key exchange for the TLS protocol from the ring learning with errors problem," in *Proceedings of the 2015 IEEE Symposium on Security and Privacy*, pp. 553–570, IEEE, San Jose, CA, USA, May 2015.

[56] C. Peikert, *Lattice Cryptography for the Internet*, pp. 197–219, Springer, Cham, Switzerland, 2014.

[57] A. Fujioka, K. Suzuki, K. Xagawa, and K. Yoneyama, "Strongly secure authenticated key exchange from factoring, codes, and lattices," *Designs, Codes and Cryptography*, vol. 76, no. 3, pp. 469–504, 2015.

[58] M. Abouaroek and K. Ahmad, "Node authentication using NTRU algorithm in opportunistic network," *Scalable Computing: Practice and Experience*, vol. 20, no. 1, pp. 83–92, 2019.

[59] J. Hoffstein, N. Howgrave-Graham, J. Pipher et al., *NTRU-SIGN: Digital Signatures Using the NTRU lattice*, pp. 122–140, Springer, Berlin, Germany, 2003.

[60] T. C. Clancy, R. W. McGwier, and L. Chen, "Post-quantum cryptography and 5G security: tutorial," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, p. 285, ACM, Miami, FL, USA, May 2019.

[61] S. H. Jeong, K. S. Park, and Y. H. Park, "Quantum resistant NTRU-based key distribution scheme for SIP," in *Proceedings of the 2018 International Conference on Electronics, Information, and Communication (ICEIC)*, IEEE, Honolulu, HI, USA, pp. 1-2, January 2018.

[62] T. Espitau, P. A. Fouque, B. Gérard, and M. Tibouchi, "Loop-abort faults on lattice-based signatures and key exchange protocols," *IEEE Transactions on Computers*, vol. 67, no. 11, pp. 1535–1549, 2018.

[63] M. Bellare, D. Pointcheval, and P. Rogaway, *Authenticated Key Exchange Secure against Dictionary Attacks*, pp. 139–155, Springer, Berlin, Germany, 2000.

[64] M. Bellare and P. Rogaway, *Entity Authentication and Key Distribution*, pp. 232–249, Springer, Berlin, Germany, 1993.

[65] M. Bellare and P. Rogaway, "Provably secure session key distribution: the three party case," in *Proceedings of the Twenty-Seventh Annual ACM Symposium on Theory of computing—STOC'95*, pp. 57–66, Las Vegas, NV, USA, May 1995.

[66] P. Flajolet, D. Gardy, and L. Thimonier, "Birthday paradox, coupon collectors, caching algorithms and self-organizing search," *Discrete Applied Mathematics*, vol. 39, no. 3, pp. 207–229, 1992.

[67] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, vol. 426, no. 1871, pp. 233–271, 1989.