IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received July 19, 2019, accepted July 31, 2019, date of publication August 6, 2019, date of current version August 21, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2933576

A Privacy-Preserving RLWE-Based Remote Biometric Authentication Scheme for Single and Multi-Server Environments

HAILONG YAO[1,2], **(Student Member, IEEE), CAIFEN WANG**[3], **XINGBING FU**[4,5,6], **CHAO LIU**[7], **BIN WU**[1], **AND FAGEN LI**[8]

[1]College of Mathematics and Statistics, Northwest Normal University, Lanzhou 730070, China
[2]School of Electronic and Information Engineering, Lanzhou City University, Lanzhou 730070, China
[3]College of Big Data and Internet, Shenzhen Technology University, Shenzhen 518118, China
[4]Guangdong Provincial Key Laboratory of Information Security Technology, Guangzhou 510275, China
[5]School of Cyberspace, Hangzhou Dianzi University, Hangzhou 310018, China
[6]Guangxi Key Laboratory of Cryptography and Information Security, Gulin 541004, China
[7]Department of Computer Science and Electrical Engineering, University of Maryland at Baltimore, Baltimore, MD 21201, USA
[8]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China

Corresponding authors: Caifen Wang (soloren@yeah.net) and Xingbing Fu (uestcfuxb@126.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61562077 and Grant 61772022, in part by the Opening Project of Guangdong Provincial Key Laboratory of Information Security Technology under Grant 2017B030314131-05, in part by the Gansu Natural Science Foundation under Grant 18JR3RA224, in part by the Gansu Higher Education Research Foundation under Grant 2018A-112, in part by the Zhejiang Province Natural Science Foundation of China under Grant LY19F020045, in part by the Department of Education of Zhejiang Province of China under Grant Y201636547, in part by the Guangxi Key Laboratory of Cryptography and Information Security under Grant GCIS201718, in part by the Key Research Project of Zhejiang Province under Grant 2017C01062, in part by the Fund of Lab of Security Insurance of Cyberspace, Sichuan Province, under Grant szjj2017-055, in part by the Cyberspace Subject of Hangzhou Dianzi University under Grant GK168800225075, in part by the Higher Education Research of Hangzhou Dianzi University, in 2017, and in part by the Research on the Innovation of Training Mode of the First Level Subject of Cyberspace Security under Grant YB201767.

ABSTRACT Lwamo *et al.* recently proposed a robust and efficient remote single and multi-server biometric authentication scheme using smart card and *RSA*. The scheme is vulnerable to the smart card lost attacks; therefore, the scheme cannot resist offline guessing attacks and user impersonation attacks, and cannot provide forward security and user anonymity. To address these issues, we propose a new privacy-preserving ring learning with errors (*RLWE*)-based remote biometric authentication scheme (*RRBAS*) for single and multi-server environments. *RRBAS* is the first lattice-based remote biometric authentication scheme for multi-server environments. Security analysis show that *RRBAS* can satisfy the authenticated key exchange (*AKE*) security in the random oracle model, resist known security attacks, and provide post-quantum security. The experimental evaluation and comparative analysis show that *RRBAS*'s computational efficiency is better than that of Lwamo *et al.*, while the communication efficiency is slightly lower than traditional schemes because of the large-size ciphertext of the lattice-based cryptosystem, but it is fully capable of session key agreement in single and multi-server environments.

INDEX TERMS Authenticated key exchange, biometric authentication, privacy-preserving, *RLWE*.

I. INTRODUCTION

As the information society becomes more developed, the higher the reliance on information, and the higher the security requirements for sensitive information during the processes of information storage, exchange, and use. The development of modern communication technologies facilitates information exchanges that are almost free of time and space constraints. However, information security continues to be a concern. To achieve data security and user privacy in remote communications, a privacy-preserving remote authentication scheme (*RAS*) is proposed.

In 1981, Lamport proposed a password-based identity authentication protocol for a single-server environment [25].

The associate editor coordinating the review of this manuscript and approving it for publication was Zahid Akhtar.

2169-3536 © 2019 IEEE. Translations and content mining are permitted for academic research only.
Personal use is also permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

Subsequently, some improved schemes and similar single-server environments *RAS* have been proposed [27], [42], [47], [48]. Such schemes require users to register for each application server one by one and they may need to set different passwords to achieve security and eliminate linkability between registration data. However, it is costly to record and use these passwords when the number of servers is large and storing the same user's information on each server is inefficient and uneconomic. To overcome these drawbacks, the multi-server environment *RAS* have been proposed in the literature [1], [10]–[20], [43], [46]. Users only need to register once in a trusted registration center (*RC*) to authenticate and negotiate the session key with the third-party remote server registered in the same registry. In recent years, to meet new application requirements and their corresponding security objectives, *RAS* has been improved from being a single password authentication scheme into a multi-factor combination authentication scheme, such as password, smart cards, and biometrics. Security assumptions have been improved from hash functions, large integer factoring problems, discrete logarithm problems (*DLP*) in finite fields to *DLP* over elliptic curve (*ECDLP*) [29]–[32], and even post-quantum security assumptions such as lattice hard problems [33]–[35]. The cryptography also uses a public key encryption that is adapted to privacy.

Although many of the existing remote authentication schemes have achieved good security and usability, there are several issues to be addressed.

1) ***Vulnerable to hardware loss attack***. The easy loss of hardware authentication factors is the weakness of hardware-based schemes, such as smart cards. With the development of side-channel attack technology, some hardware-based schemes are vulnerable to hardware loss attacks [24]. Lwamo *et al.* [1], Li *et al.* [18] and Challa *et al.* [20] even lost its anonymity and forward security.
2) ***Vulnerable to offline guessing attack***. Some smart card-based schemes use smart card local authentication methods on the user side; therefore, the smart card must store the secrets necessary for authentication [1], [10], [11]. Once the smart card is lost, there is a possibility that the scheme will be destroyed by an offline password attack [2], [3]. It is also possible for an adversary to launch a centre search attacks against biometric security [8], [9].
3) ***Vulnerable to user impersonation attack***. As mentioned above, the user side of most smart card-based schemes adopts smart card local authentication. The *RC* is only responsible for issuing certificates and assisting authentication, but not storing user information; therefore, the schemes are vulnerable to user impersonation attacks caused by offline guessing attacks [1], [11], [16], [17]. Even some schemes use an offline *RC* and the key agreement process is related only to the secrets on the smart card, it is still possible for the adversary to bypass the local authentication and directly launch the user impersonation attacks [1].
4) ***Vulnerable to user quantum attack***. The development of quantum computing technology poses a huge security threat to *RAS* based on classical number theoretical hard problems. The existing *RAS* for multi-server environments are based on classical number theory problems, while existing post-quantum *RAS* are only suitable for single-server environments [6], [56]–[58], [60].

As mentioned above, some hardware-based *RAS* are vulnerable to hardware loss attacks. Local authentication and even offline *RC* mode, while reducing communication overhead and improving protocol efficiency, may lead to offline guessing attacks and biometric security attacks, which may result in user impersonation attacks. Finally, traditional *RAS* cannot resist quantum attacks.

A. OUR CONTRIBUTIONS

To overcome the above challenges, this work proposes a privacy-preserving post-quantum security remote authentication scheme for single and multi-server environments. Following the security proof, performance analysis, and implementation evaluation, the proposed scheme makes up for all the shortcomings of *Lwamo2019* and other discussed schemes. We summarized our main contributions as follows:

Our scheme can provide authenticated key exchange (*AKE*) security in the random oracle model (*ROM*) and resist known security attacks. Both computational and communication overheads are achieved at a practical level. The computational overhead is even lower than that of the state-of-the-art works.

- We analyze the typical protocols such as *Lwamo2019* and find that these anonymous remote authentication protocols for multi-server environments are unable to achieve their claimed multi-factor security. And *Lwamo2019* is vulnerable to offline password guessing attacks and user impersonation attacks, and has forward security risks.
- We propose a privacy-preserving ring learning with errors (*RLWE*)-based remote biometric authentication scheme for single and multi-server environments (*RRBAS*), which is a distributed remote authentication system using hash functions to mask user IDs and passwords, protects the biometric information using fuzzy extractor [10], [23], and uses an efficient *RLWE*-based public key encryption scheme to achieve the security of this information during transmission.
- We give the formal proof and an informal security analysis of the proposed scheme. The results show that it can satisfy *AKE* security in the *ROM* and resist the known traditional and quantum attacks.
- We evaluate the performance of the proposed scheme through experimental implementation and comparative analyses. The results show that the computational and communication overheads of the proposed scheme are

practical and the computational overhead is even lower than that of the state-of-the-art works.

B. ORGANIZATION

The rest of this work is organized as follows. In Section 2, we briefly discuss the related work. Basic notations, *RLWE* security assumptions, *NewHope* public key encryption scheme and system model definition will be described in Section 3. The *Lwamo2019* is reviewed and its weaknesses are analyzed in Sections 4 and 5, respectively. We describe the details of our privacy-preserving remote authentication scheme in Section 6. The security analysis and performance evaluation will be given in Sections 7 and 8, respectively. Finally, we present our conclusions in Section 9.

II. RELATED WORK

This section introduces the related research work for single and multi-server remote authentication schemes from the perspective of the two security assumptions of classical security and post-quantum security.

A. CLASSICAL-HARD-PROBLEM-BASED RAS

Most of the existing *RAS* are constructed on classical hard problems. In 1981, Lamport proposed the seminal work, *Lamport1981* based on the hash function [25]. Later, many password-based *RAS* were proposed [27], [28]. But they are vulnerable to the offline guessing attacks due to the weak password [36]. To overcome this security weakness, password and smart card-based two-factor *RAS* were proposed [37]–[39]. The security of the password-based *RAS* is significantly enhanced by the addition of smart cards. Such schemes are also widely used in campus and enterprise networks, and even e-banks because of their low cost and high usability. However, researcher quickly found that password and smart card-based RAS are still vulnerable to offline guessing attacks when the smart card is lost [2], [40], [41].

To overcome the problem of *RAS* security degradation caused by smart card loss, a third authentication factor is naturally introduced, such as biometrics or other out-of-band information (e.g., short message services [*SMS*] or email). However, for real-time and security considerations, it is not recommended to use *SMS* as the third authentication factor in *RAS* [45].

Pointcheval and Zimmer (2008) proposed the first provably secure three-factor AKE scheme [47]. They introduced a security model for multi-factor authenticated key exchange that combines a password, a secure device, and biometric authentications based on the ElGamal cryptosystem [50]. Since the ElGamal encryption scheme is bit-wise, the scheme is expensive and inefficient. Fan and Lin (2009) proposed another provably secure three-factor AKE scheme based on public-key encryption scheme [48]. In the login and authentication phase, the scheme also uses a symmetric encryption algorithm to ensure confidentiality. Combined with the advantages of public key and symmetric encryption tools, its computational efficiency is improved compared to Pointcheval-Zimmer's scheme. Yang and Yang (2010) proposed a three-factor AKE scheme based on the *DLP* [49], which is the first multi-factor AKE scheme for multi-server environments, but it is less efficient because it requires multiple exponential operations. Five months later, Yoon and Yoo proposed another multi-factor AKE scheme for multi-server environments based on *ECDLP* [43]. However, He et al. proved that Yoon-Yoo's scheme was vulnerable to the privileged insider attack, the masquerade attack and the smart cart lost attack [52], and an improvement was designed by He and Wang [51]. Chuang and Chen simultaneously revealed that Yoon-Yoo's scheme still had anonymity problems and proposed a lightweight anonymous multi-server authenticated key agreement scheme based on trust computing using nonce and hash functions [46]. In 2015, Odelu *et al.* [10] showed that He-Wang's scheme had weak anonymity and could not resist replay attack and user impersonation attack, while Lin *et al.* [53] showed that Chuang-Chen's scheme could not provide the claimed anonymity and could not resist user impersonation attacks, and server spoofing attacks.

Kumari and Om (2017) showed that Chuang-Chen's scheme could not resist intermediate data attacks, user impersonation attacks and lacks forward security [54]. Kumari and Om claimed that their improved scheme can provide non-repudiation as the authentication message sent by a user is signed by the server using the RSA digital signature; therefore, it can be resistant to all of the above attacks. Lwamo et al. (2018) found that Kumari-Om's scheme used too many exponential operations, resulting in excessive computational overhead. They proposed a new symmetric encryption and public key encryption-based remote authentication scheme for the single and multi-server environments to achieve lower computational overhead and higher security [1]. However, in this work, we show that Lwamo et al.'s scheme is vulnerable to smart card loss attack, and as a result, their scheme cannot resist the offline guessing attacks, user impersonation attacks, and lacks user anonymity. In addition, we show that their scheme cannot provide forward security.

B. LWE-BASED RAS

Post-quantum security is a new type of cryptographic primitive. *RAS* research based on post-quantum security assumptions focuses on lattice-based *RAS*, in particular, learning with errors (*LWE*)-based *RAS*. *LWE*'s post-quantum security is due to the error component in its structure; therefore, the key agreement protocol implemented with *LWE* can only obtain approximately equal values instead of expecting the same value. There are currently two main ideas for solving this challenge academically: the error reconciliation mechanism where the key technology is the error reconciliation method [55], and the public key encryption mechanism where its key technology is the ciphertext compression method.

Ding et al. (2012) invented an error reconciliation mechanism in which both parties can reconcile the same bits based on signal bits [56]. However, the common bits reconciled by this method can not obey the uniform distribution and a random extraction operation is required to obtain a random value. Peikert (2014) proposed an improved error reconciliation mechanism so that both parties can directly obtain uniformly distributed common bits [57]. Bos et al. (2015) demonstrated the practicality of post-quantum key agreement by constructing ciphersuites for the transport layer security protocol, which provides an *AKE* based on Peikert's reconciliation mechanism. Compared with the elliptic curve Diffie-Hellman (*ECDH*) scheme, this method has a higher communication overhead, but the computational complexity is quite close. Subsequently, Alkim et al. extended Peikert's reconciliation mechanism to lattice $\tilde{D}_4$ decoding and proposed a new *RLWE*-based point-to-point key exchange protocol, i.e., NewHope [6]. Compared with Bos et al.'s scheme, this method has a less than 50% communication overhead, but is more computationally efficient than *ECDH* scheme. In 2017, Xu et al. proposed the first password-based three-party *AKE* protocol over *RLWE* [59]. Our study found that the scheme could not provide anonymity and caused all-for-the-price-of-one attacks due to the public parameter *a* [6].

Bos et al.(2018) introduced a chosen plaintext attack (CPA)-secure public key encryption scheme based on Module-LWE, and designed a chosen ciphertext attack (CCA)-secure key agreement scheme based on this, i.e., Kyber [60]. Compared with NewHope, these schemes have similar performances, but Kyber has smaller communication overhead.

The schemes discussed above are single factor key agreement protocol, where [6], [56]–[58] require the cooperation of other signature protocol to achieve mutual authentication of entities. Only [59] is suitable for multi-server environments. In this work we propose the first *RLWE*-based three-factor remote biometric authentication scheme for single and multi-server environments.

III. PRELIMINARIES

In this section, we describe the preliminaries which is necessary to understand the rest of this work.

A. NOTATIONS

In this work, we use the symbol $\mathbb{F}_q$ to represent the finite field with q elements. The polynomial ring $R = \mathbb{Z}/\left(x^d + 1\right)$, d is a power of 2. We write elements of R in lowercase, e.g., $r \in R$. The notation $r\,[i]$ refers to the i-th coefficients of r. For $r \in R$, we use the notation $[r]_q$ to refer to $r \bmod q$, with coefficients reduced into the range $(-q/2, q/2]$. We write the dot product of $a, b \in R$ as $\langle a, b\rangle = \sum_{i=1}^{n} a\,[i] \cdot b\,[i]$. The symbol $f\,(\cdot)$ represents that the function is run by the input specification. Other symbols used in this work and their descriptions are shown in Table 1.

B. RLWE

Learning with error over ring (*RLWE*) is a famous variant of the Learning with error (*LWE*) problem, which replaces the inner product in *LWE* with a polynomial product. Lyubashevsky et al. introduced this problem in [4] and gave the quantum reduction of the worst-case approximate shortest vector problem SVP_γ over ring to the search *RLWE* in [5].

Lemma 1 (RLWE security assumptions): For security parameter λ, let $f\,(x) = \left(x^d + 1\right)$, let $q \geq 2$ be an integer. Let $R = \mathbb{Z}/f\,(x)$ and $R_q = R/qR$. Let χ be a distribution over R, $a, s \in R_q$ and $e \in \chi$, construct distribution $A_{s,e} = (a, \langle a, s\rangle + e)$. Then, it is difficult to find s from any number of independent instances of the distribution $A_{s,e}$, i.e., search *RLWE* (*SRLWE*) problem. It is also difficult to distinguish between an instance of the distribution $A_{s,e}$ and a uniform distribution over the distribution R_q^2 with a non-negligible probability $(1 - negl\,(\lambda))$, i.e., decision *RLWE* (*DRLWE*) problem, where $negl\,(\lambda)$ is a negligible probability function.

C. NEWHOPE-CPA-PKE

Alkim et al. proposed a semantic secure public key encryption (PKE) scheme with respect to adaptive chosen plaintext attacks based on the work [6], i.e., *NewHope-CPA-PKE*. The PKE can be used to construct a *RLWE*-based key exchange protocol with CPA semantic security. In this section, we briefly introduce its three main algorithms: key generation algorithm $NPKE.Gen\,(\cdot)$, encryption algorithm $NPKE.Enc\,(\cdot)$ and decryption algorithm $NPKE.Dec\,(\cdot)$ [7].

- $NPKE.Gen\,()$: First, Alice selects a 256-bit random seed *seed*, generates $a \in R_q$ with $GenA\,(seed)$, and generates $s, e \in R_q$ with $Sample\,(seed, nonce)$. See Algorithm 5 and Algorithm 4 of literature [7] for details. Second, computes $b = \langle a, s\rangle + e$. Finally, returns $pk = (b, seed)$, $sk = s$.
- $NPKE.Enc\,(\mu, pk)$: First, Bob encodes message $\mu \in \{0, 1\}^{256}$ into $\mu' \in R_q$ with $Encode\,(\mu)$, generates $a \in R_q$ with $GenA\,(seed)$, and generates $s', e', e'' \in \psi_8^n$ with $Sample\,(seed, nonce)$. See Algorithm 10, Algorithm 5 and Algorithm 4 of literature [7] for details. Second, computes $u = \langle a, s'\rangle + e'$ and $v = \langle b, s'\rangle + e'' + \mu'$. Finally, returns $c = (u, v)$.
- $NPKE.Dec\,(c, sk)$: Alice computes $\mu' = v - \langle u, s\rangle$ and returns $\mu = Decode\left(\mu'\right)$, where, $Decode\,(\cdot)$ is the message decoding algorithm. See Algorithm 11 of literature [7] for details.

Theorem 1 (IND-CPA security of NewHope-CPA-PKE): Let n and q be integers. Let χ be a probability distribution on R_q. For any quantum algorithm $\mathcal{A}$ against the

TABLE 1. Notations.

Notations	Descriptions
$U_i/UID_i/PW_i/Bio_i/SC_i$	User/ID/Password/Biometrics/Smart card
$AS_j/SID_j/pk_j/sk_j$	Application server/ID/Public & secret key
$RC/pk/sk$	Registration center/Public & secret key
E_k/D_k	Symmetric encryption algorithm for k
$Gen\,(\cdot)\,/Rep\,(\cdot)$	Fuzzy extractor algorithm
$h\,(\cdot)$	Cryptographic hash algorithm
$\leftarrow / \perp$	Normal output / Abnormal output
$\oplus/\|$	XOR operator / Concatenation operator
$\overset{\$}{\leftarrow}$	Sampling from the given distribution

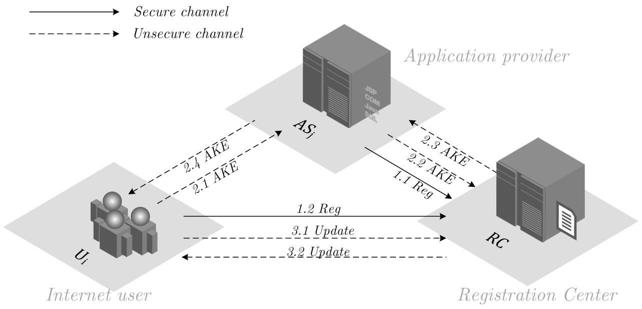


FIGURE 1. Communication model of remote authentication scheme.

indistinguishability under CPA (IND-CPA) security of *NewHope-CPA-PKE*, there exists quantum algorithms $\mathcal{B}_1$ and $\mathcal{B}_2$ against the DRLWE problem such that

$$Adv_{NewHope-CPA-PKE}^{IND-CPA}(\mathcal{A}) \le Adv_{n,q,\chi}^{DRLWE}(\mathcal{B}_1) + Adv_{n,q,\chi}^{DRLWE}(\mathcal{B}_2). \quad (1)$$

Moreover, the running times of $\mathcal{B}_2$ and $\mathcal{B}_1$ are the same as that of $\mathcal{A}$, see the *Theorem 4.4* of [7] for details.

D. SYSTEM MODEL

1) COMMUNICATION MODEL

The network of a remote authentication scheme for the single and multi-server environments is depicted in Figure 1. It consists of three entities: Internet user U_i, application server AS_j and registration center RC. In the single server environments, the application server and the registration server are combined into one.

RC is a trusted or semi-honest third-party server whose role is to initialize the system and generate system parameters. U_i and AS_j could negotiate the session key without the pre-shared secret with the help of the RC.

AS_j is a service provider server that provides users with specific Internet services and is one of the subjects of authentication. Application servers are typically deployed on private or public clouds, and their functionality and security are better than those of user devices.

U_i is a user of various Internet services and is another subject of authentication. A variety of user entities are the main components of the Internet, but their resources and security are limited.

2) SECURITY GOALS

In addition to ensure the privacy of the private key of RC, the scheme should also meet the following security goals.

- Session key security: The main security goal of the scheme is to negotiate a secure session key between the U_i and AS_j with the help of the RC, and to ensure the privacy of the key to the RC.
- Mutual authentication: To ensure the security and effectiveness of the scheme, it must be mutual authentication between participating entities.
- Multi-factor security: When the adversary only gets any two of the three factors, the system is safe and does not increase the advantage of obtaining the third one.
- Forward security: The scheme has forward security, meaning that even if the adversary obtains all the long-term secret factors of all protocol entities, and it can't improve the advantage of destroying the security of the previously established session key.
- Privacy security: Biometric-based *RAS* privacy security includes two aspects: anonymity [2] and biometric security [8]. Anonymity has two meanings, which are the user's identity privacy and untrackability. User identity privacy is user ID protection, and user untrackability is the unlinkable of user sessions. Biometric security also includes two aspects, which are the security of fresh biometric samples and the security of the biometric templates stored on the other devices. The security of a fresh biometric sample is whether the sample is protected from leakage when the scheme encounters a social engineering attack or a brute force attack. The biometric template security is whether the template can be prevented from leaking when the protocol encounters a brute force attack or other template recovery attack. A valid template recovery attack is a centre search attack [9].
- Resilience to other known attacks: The scheme should resist known attacks on the Internet, such as intermediate data attacks, and privileged insider attacks and so on.

3) ADVERSARY MODEL

Let $\mathcal{P}$ is an *AKE* protocol, and P_i^x denotes the x-th session instance of the protocol participant $P_i = \left(U_i, AS_j, RC\right)$. During the running of the protocol, multiple parallel sessions are allowed to execute. The security of $\mathcal{P}$ is modeled by hybrid games between a challenger $\mathcal{C}$ and a probability polynomial time (PPT) adversary $\mathcal{A}$, $\mathcal{C}$ simulates the output of participant in accordance with the protocol, the event $\mathcal{A}$ winning the game is denoted as *Succ*. The ability of the $\mathcal{A}$ is simulated by the following oracle queries:

- $Execute\left(U_i^x, AS_j^y\right)$: This oracle simulates a passive attack, and the output is the interaction information of U_i and AS_j during protocol is run.
- $SendU2RC\,(RC^z, m)$: This oracle simulates an active attack by $\mathcal{A}$ impersonating an application-side entity to RC. Since mutual authentication between U_i and AS_j is implemented by means of RC, we have reason to suspect that the messages transmitted by U_i and AS_j before the mutual authentication are forged. $\mathcal{A}$ sends a message m to instance RC^z directly, $\mathcal{C}$ returns the processing result of m to $\mathcal{A}$ in accordance with the protocol. In addition, $Send\,(P^x, Start)$ is used to initiate a session.
- $SendRC2AS\left(AS_j^y, m\right)$: This oracle simulates an active attack by $\mathcal{A}$ impersonating to AS. $\mathcal{A}$ sends a message m

to instance AS_j^y, $\mathcal{C}$ returns the processing result of m to $\mathcal{A}$ in accordance with the protocol.

- *SendAS2U* $\left(U_i^x, m\right)$: This oracle simulates an active attack by $\mathcal{A}$ impersonating to U_i. $\mathcal{A}$ sends a message m to instance AS_j^y, $\mathcal{C}$ returns the processing result of m to $\mathcal{A}$ in accordance with the protocol.
- *Reveal* $\left(U_i^x, AS_j^y\right)$: This oracle simulates the known session key attack. On receiving this query, returns the established session key.
- *Corrupt* $\left(U_i^x, PW_i\right)$: This oracle simulates that the user is partially corrupted and output the PW_i of U_i.
- *Corrupt* $\left(U_i^x, Bio_i\right)$: This oracle simulates that the user is partially corrupted and output the Bio_i of U_i.
- *Corrupt* $\left(U_i^x, SC_i\right)$: This oracle simulates that the user is partially corrupted and output the α_i, δ_i, γ_i of SC_i.
- *Corrupt* (P^x): This oracle is only used to describe forward security, that is, when $\mathcal{A}$ obtains all long-term secrets of all protocol entities, the session key that has been established are safe. The *RC* in this protocol may be honest and curious. We only assume that the private key of *RC* is leaked when evaluating the forward security of the session key.
- *Test* $\left(U_i^x, AS_j^y\right)$: This oracle does not simulate the attack ability of $\mathcal{A}$, but is used to define the semantic security of the session key, which is only valid for fresh sessions (Definition 1). Returns $\perp$ if the session key of instance has not been established, otherwise returns the session key only if $\mathcal{A}$ wins the coin flipping game, otherwise returns a random string of the same length as the session key. The privacy of the session key to *RC* the is also captured by this oracle.

Definition 1 (Freshness):

An instance P^x is fresh if the following facts are true:

1) Instance P^x accepts the protocol, runs and generates session key.
2) *Reveal* $(\cdot)$ has not been asked.
3) *Corrupt* $(\cdot)$ has not been asked until the protocol was terminated.

Definition 2 (Adversary advantage): The advantage of an adversary $\mathcal{A}$ in destroying the *AKE* semantic security of the protocol $\mathcal{P}$, is defined as

$$Adv_{\mathcal{P}}^{AKE}(\mathcal{A}) = |2 \cdot Pr[Succ] - 1|. \tag{2}$$

Definition 3 (AKE security):

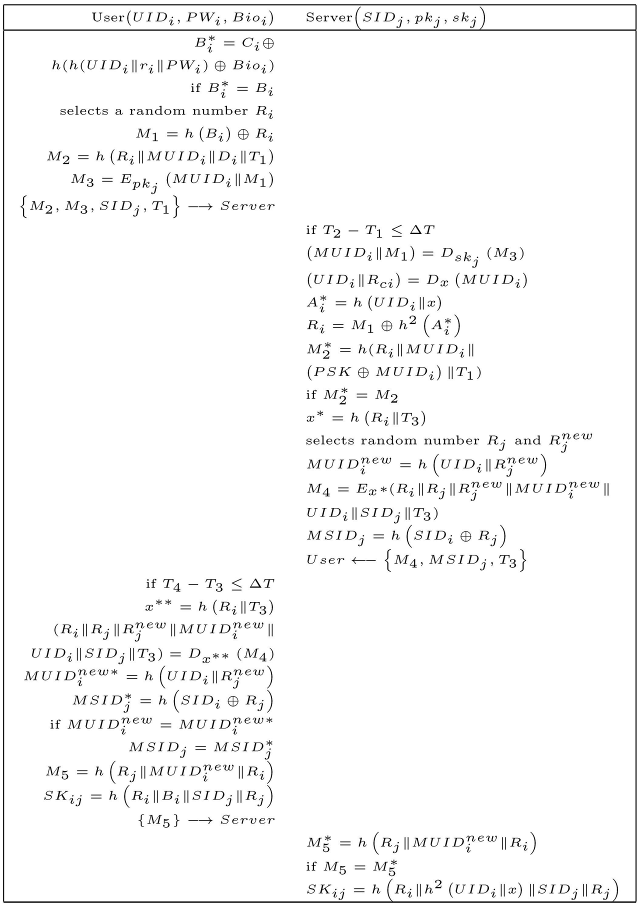
A protocol $\mathcal{P}$ is said to be AKE secure if the adversary advantage $Adv_{\mathcal{P}}^{AKE}$ is negligible.

IV. REVIEW OF THE *Lwamo2019*

In order to facilitate the understanding of the subsequent cryptanalysis of *Lwamo2019*, in this section we briefly review the registration and authentication process of it [1].

A. SERVER REGISTRATION

The application server sends identity SID_j and its public key pub_j to RC through a secure channel. The RC then replies to the server with a secure key PSK and a secret value x through a secure channel [1].



User(UID_i, PW_i, Bio_i)	Server$\left(SID_j, pk_j, sk_j\right)$
$B_i^* = C_i \oplus$	
$h(h(UID_i \| r_i \| PW_i) \oplus Bio_i)$	
if $B_i^* = B_i$	
selects a random number R_i	
$M_1 = h(B_i) \oplus R_i$	
$M_2 = h(R_i \| MUID_i \| D_i \| T_1)$	
$M_3 = E_{pk_j}(MUID_i \| M_1)$	
$\left\{M_2, M_3, SID_j, T_1\right\} \longrightarrow Server$	
	if $T_2 - T_1 \leq \Delta T$
	$(MUID_i \| M_1) = D_{sk_j}(M_3)$
	$(UID_i \| R_{ci}) = D_x(MUID_i)$
	$A_i^* = h(UID_i \| x)$
	$R_i = M_1 \oplus h^2\left(A_i^*\right)$
	$M_2^* = h(R_i \| MUID_i \|$
	$(PSK \oplus MUID_i) \| T_1)$
	if $M_2^* = M_2$
	$x^* = h(R_i \| T_3)$
	selects random number R_j and R_j^{new}
	$MUID_i^{new} = h\left(UID_i \| R_j^{new}\right)$
	$M_4 = E_{x^*}(R_i \| R_j \| R_j^{new} \| MUID_i^{new} \|$
	$UID_i \| SID_j \| T_3)$
	$MSID_j = h\left(SID_i \oplus R_j\right)$
	$User \longleftarrow \left\{M_4, MSID_j, T_3\right\}$
if $T_4 - T_3 \leq \Delta T$	
$x^{**} = h(R_i \| T_3)$	
$(R_i \| R_j \| R_j^{new} \| MUID_i^{new} \|$	
$UID_i \| SID_j \| T_3) = D_{x^{**}}(M_4)$	
$MUID_i^{new*} = h\left(UID_i \| R_j^{new}\right)$	
$MSID_j^* = h\left(SID_i \oplus R_j\right)$	
if $MUID_i^{new} = MUID_i^{new*}$	
$MSID_j = MSID_j^*$	
$M_5 = h\left(R_j \| MUID_i^{new} \| R_i\right)$	
$SK_{ij} = h\left(R_i \| B_i \| SID_j \| R_j\right)$	
$\{M_5\} \longrightarrow Server$	
	$M_5^* = h\left(R_j \| MUID_i^{new} \| R_i\right)$
	if $M_5 = M_5^*$
	$SK_{ij} = h\left(R_i \| h^2(UID_i \| x) \| SID_j \| R_j\right)$

FIGURE 2. Login and authentication of *Lwamo2019*.

B. USER REGISTRATION

The user selects a random number r_i, computes $MPW_i = h(UID_i \| r_i \| PW_i)$ and $REG(\cdot) = (MPW_i \oplus Bio_i)$, and sends tuple $\{UID_i, REG(\cdot)\}$ to RC. The RC then computes $A_i = h(UID_i \| x)$, $B_i = h(A_i)$ and $C_i = h(REG(\cdot)) \oplus B_i$. RC selects a random number R_{ci}, computes $MUID_i = E_x(UID_i \| R_{ci})$ and $D_i = PSK \oplus MUID_i$, and stores them into the smart card SC_i. Finally, the user writes r_i into smart card, then $SC_i = \{MUID_i, r_i, B_i, C_i, D_i, h(\cdot)\}$.

C. LOGIN AND AUTHENTICATION PROCESS

The login and authentication process of *Lwamo2019* is shown in Figure 2.

V. WEAKNESSES OF *Lwamo2019*

In this section, we show that *Lwamo2019* is vulnerable to smart card lost attack and thus cannot resist offline password guessing attack and user impersonation attack, and has other security flaw [1].

A. OFFLINE PASSWORD GUESSING ATTACK

Lwamo2019 adopts the offline authentication mode, and user device initiates a key agreement request after the smart card authenticating the user with $B_i^* = C_i \oplus h(h(UID_i \| r_i \| PW_i) \oplus Bio_i)$. The offline mode and local authentication decisions that lack RC security protection are convenient for offline password guessing attacks. Under the non-tamper-resistance assumption about the smart card [2] and the three-factor security assumption [1], after the adversary gets the smart card and biometric, the offline password guessing attack could be implemented. Details are as follows:

Step 1 The adversary uses the side channel attack technique to get the secrets $\{MUID_i, r_i, B_i, C_i, D_i, h(\cdot)\}$ on the smart card.

Step 2 The adversary guesses $\left(UID_i^*, PW_i^*\right)$ from the user identity space D_{UID} and the password space D_{PW}.

Step 3 The adversary computes $B_i^* = C_i \oplus h(h(UID_i \| r_i \| PW_i) \oplus Bio_i)$.

Step 4 If $B_i^* = B_i$ is true, the adversary wins the attack game, otherwise goes back to *Step 2*.

The time complexity of the above attack is $\mathcal{O}((2T_h + 2T_{XOR}) \cdot |D_{UID}| \cdot |D_{PW}|)$. Where T_h is the hash operation cost and T_{XOR} is the XOR operation cost. Typically, user's *UID* and *PW* are low entropy strings for ease of memory and use. Therefore, the actual advantage of the adversary is even higher [3].

B. USER IMPERSONATION ATTACK

The lack of multi-factor security is likely to lead to user impersonation attack, but there is another possibility of user impersonation attack in *Lwamo2019*. As analyzed in the previous section, *Lwamo2019* uses *RC* offline local authentication method. Once the smart card computes and determines that $B_i^* = B_i$ is true, a key negotiation request could be initiated. However, the calculation of all messages in the subsequent process only requires the secrets on the smart card, without any of UID_i, PW_i and Bio_i. This means that once the adversary gets the secrets $\{MUID_i, r_i, B_i, C_i, D_i, h(\cdot)\}$ on the smart card, it could spoof successfully the server by selecting the random number R_i and faking $\{M_2, M_3\}$ to start a user impersonation attack, because it thinks that the local authentication is negligible. The adversary can easily fake the M_5 because the calculated $x^{**} = h(R_i \| T_3)$ could correctly decrypt the M_4. Eventually it will have the same session key $SK_{ij} = h\left(R_i \| B_i \| SID_j \| R_j\right)$ as the server.

M_4 is like a big gift box. After decryption, it is all a surprise, $\left(R_i \| R_j \| R_j^{new} \| MUID_i^{new} \| UID_i \| SID_j \| T_3\right) = D_{x^{**}}(M_4)$. As someone wishes, UID_i and SID_j appear hand in hand, and user anonymity is lost.

C. FORWARD SECURITY ATTACK

Forward security requires that the established session key be secure even if the long-term secrets of all protocol entities are compromised. In *Lwamo2019*, if the adversary obtains the server private key sk_j and the secrets in the user's smart card, it could derive the session key associated with it based on the captured login and authentication information $\left\{M_2, M_3, SID_j, T_1\right\}$ and $\left\{M_4, MSID_j, T_3\right\}$. Details are as follows:

Application Server$\left(AS_j, SID_j\right)$	Registration Server(RS, pk, sk)
$\left\{SID_j\right\} \longrightarrow RS$	
	$v_j^* \xleftarrow{\$} \{0,1\}^{256}$
	$MSID_j \leftarrow h\left(SID_j\right)$
	$SIK_j \leftarrow h\left(MSID_j \| v_j^* \| sk\right)$
	$T_S \leftarrow \left[MSID_j, v_j^*\right]$
	$AS_j \longleftarrow \left\{SIK_j\right\}$

FIGURE 3. Application server registration of our scheme.

Step 1 The adversary uses the side channel attack technique to get the secrets $\{MUID_i, r_i, B_i, C_i, D_i, h(\cdot)\}$ on the smart card.

Step 2 The adversary decrypts M_3 to get M_1.

Step 3 The adversary computes $R_i = M_1 \oplus h(B_i)$ and $x^{**} = h(R_i \| T_3)$.

Step 4 The adversary decrypts M_4 to get R_j, and computes $SK_{ij} = h\left(R_i \| B_i \| SID_j \| R_j\right)$.

The adversary only gets UID_i, secret x and server private key sk_j can still destroy the forward security of *Lwamo2019*. Details are as follows:

Step 1 The adversary decrypts M_3 to get M_1.

Step 2 The adversary computes $A_i = h(UID_i \| x)$, $B_i = h(A_i)$, $R_i = M_1 \oplus h(B_i)$ and $x^{**} = h(R_i \| T_3)$.

Step 3 The adversary decrypts M_4 to get R_j, and computes $SK_{ij} = h\left(R_i \| B_i \| SID_j \| R_j\right)$.

VI. RRBAS

In this section, we propose a new remote single and multi-server biometric authentication scheme using *RLWE*, i.e., *RRBAS*, which withstands the security pitfalls of *Lwamo2019* and provides post-quantum security. *RRBAS* consists of three entities: user, application server, and registration center. The protocol consists of five phases: initialization phase, application registration phase, user registration phase, authentication and key agreement phase, and user's long-term secret update phase.

A. INITIALIZATION

In this phase, the registration center *RC* generates system parameters. First, it runs the key generation algorithm $NPKE.Gen(\cdot)$ to generate system key (pk, sk). Then, it selects fuzzy extractor algorithms $Gen(\cdot)/Rep(\cdot)$ and secure hashing algorithms $h(\cdot)$. Finally, it keeps *sk* and announces other parameters.

B. APPLICATION SERVER REGISTRATION

In this phase, AS_j needs to register with *RC*. As described in Figure 3, the details are as follows:

1) AS_j selects SID_j and sends the tuple $\left\{SID_j\right\}$ to *RC* to request the registration by secure communication.
2) *RC* selects a 256-bit random number v_j^*, and computes $MSID_j$ and SIK_j.
3) *RC* writes $MSID_j$, v_j^* into table T_S.

User$(U_i, UID_i, PW_i, Bio_i)$	Registration Server(RS, pk, sk)
$(\alpha_i, \beta_i) \leftarrow Gen\,(Bio_i)$	
$MUID_i \leftarrow h\,(UID_i)$	
$MPB_i \leftarrow h(PW_i \| \beta_i)$	
$\{MUID_i, MPB_i\} \longrightarrow RS$	
	$v_i^* \xleftarrow{\$} \{0,1\}^{256}$
	$UIK_i \leftarrow h(MUID_i \| v_i^* \| sk)$
	$\delta_i \leftarrow UIK_i \oplus MPB_i$
	$\gamma_i \leftarrow h(MUID_i \| MPB_i \| UIK_i)$
	write $\{\delta_i, \gamma_i\}$ into SC_i
	$T_U \leftarrow \left[MUID_i, v_i^*\right]$
	$U_i \longleftarrow \{SC_i\}$
insert α_i into SC_i	
then $SC_i = \{\alpha_i, \delta_i, \gamma_i\}$	

FIGURE 4. User registration of our scheme.

4) *RC* sends the tuple $\left\{SIK_j\right\}$ to AS_j by secure communication, then application server registration completes.

C. USER REGISTRATION

U_i submits registration information to *RC* which responds with the smart card SC_i. As described in Figure 4, the details are as follows:

1) U_i selects UID_i, PW_i and extracts biometric Bio_i using the sensor.
2) U_i uses $Gen(\cdot)$ of fuzzy extractor to generate (α_i, β_i), and computes $MUID_i$ and MPB_i, and sends the tuple $\{MUID_i, MPB_i\}$ to *RC* to request the registration by secure communication.
3) *RC* selects a 256-bit random number v_i^*, and computes UIK_i, δ_i and γ_i.
4) *RC* writes δ_i, γ_i into SC_i and issues it to U_i securely, and updates the user registry T_U.
5) U_i inserts α_i into SC_i and keeps it safe, then user registration completes.

D. AUTHENTICATION AND SESSION KEY AGREEMENT

In this phase, U_i and AS_j mutually authenticate each other's identity and create a session key to ensure subsequent communication security. As described in Figure 5, the details are as follows:

1) U_i inputs UID_i, PW_i' and extracts biometric Bio_i' using the sensor.
2) U_i uses $Rep(\cdot)$ of fuzzy extractor to computes β_i', and computes $MSID_j$, $MUID_i$ and MPB_i'.
3) U_i computes UIK_i', and determines if $\gamma_i = h(MUID_i \| MPB_i' \| UIK_i')$ is true, then goes to next step, otherwise abort the protocol.
4) U_i selects a 256-bit random number v_i, and computes CV_i and $CUID_i$, and generates the temporary public-private key pair (pk_i, sk_i) for this session.
5) U_i computes digest h_1, and sends the tuple $\{CUID_i, CV_i, pk_i, h_1\}$ to AS_j to request the authentication.
6) AS_j selects a 256-bit random number v_j, and computes CV_j, $CSID_j$ and digest h_2, and sends the tuple $\left\{CUID_i, CSID_j, CV_i, CV_j, h_1, h_2\right\}$ to *RC* to request the authentication.
7) *RC* recovers $MSID_j$ and v_j, and retrieves the table T_S by $MSID_j$, and if the corresponding entry $\left[MSID_j, v_j^*\right]$ is found, then goes to next step, otherwise abort the protocol.
8) *RC* computes SIK_j, and determines if $h_2 = h(MSID_j \| v_j \| h_1 \| SIK_j)$ is true, then goes to next step, otherwise abort the protocol.
9) *RC* recovers $MUID_i$ and v_i, and retrieves the table T_U by $MUID_i$, and if the corresponding entry $\left[MUID_i, v_i^*\right]$ is found, then goes to next step, otherwise abort the protocol.
10) *RC* computes UIK_i, and determines if $h_1 = h(MUID_i \| MSID_j \| v_i \| UIK_i \|)$ is true, then goes to next step, otherwise abort the protocol.
11) *RC* selects a 256-bit random number v_s, and computes H, MH_i and MH_j, and computes digests h_3 and h_4, and sends the tuple $\left\{MH_i, MH_j, h_3, h_4\right\}$ to AS_j to request the authentication.
12) AS_j recovers H from MH_j, determines if both $h_3 = h(H \| v_j \| SIK_j')$ is true, then goes to next step, otherwise abort the protocol.
13) AS_j generates a 256-bit random number *coin*, and uses *coin* as the seed to select a 512-bit random number $K \| coin'$, and computes c_{ij} and digest h_5, and sends the tuple $\left\{MH_i, c_{ij}, h_4, h_5\right\}$ to U_i to request the authentication and key agreement.
14) AS_j computes session key $ss = h\,(H \| K)$.
15) U_i recovers H from MH_i, determines if both $h_4 = h(H \| v_i \| UIK_i')$ and $h_5 = h(H \| c_{ij} \| h_4)$ are true, then goes to next step, otherwise abort the protocol.
16) U_i recovers K from c_{ij}, and computes session key $ss = h\,(H \| K)$.

E. UPDATE OF USER'S LONG-TERM SECRET

After U_i authenticates with the smart card, the password PW_i can be updated. If the credential UIK_i needs to be updated, the RC authentication must be passed. As described in Figure 6, the details of the process are similar to the previous authentication process, and will not be repeated here.

VII. SECURITY ANALYSIS

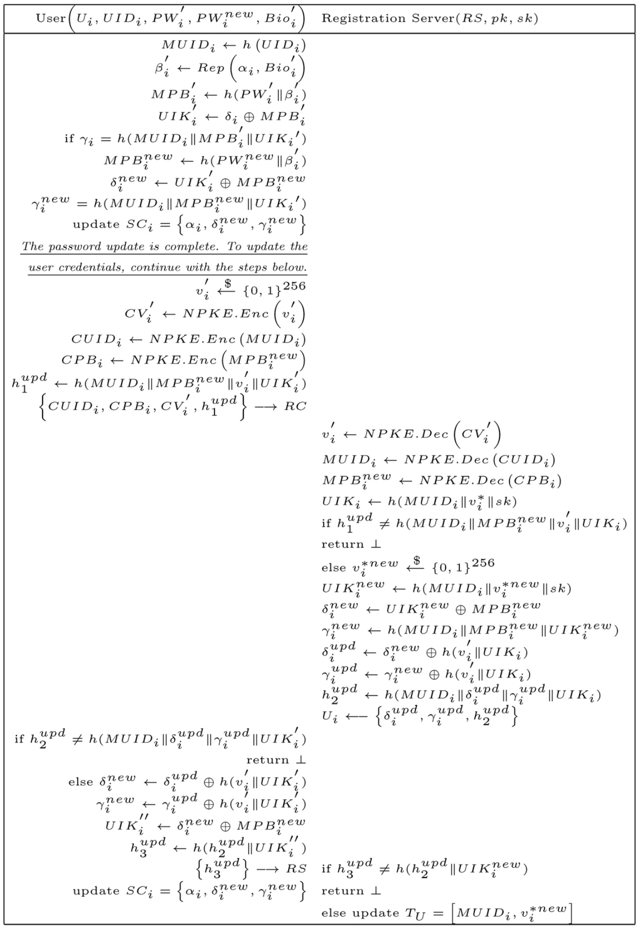
In this section, we show that the proposed scheme is provably secure under the security model defined in section 3. Moreover, some other security properties are discussed in the last subsection.

A. FORMAL PROOF

Theorem 2 (RRBAS is AKE Secure): Let $\mathcal{P}$ be our *RRBAS* protocol. If the *NewHope-CPA-PKE* satisfies the IND-CPA security, and the $h\,(\cdot)$ is random oracle. Let $\mathcal{A}$ be a PPT adversary against $\mathcal{P}$, who makes at most q_s *Send-query* and q_h *Hash-query*, the maximum advantage

User$\left(U_i, UID_i, PW_i^{'}, Bio_i^{'}\right)$	Application Server$\left(AS_j, SID_j, SIK_j^{'}\right)$	Registration Server(RS, pk, sk)
$MUID_i \leftarrow h\left(UID_i\right)$		
$MSID_j \leftarrow h\left(SID_j\right)$		
$\beta_i^{'} \leftarrow Rep\left(\alpha_i, Bio_i^{'}\right)$		
$MPB_i^{'} \leftarrow h(PW_i^{'} \| \beta_i^{'})$		
$UIK_i^{'} \leftarrow \delta_i \oplus MPB_i^{'}$		
if $\gamma_i = h(MUID_i \| MPB_i^{'} \| UIK_i{'})$		
$v_i \xleftarrow{\$} \{0,1\}^{256}$		
$CV_i \leftarrow NPKE.Enc\left(v_i\right)$		
$CUID_i \leftarrow NPKE.Enc\left(MUID_i\right)$		
$(pk_i, sk_i) \leftarrow NPKE.Gen\left(\cdot\right)$		
$h_1 \leftarrow h(MUID_i \| MSID_j \| v_i \| UIK_i^{'})$		
$I_1 = \{CUID_i, CV_i, pk_i, h_1\}$		
$I_1 \longrightarrow AS_j$		
	$v_j \xleftarrow{\$} \{0,1\}^{256}$	
	$CV_j \leftarrow NPKE.Enc\left(v_j\right)$	
	$MSID_j \leftarrow h\left(SID_j\right)$	
	$CSID_j \leftarrow NPKE.Enc\left(MSID_j\right)$	
	$h_2 \leftarrow h\left(MSID_j \| v_j \| h_1 \| SIK_j^{'}\right)$	
	$I_2 = \left\{CUID_i, CSID_j, CV_i, CV_j, h_1, h_2\right\}$	
	$I_2 \longrightarrow RC$	
		$MSID_j \leftarrow NPKE.Dec\left(CSID_j\right)$
		$v_j \leftarrow NPKE.Dec\left(CV_j\right)$
		$SIK_j \leftarrow h(MSID_j \| v_j^* \| sk)$
		if $h_2 \neq h\left(MSID_j \| v_j \| h_1 \| SIK_j\right)$
		return $\perp$
		else $MUID_i \leftarrow NPKE.Dec\left(CUID_i\right)$
		$v_i \leftarrow NPKE.Dec\left(CV_i\right)$
		$UIK_i \leftarrow h(MUID_i \| v_i^* \| sk)$
		if $h_1 \neq h(MUID_i \| MSID_j \| v_i \| UIK_i)$
		return $\perp$
		else $v_s \xleftarrow{\$} \{0,1\}^{256}$
		$H \leftarrow h(UIK_i \| SIK_j \| v_s \| sk)$
		$MH_j \leftarrow H \oplus h(SIK_j \oplus v_j)$
		$MH_i \leftarrow H \oplus h(UIK_i \oplus v_i)$
		$h_3 \leftarrow h\left(H \| v_j \| SIK_j\right)$
		$h_4 \leftarrow h\left(H \| v_i \| UIK_i\right)$
		$I_3 = \left\{MH_i, MH_j, h_3, h_4\right\}$
		$AS_j \longleftarrow I_3$
	$H \leftarrow MH_j \oplus h(SIK_j^{'} \oplus v_j)$	
	if $h_3 \neq h\left(H \| v_j \| SIK_j^{'}\right)$	
	return $\perp$	
	else $coin \xleftarrow{\$} \{0,1\}^{256}$	
	$K \| coin^{'} \leftarrow h\left(coin\right) \in \{0,1\}^{512}$	
	$c_{ij} \leftarrow NPKE.Enc\left(pk_i, K; coin^{'}\right)$	
	$h_5 \leftarrow h\left(H \| c_{ij} \| h_4\right)$	
	$I_4 = \left\{MH_i, c_{ij}, h_4, h_5\right\}$	
	$U_i \longleftarrow I_4$	
	$ss \leftarrow h\left(H \| K\right)$	
$H \leftarrow MH_i \oplus h(UIK_i^{'} \oplus v_i)$		
if $h_4 \neq h\left(H \| v_i \| UIK_i^{'}\right)$		
or $h_5 \neq h\left(H \| c_{ij} \| h_4\right)$		
return $\perp$		
else $K \leftarrow NPKE.Dec\left(sk_i, c_{ij}\right)$		
$ss \leftarrow h\left(H \| K\right)$		

FIGURE 5. Authentication and session key agreement of our scheme.



User $\left(U_i, UID_i, PW_i^{'}, PW_i^{new}, Bio_i^{'}\right)$	Registration Server(RS, pk, sk)
$MUID_i \leftarrow h\left(UID_i\right)$	
$\beta_i^{'} \leftarrow Rep\left(\alpha_i, Bio_i^{'}\right)$	
$MPB_i^{'} \leftarrow h(PW_i^{'} \Vert \beta_i^{'})$	
$UIK_i^{'} \leftarrow \delta_i \oplus MPB_i^{'}$	
if $\gamma_i = h(MUID_i \Vert MPB_i^{'} \Vert UIK_i{'})$	
$MPB_i^{new} \leftarrow h(PW_i^{new} \Vert \beta_i^{'})$	
$\delta_i^{new} \leftarrow UIK_i^{'} \oplus MPB_i^{new}$	
$\gamma_i^{new} = h(MUID_i \Vert MPB_i^{new} \Vert UIK_i{'})$	
update $SC_i = \left\{\alpha_i, \delta_i^{new}, \gamma_i^{new}\right\}$	
The password update is complete. To update the user credentials, continue with the steps below.	
$v_i^{'} \xleftarrow{\$} \{0,1\}^{256}$	
$CV_i^{'} \leftarrow NPKE.Enc\left(v_i^{'}\right)$	
$CUID_i \leftarrow NPKE.Enc\left(MUID_i\right)$	
$CPB_i \leftarrow NPKE.Enc\left(MPB_i^{new}\right)$	
$h_1^{upd} \leftarrow h(MUID_i \Vert MPB_i^{new} \Vert v_i^{'} \Vert UIK_i^{'})$	
$\left\{CUID_i, CPB_i, CV_i^{'}, h_1^{upd}\right\} \longrightarrow RC$	
	$v_i^{'} \leftarrow NPKE.Dec\left(CV_i^{'}\right)$
	$MUID_i \leftarrow NPKE.Dec\left(CUID_i\right)$
	$MPB_i^{new} \leftarrow NPKE.Dec\left(CPB_i\right)$
	$UIK_i \leftarrow h(MUID_i \Vert v_i^{*} \Vert sk)$
	if $h_1^{upd} \neq h(MUID_i \Vert MPB_i^{new} \Vert v_i^{'} \Vert UIK_i)$
	return $\perp$
	else $v_i^{*new} \xleftarrow{\$} \{0,1\}^{256}$
	$UIK_i^{new} \leftarrow h(MUID_i \Vert v_i^{*new} \Vert sk)$
	$\delta_i^{new} \leftarrow UIK_i^{new} \oplus MPB_i^{new}$
	$\gamma_i^{new} \leftarrow h(MUID_i \Vert MPB_i^{new} \Vert UIK_i^{new})$
	$\delta_i^{upd} \leftarrow \delta_i^{new} \oplus h(v_i^{'} \Vert UIK_i)$
	$\gamma_i^{upd} \leftarrow \gamma_i^{new} \oplus h(v_i^{'} \Vert UIK_i)$
	$h_2^{upd} \leftarrow h(MUID_i \Vert \delta_i^{upd} \Vert \gamma_i^{upd} \Vert UIK_i)$
	$U_i \longleftarrow \left\{\delta_i^{upd}, \gamma_i^{upd}, h_2^{upd}\right\}$
if $h_2^{upd} \neq h(MUID_i \Vert \delta_i^{upd} \Vert \gamma_i^{upd} \Vert UIK_i^{'})$	
return $\perp$	
else $\delta_i^{new} \leftarrow \delta_i^{upd} \oplus h(v_i^{'} \Vert UIK_i^{'})$	
$\gamma_i^{new} \leftarrow \gamma_i^{upd} \oplus h(v_i^{'} \Vert UIK_i^{'})$	
$UIK_i^{''} \leftarrow \delta_i^{new} \oplus MPB_i^{new}$	
$h_3^{upd} \leftarrow h(h_2^{upd} \Vert UIK_i^{''})$	
$\left\{h_3^{upd}\right\} \longrightarrow RS$	if $h_3^{upd} \neq h(h_2^{upd} \Vert UIK_i^{new})$
update $SC_i = \left\{\alpha_i, \delta_i^{new}, \gamma_i^{new}\right\}$	return $\perp$
	else update $T_U = \left[MUID_i, v_i^{*new}\right]$

FIGURE 6. Password and biometric updating of our scheme.

of $\mathcal{A}$ winning the game is

$$
\begin{aligned}
Adv_{\mathcal{P}}^{AKE}(\mathcal{A}) \leq\ & q_h^2/2^{l+1} \\
& + max\left(q_h^2/2^{l+1}, q_s/2^n, q_s/2^{\theta}\right) + negl(\lambda). \qquad (3)
\end{aligned}
$$

where l, n and θ denote the bit length of hash function, user's biometric and password.

Proof:

Let $Succ_i$ be the event that $\mathcal{A}$ wins game G_i. These games begin from the real attack scenario. We gradually change the simulation rules of each game. In the final game, $\mathcal{A}$ will have no other advantage.

Game G_0: G_0 is the real attack scenario, according to the *definition 2*, we have

$$Adv_{\mathcal{P}}^{AKE}(\mathcal{A}) = |2 \cdot Pr[Succ_0] - 1|. \qquad (4)$$

Game G_1: G_1 models a passive attack by querying the *Execute* $\left(U_i^x, AS_j^y\right)$ oracle. But $\mathcal{A}$ can hardly increase the advantage of winning the game. Since the session key ss is computed by K and H, it is difficult for $\mathcal{A}$ to extract these values from $\{I_1, I_2, I_3, I_4\}$. According to section 6, $K = NPKE.Dec\left(sk_i, c_{ij}\right)$ and the temporary secrets s, e, s', e', e'' used to compute K are sampled for each connection, $H = h(UIK_i \Vert SIK_j \Vert v_s \Vert sk)$, and the temporary secrets v_i, v_j, v_s used to compute H are sampled for each connection. Therefore $\mathcal{A}$ cannot get more advantages than the *Test* $\left(U_i^x, AS_j^y\right)$ oracle. Thus we have

$$Pr[Succ_1] = Pr[Succ_0]. \qquad (5)$$

Game G_2: We transfer G_1 to this game by adding the *SendU2RC* (RC^z, m) oracle to model an active attack. $\mathcal{A}$ sends a fake tuple I_2' by modifying the response of the *Send* $(P^x, Start)$ oracle gradually:

Case1: $\mathcal{A}$ replaces the h_1 and h_2 in I_2 with the result of the *Hash-query*. According to the birthday attack, we have

$$\left|Pr\left[Succ_2^{Case1}\right] - Pr[Succ_1]\right| \leq q_h^2/2^{l+1}. \qquad (6)$$

Case2: $\mathcal{A}$ continues to modify I_2, replacing the $CUID_i$, CV_i, $CSID_j$ and CV_j with elements randomly selected over R_q. According to the IND-CPA security of *NewHope-CPA-PKE*, we have

$$\left|Pr\left[Succ_2^{Case2}\right] - Pr\left[Succ_2^{Case1}\right]\right| \leq negl(\lambda). \qquad (7)$$

Combining the *Case1*-*Case2* of G_2 and comparing to G_1, we have

$$|Pr[Succ_2] - Pr[Succ_1]| \leq q_h^2/2^{l+1} + negl(\lambda). \qquad (8)$$

Game G_3: We transfer G_2 to this game by adding the *SendRC2AS* $\left(AS_j^y, m\right)$ oracle to model an active attack. $\mathcal{A}$ sends a fake tuple I_3' by modifying the response of the *SendU2RC* (RC^z, m) oracle. $\mathcal{A}$ replaces the MH_i, MH_j, h_3 and h_4 in I_3 with the result of the *Hash-query*, we have

$$Pr[Succ_3] = Pr[Succ_2]. \qquad (9)$$

Game G_4: We transfer G_3 to this game by adding the *SendAS2U* $\left(U_i^x, m\right)$ oracle to model an active attack. $\mathcal{A}$ sends a fake tuple I_4' by modifying the response of the *SendRC2AS* $\left(AS_j^y, m\right)$ oracle gradually:

Case1: $\mathcal{A}$ replaces the h_4 and h_5 in I_4 with the result of the *Hash-query*, we have

$$Pr\left[Succ_4^{Case1}\right] = Pr[Succ_3]. \qquad (10)$$

Case2: $\mathcal{A}$ continues to modify I_4, replacing the c_{ij} with elements randomly selected over R_q. According to the IND-CPA security of *NewHope-CPA-PKE*, we have

$$\left|Pr\left[Succ_4^{Case2}\right] - Pr\left[Succ_4^{Case1}\right]\right| \leq negl(\lambda). \qquad (11)$$

Combining the *Case1*-*Case2* of G_4 and comparing to G_3, we have

$$|Pr[Succ_4] - Pr[Succ_3]| \leq negl(\lambda). \qquad (12)$$

Game G_5: We transfer G_4 to this game by adding the *Corrupt* $\left(U_i^x, PW_i\right)$ or *Corrupt* $\left(U_i^x, Bio_i\right)$ oracle to enhance attack ability of $\mathcal{A}$. We assume that $\mathcal{A}$ has acquired the secrets in the smart card SC_i, then there are three strategies to attack three-factor security, and he/she chooses the one with the highest probability.

Case1: $\mathcal{A}$ fakes the β_i' with the result of the *Hash-query* when the PW_i has been compromised. According to the birthday attack, we have

$$|Pr\left[Succ_5^{Case1}\right] - Pr\left[Succ_4\right]| \leq q_h^2/2^{l+1}. \tag{13}$$

Case2: $\mathcal{A}$ also fakes the β_i' by guessing result Bio_i^* when the PW_i has been compromised, we have

$$|Pr\left[Succ_5^{Case2}\right] - Pr\left[Succ_4\right]| \leq q_s/2^n. \tag{14}$$

Case3: $\mathcal{A}$ fakes the MPB_i' by guessing result PW_i^* when the Bio_i has been compromised, we have

$$|Pr\left[Succ_5^{Case3}\right] - Pr\left[Succ_4\right]| \leq q_s/2^\theta. \tag{15}$$

Combining the *Case1-Case3* of G_5 and comparing to G_4, we have

$$|Pr\left[Succ_5\right] - Pr\left[Succ_4\right]| \leq max\left(q_h^2/2^{l+1}, q_s/2^n, q_s/2^\theta\right). \tag{16}$$

Game G_6: This game is the final game, which is translated from G_5. To compute the session key $ss = h\left(H\|K\right)$, in addition to H, $\mathcal{A}$ must know K. According to the IND-CPA security of *NewHope-CPA-PKE*, the advantage of $\mathcal{A}$ winning the game is negl (λ). Thus we have

$$|Pr\left[Succ_6\right] - Pr\left[Succ_5\right]| \leq negl\left(\lambda\right). \tag{17}$$

Otherwise, G_6 is just as the real case and $Pr\left[Succ_6\right] = 1/2$. Combining the Game G_1 to Game G_6, we have

$$\begin{aligned} Adv_{\mathcal{P}}^{AKE}\left(\mathcal{A}\right) \leq{}& q_h^2/2^{l+1} \\ &+max\left(q_h^2/2^{l+1}, q_s/2^n, q_s/2^\theta\right) + negl\left(\lambda\right). \end{aligned} \tag{18}$$

Theorem 2 is proven.

B. OTHER DISCUSSIONS

In this section, we demonstrate how our scheme achieves mutual authentication, three-factor security, session key security, forward security, user privacy security and resists other known attacks.

1) MUTUAL AUTHENTICATION

During the authentication and session key agreement phase of *RRBAS*, *RC* authenticates AS_j with h_2 which contains the registration credentials $\left\{MSID_j, SIK_j\right\}$ of AS_j, authenticates U_i with h_1 which contains the registration credentials $\{MUID_i, UIK_i\}$ of U_i. AS_j authenticates *RC* with h_3 which confirms that the private key *sk* owner of system public key *pk* holds the registration credentials $\left\{MSID_j, SIK_j\right\}$ of it, indirectly authenticates U_i by means of the *RC* authentication. U_i authenticates *RC* with h_4 which confirms that the private key *sk* owner of system public key *pk* holds the registration credentials $\{MUID_i, UIK_i\}$ of it, indirectly authenticates AS_j by means of the *RC* authentication.

2) THREE-FACTOR SECURITY

As shown in the Game G_5 of the security proof, the advantage of $\mathcal{A}$ destroys AKE security is $max\left(q_h^2/2^{l+1}, q_s/2^n, q_s/2^\theta\right)$ by attacking three-factor authentication security. Therefore, *RRBAS* has three-factor security.

3) SESSION KEY SECURITY

During the authentication and session key agreement phase of *RRBAS*, U_i and AS_j independently calculate the session key $ss = h\left(H\|K\right)$. According to the hash function one-way security and the IND-CPA security of the *NewHope-IND-PKE*, the advantage of $\mathcal{A}$ obtaining H and K is negligible. Therefore, *RRBAS* has session key security.

4) FORWARD SECURITY

During the authentication and session key agreement phase of *RRBAS*, the session key $ss = h\left(H\|K\right)$ is calculated independently by U_i and AS_j. $K = NPKE.Dec\left(sk_i, c_{ij}\right)$ and the temporary secrets s, e, s', e', e'' used to compute it are sampled for each connection, $H = h(UIK_i\|SIK_j\|v_s\|sk)$ and the temporary secrets v_i, v_j, v_s used to compute it are sampled for each connection. Therefore, even if $\mathcal{A}$ obtains the long-term secret of all the protocol entities, it cannot improve his advantage of destroying the security of the established session key.

5) PRIVACY SECURITY

Biometric-based AKE privacy security includes anonymity [2] and biometric security [8].

During the authentication and session key agreement phase of *RRBAS*, UID_i and SID_j are hidden in *NewHope-IND-PKE* ciphertexts $CUID_i$ and $CSID_j$. According to the IND-CPA security, the advantage of $\mathcal{A}$ obtaining the UID_i and SID_j is negligible, distinguishing different session key negotiation information from the same user is also negligible. Therefore, the UID_i is neither leaked nor tracked, so *RRBAS* has user anonymity.

Biometric security includes the fresh biometric samples security and the biometric templates security. In the authentication and session key agreement phase of *RRBAS*, fresh biometric samples and biometric templates are protected by fuzzy extractor and secure hash. According to the security assumption of fuzzy extractor [23], the advantage of $\mathcal{A}$ obtaining Bio_i and Bio_i' is negligible. Therefore, regardless of the social engineering attacks, the advantage of $\mathcal{A}$ against the fresh biometric samples attack is equivalent to brute force attacks. The system architecture of *RRBAS* does not meet the conditions of the centre search attack [9]. Therefore, *RRBAS* has biometric security.

6) RESISTANCE TO KNOWN SESSION-SPECIFIC TEMPORARY INFORMATION ATTACK

During the authentication and session key agreement phase of *RRBAS*, the session key $ss = h\left(H\|K\right)$ is calculated independently by U_i and AS_j. Since $H = h(UIk_i\|SIK_j\|v_s\|sk)$, and

$UIK_i = h(MUID_i \| v_i^* \| sk)$ and $SIK_j = h(MSID_j \| v_j^* \| sk)$, even if $\mathcal{A}$ knows the temporary information K of a specific session, he/she cannot calculate H without knowing UID_i, SID_j, sk, v_i^*, v_j^* and random number v_s, and thus cannot destroy the security of the session key.

7) RESISTANCE TO PRIVILEGED INSIDER ATTACK

In the registration and authentication phase of the *RRBAS*, PW_i and Bio_i of U_i are protected by fuzzy extractor and secure hash, and encapsulated in the form of $MPB_i = h(PW_i \| \beta_i)$. Moreover, only the hash value of UID_i and the random number are stored in the user registry T_U. Therefore, even if $\mathcal{A}$ completely corrupts the RC, the security of the password and biometrics cannot be threatened.

8) RESISTANCE TO USER IMPERSONATION ATTACK

As shown in the security proof in section 6, *RRBAS* has three-factor security, so that it can resist the user impersonation attack.

9) RESISTANCE TO INTERMEDIATE DATA ATTACKS

In the network of *RRBAS*, the communication link between AS_j and RC is relatively secure. The intermediate data attack mainly occurs on the open link between AS_j and U_i. *RRBAS* has good anonymity, $\mathcal{A}$ can't get UID_i and SID_j, and can't track the session, so the replay attack against *RRBAS* is difficult to work. In addition, only hash values and *NewHope-IND-PKE* ciphertexts are forwarded between protocol entities, and the secrets that generats these values are freshly selected for each session, so the man-in-the-middle attack against *RRBAS* is also difficult to work.

10) RESISTANCE TO PASSWORD GUESSING ATTACK

According to the three-factor security of *RRBAS*, if the secrets of smart card SC_i has been learned by the adversary $\mathcal{A}$, and Bio_i is compromised, the advantage of $\mathcal{A}$ destroying the AKE security by the offline password guessing attack is $q_s/2^{\theta}$, otherwise, its maximum probability is $q_s/2^{\theta+l}$. And because *RRBAS* is an online authentication method, it can effectively resist online dictionary attacks with the intrusion prevention strategy of RC. Therefore, *RRBAS* can resist the password guessing attack.

11) RESISTANCE TO KNOWN QUANTUM ATTACKS

RRBAS is designed based on the NewHope-CPA-PKE. According to Lemma 1 and Theorem 1, the advantage of any known quantum algorithm adversary to destroy the AKE security of RRBAS is equivalent to the advantage of against the DRLWE problem, which is negligible.

VIII. EVALUATION

This section demonstrates that *RRBAS* how to satisfy the security goals and application requirements from the security properties, computational complexity and communication overhead.

TABLE 2. Comparison of security properties.

Security Properties	P-1	P-2	P-3	P-4	P-5	P-6	P-7	P-8	P-9	P-10	P-11	P-12
RRBAS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Odelu et al. [10]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Feng et al. [11]	Yes	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes	Yes	No
Lwamo et al. [1]	Yes	Yes	Yes	No	No	No	No	Yes	No	Yes	Yes	No
Xu et al. [16]	Yes	No	Yes	Yes	No	–	No	No	No	Yes	Yes	No
Ying-Nayak [17]	Yes	No	Yes	Yes	No	–	No	Yes	No	Yes	Yes	No
Li et al. [18]	No	Yes	No	No	No	Yes	Yes	Yes	No	No	No	No
Qi et al. [19]	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No
Challa et al. [20]	No	Yes	No	No	No	Yes	Yes	No	No	Yes	No	No

P-1: Mutual authentication, P-2: Multi-factor security, P-3: Session key security, P-4: Forward security, P-5: Anonymity, P-6: Biometric security, P-7: Resistance to offline password guessing attack, P-8: Resistance to privileged insider attack, P-9: Resistance to user impersonation attack, P-10: Resistance to replay attack, P-11: Resistance to man-in-the-middle attack, P-12: Resistance to quantum attacks.

TABLE 3. Runtime of related operation ($n = 1024, p = 2, q = 12289, l = 256$) .

Operation	T_h	T_{Gen}	T_{Enc}	T_{Dec}	T_S	T_{PE}/T_{PD}	T_m
Time(ms)	0.0010	0.1356	0.1929	0.0494	0.0022	1.9150	1.1006

T_h: Runtime of a SHAKE256; T_{Gen}: Runtime of the NPKE.Gen $(\cdot)$; T_{Enc}: Runtime of the NPKE.Enc $(\cdot)$; T_{Dec}: Runtime of the NPKE.Enc $(\cdot)$; T_S: Runtime of the *AES256*; T_{PE}:Runtime of the *RSA1024* encryption operation; T_{PD}:Runtime of the *RSA1024* decryption operation; T_m: Runtime of the elliptic curve scalar point multiplication.

A. COMPARISON OF SECURITY PROPERTIES

We evaluated the security properties of our improved scheme and compared it with eight recently proposed schemes in the literature, e.g., Odelu *et al.* [10], Feng *et al.* [11], Lwamo *et al.* [1], Xu *et al.* [16], Ying and Nayak [17], Li *et al.* [18], Qi *et al.* [19], and Challa *et al.* [20]. The details are shown in Table 2.

The results show that Feng et al. [11], Lwamo et al. [1], Xu et al. [16], Ying-Nayak [17], Li et al. [18], Qi et al. [19] and Challa et al. [20] are vulnerable to hardware loss attack. In turn, offline password guessing attacks and biometric security attacks are caused, which leads to user impersonation attack and even loss of anonymity and forward security.

B. COMPARISON OF COMPUTATIONAL COMPLEXITY

To evaluate the computational complexity of *RRBAS*, we implemented all the basic operations of the scheme on the personal computer (Intel(R) Core(TM) i3-M380@2.53GHz processor, 6 GB RAM and with Ubuntu 16.04 operating system). We used gcc 5.4.0 to compile and run the *RRBAS* related operations based on the *Newhope* library [21], and other discussed scheme related operations based on PBC library [22], as shown in Table 3.

We assume that the computational complexity of the fuzzy extractor, Biohash and elliptic curve scalar point multiplication are close. As shown in Table 4, we use the results shown in Table 3 to estimate the computational cost of the protocol entities in the *RRBAS* authentication and key exchange phase. Regardless of the overhead of *XOR* operation, and the runtime of *RRBAS* is the lowest of the five online

TABLE 4. Performance evaluation for *RRBAS* and other discussed schemes.

Scheme	Problem	Computational complexity (ms)		
		U_i	$AS_j + RC$	*Total*
RRBAS	RLWE	$8T_h + 2T_{Enc} + T_{Gen} + T_{Dec}$ $\underline{0.5798}$	$13T_h + 4T_{Dec} + 3T_{Enc}$ $\underline{0.7923}$	$\underline{1.3721}$
Odelu et al. [10]	ECDLP	$7T_h + 3T_m$ $\underline{3.3088}$	$16T_h + 5T_m$ $\underline{5.5190}$	$\underline{8.8278}$
Feng et al. [11]	ECDLP	$7T_h + 3T_m$ $\underline{3.3088}$	$17T_h + 5T_m$ $\underline{5.5200}$	$\underline{8.8288}$
Lwamo et al. [1]	RSA	$8T_h + T_{PE} + T_s$ $\underline{1.9252}$	$11T_h + T_{PD} + 2T_s$ $\underline{1.9304}$	$\underline{3.8556}$
Xu et al. [16]	ECDLP	$9T_h + 3T_m$ $\underline{3.3108}$	$6T_h + 3T_m$ $\underline{3.3078}$	$\underline{6.6186}$
Ying-Nayak [17]	ECDLP	$9T_h + 3T_m + Ts$ $\underline{3.3110}$	$6T_h + 2T_m + 2Ts$ $\underline{2.2116}$	$\underline{5.5226}$
Li et al. [18]	ECDLP	$8T_h + 2T_m$ $\underline{2.2092}$	$13T_h + T_m$ $\underline{1.1136}$	$\underline{3.3228}$
Qi et al. [19]	ECDLP	$5T_h + 3T_m$ $\underline{3.3068}$	$12T_h + 5T_m + 2Ts$ $\underline{5.5184}$	$\underline{8.8252}$
Challa et al. [20]	ECDLP	$10T_h + 2T_m$ $\underline{2.2112}$	$5T_h + T_m$ $\underline{1.1096}$	$\underline{3.3208}$

TABLE 5. Binary length of each data structure.

Metadata	L_{seed}	L_h	L_{R_q}
Length$(Byte)$	32	32	1792

L_{seed}: Length of the seed; L_h: Length of a SHAKE256; L_{R_q}: Length of a ring element over L_{R_q}.

TABLE 6. Communication overhead of *RRBAS* authentication and key exchange phases.

Data	I_1	I_2	I_3	I_4	Total
Overhead $(Byte)$	$3L_{R_q} + 2L_h$ $\underline{5440}$	$4L_{R_q} + 2L_h$ $\underline{7232}$	$4L_h$ $\underline{128}$	$L_{R_q} + 3L_h$ $\underline{1888}$	$\underline{14688}$

authentication schemes [10], [11], [18]–[20] even lower than the three offline schemes [1], [16], [17].

C. COMPARISON OF COMMUNICATION OVERHEAD

To estimate the communication overhead of the proposed scheme authentication and key exchange phase, we calculated the bit length of all data structures transmitted in *RRBAS*, as shown in Table 5. Due to the special algebraic structure, the ciphertext size of the lattice-based scheme is generally larger than that of the traditional scheme, so no comparison is made here.

We use the results shown in Table 5 to analyze the communication overhead of *RRBAS*'s authentication and key exchange phase, the details are shown in Table 6. Regardless of the overhead of the underlying communication protocol, the overhead of the user side of the *RRBAS* is 7328 bytes, which can meet the practical requirements.

IX. CONCLUSION

In this work, we reviewed the recently proposed *Lwamo2019* scheme and showed that the scheme is vulnerable to the smart card lost attack; therefore, the scheme fails to prevent the offline guessing attack and user impersonation attack, and cannot provide forward security and user anonymity. In addition, *Lwamo2019* also cannot resist known quantum attacks. To withstand these drawbacks, we have proposed a secure and efficient remote single and multi-server biometric authentication scheme using *RLWE*, which is the first lattice-based remote biometric authentication scheme for the multi-server environments. We proved the *AKE* security of the proposed scheme in the *ROM* and demonstrated that it can resist known security attacks through an informal security analysis. Moreover, we implemented the proposed scheme using C language based on the NewHope library. The results show that the computational cost of our scheme is less than *Lwamo2019* and other discussed schemes, and the communication overhead is slightly higher than other schemes because the ciphertext of the lattice-based cryptosystem is inherently a big chunk, and the total communication overhead is only 14 KB, which meets the scenario requirements of no pre-shared information between users and servers but requires authentication key agreement.

ACKNOWLEDGMENT

The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

REFERENCES

[1] N. M. R. Lwamo, L. Zhu, K. Sharif, X. Liu, C. Zhang, and C. Xu, "SUAA: A secure user authentication scheme with anonymity for the single & multi-server environments," *Inf. Sci.*, vol. 477, pp. 369–385, Mar. 2019. doi: 10.1016/j.ins.2018.10.037.

[2] D. Wang and P. Wang, "On the anonymity of two-factor authentication schemes for wireless sensor networks: Attacks, principle and solutions," *Comput. Netw.*, vol. 73, pp. 41–57, Jul. 2014. doi: 10.1016/j.comnet.2014.07.010.

[3] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1086–1090, Mar. 2009. doi: 10.1109/TWC.2008.080128.

[4] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science), vol. 6110. Berlin, Germany: Springer, 2010, pp. 1–23. doi: 10.1007/978-3-642-13190-5_1.

[5] V. Lyubashevsky, C. Peikert, and O. Regev, "A toolkit for ring-LWE cryptography," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science), vol. 7881. Berlin, Germany: Springer, 2013, pp. 35–54. doi: 10.1007/978-3-642-38348-9_3.

[6] E. Alkim, L. Ducas, and T. Pöppelmann, "Post-quantum key exchange—A new hope," IACR Cryptol. ePrint Arch., NV, USA, Tech. Rep. 2015/1092, 2015, p. 1092.

[7] E. Alkim, R. Avanzi, and J. Bos. (2018). *Algorithm Specifications and Supporting Documentation of NewHope, NewHope Post-Quantum Key Encapsulation*. Accessed: Dec. 10, 2018. [Online]. Available: https://newhopecrypto.org/data/NewHope.pdf.

[8] E. Pagnin and A. Mitrokotsa, "Privacy-preserving biometric authentication: Challenges and directions," *Secur. Commun. Netw.*, vol. 2017, Oct. 2017, Art. no. 7129505. doi: 10.1155/2017/7129505.

[9] K. Simoens, J. Bringer, H. Chabanne, and S. Seys, "A framework for analyzing template security and privacy in biometric authentication systems," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 833–841, Apr. 2012. doi: 10.1109/tifs.2012.2184092.

[10] V. Odelu, A. K. Das, and A. Goswami, "A secure biometrics-based multi-server authentication protocol using smart cards," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 9, pp. 1953–1966, Sep. 2015. doi: 10.1109/TIFS.2015.2439964.

[11] Q. Feng, D. He, S. Zeadally, and H. Wang, "Anonymous biometrics-based authentication scheme with key distribution for mobile multi-server environment," *Future Gener. Comput. Syst.*, vol. 84, pp. 239–251, Jul. 2018. doi: 10.1016/j.future.2017.07.040.

[12] C.-C. Chang and N.-T. Nguyen, "An untraceable biometric-based multi-server authenticated key agreement protocol with revocation," *Wireless Pers Commun*, vol. 90, no. 4, pp. 1695–1715, 2016. doi: 10.1007/s11277-016-3418-2.

[13] A. G. Reddy, E.-J. Yoon, A. K. Das, V. Odelu, and K.-Y. Yoo, "Design of mutually authenticated key agreement protocol resistant to impersonation attacks for multi-server environment," *IEEE Access*, vol. 5, pp. 3622–3639, 2017. doi: 10.1109/ACCESS.2017.2666258.

[14] S. Barman, A. K. Das, D. Samanta, S. Chattopadhyay, J. J. P. C. Rodrigues, and Y. Park, "Provably secure multi-server authentication protocol using fuzzy commitment," *IEEE Access*, vol. 6, pp. 38578–38594, 2018. doi: 10.1109/ACCESS.2018.2854798.

[15] S. Barman, H. P. H. Shum, S. Chattopadhyay, and D. Samanta, "A secure authentication protocol for multi-server-based e-healthcare using a fuzzy commitment scheme," *IEEE Access*, vol. 7, pp. 12557–12574, 2019. doi: 10.1109/ACCESS.2019.2893185.

[16] G. Xu, S. Qiu, H. Ahmad, G. Xu, Y. Guo, M. Zhang, and H. Xu, "A multi-server two-factor authentication scheme with un-traceability using elliptic curve cryptography," *Sensors*, vol. 18, no. 7, p. 2394, 2018. doi: 10.3390/s18072394.

[17] B. Ying and A. Nayak, "Lightweight remote user authentication protocol for multi-server 5G networks using self-certified public key cryptography," *J. Netw. Comput. Appl.*, vol. 131, pp. 66–74, Apr. 2019. doi: 10.1016/j.jnca.2019.01.017.

[18] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K.-K. R. Choo, "A three-factor anonymous authentication scheme for wireless sensor networks in Internet of Things environments," *J. Netw. Comput. Appl.*, vol. 103, pp. 194–204, Feb. 2018. doi: 10.1016/j.jnca.2017.07.001.

[19] M. Qi, J. Chen, and Y. Chen, "A secure biometrics-based authentication key exchange protocol for multi-server TMIS using ECC," *Comput. Methods Programs Biomed.*, vol. 164, pp. 101–109, Oct. 2018. doi: 10.1016/j.cmpb.2018.07.008.

[20] S. Challa, A. K. Das, V. Odelu, N. Kumar, S. Kumari, M. K. Khan, and A. V. Vasilakos, "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," *Comput. Elect. Eng.*, vol. 69, pp. 534–554, Jul. 2018. doi: 10.1016/j.compeleceng.2017.08.003.

[21] E. Alkim, R. Avanzi, J. Bos, L. Ducas, A. de la Piedra, T. Pöppelmann, P. Schwabe, and D. Stebila. Software of the NIST Post-Quantum Submission NewHope. GitHub, Inc. 2018. [Online]. Available: https://github.com/newhopecrypto/newhope

[22] (2013). *The Pairing-Based Cryptography Library, Stanford.* [Online]. Available: https://crypto.stanford.edu/pbc/download.html

[23] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM J. Comput.*, vol. 38, no. 1, pp. 97–139, 2008. doi: 10.1137/060651380.

[24] N. Veyrat-Charvillon and F.-X. Standaert, "Generic side-channel distinguishers: Improvements and limitations," in *Proc. Annu. Cryptol. Conf.* Berlin, Germany: Springer-Verlag, 2011, pp. 354–372.

[25] L. Lamport, "Password authentication with insecure communication," *Commun. ACM*, vol. 24, no. 11, pp. 770–772, Nov. 1981. doi: 10.1145/358790.358797.

[26] E.-J. Yoon and K.-Y. Yoo, "Improving the dynamic ID-based remote mutual authentication scheme," in *Proc. Conf. OTM Workshops*, 2006, pp. 499–507. doi: 10.1007/11915034_73.

[27] S. M. Bellovin and M. Merritt, "Augmented encrypted key exchange: A password-based protocol secure against dictionary attacks and password file compromise," in *Proc. Conf. CCS*, 1993, pp. 244–250. doi: 10.1145/168588.168618.

[28] T. Y. Chang, M. S. Hwang, and W. P. Yang, "A communication-efficient three-party password authenticated key exchange protocol," *Inf. Sci.*, vol. 181, no. 1, pp. 217–226, Jan. 2011. doi: 10.1016/j.ins.2010.08.032.

[29] X. Fu, X. Nie, F. Li, and T. Wu, "Large universe attribute based access control with efficient decryption in cloud storage system," *J. Syst. Softw.*, vol. 135, pp. 157–164, Jan. 2018. doi: 10.1016/j.jss.2017.10.020.

[30] Y. Miao, J. Ma, X. Liu, X. Li, Q. Jiang, and J. Zhang, "Attribute-based keyword search over hierarchical data in cloud computing," *IEEE Trans. Services Comput.*, to be published. doi: 10.1109/TSC.2017.2757467.

[31] Y. Miao, J. Ma, X. Liu, J. Weng, H. Li, and H. Li, "Lightweight fine-grained search over encrypted data in fog computing," *IEEE Tran. Services Comput.*, to be published. doi: 10.1109/TSC.2018.2823309.

[32] Y. Miao, X. Liu, K.-K. R. Choo, R. H. Deng, J. Li, H. Li, and J. Ma, "Privacy-preserving attribute-based keyword search in shared multi-owner setting," *IEEE Trans. Dependable Secure Comput.*, to be published. doi: 10.1109/TDSC.2019.2897675.

[33] X. Zhang, H. Wang, and C. Xu, "Identity-based key-exposure resilient cloud storage public auditing scheme from lattices," *Inf. Sci.*, vol. 472, pp. 223–234, Jan. 2019. doi: 10.1016/j.ins.2018.09.013.

[34] X. Zhang, Y. Tang, H. Wang, C. Xu, Y. Miao, and H. Cheng, "Lattice-based proxy-oriented identity-based encryption with keyword search for cloud storage," *Inf. Sci.*, vol. 494, pp. 193–207, Aug. 2019. doi: 10.1016/j.ins.2019.04.051.

[35] X. Zhang, C. Xu, H. Wang, Y. Zhang, and S. Wang, "FS-PEKS: Lattice-based forward secure public-key encryption with keyword search for cloud-assisted industrial Internet of Things," *IEEE Trans. Dependable Secure Comput.*, to be published. doi: 10.1109/TDSC.2019.2914117.

[36] G. C. Kessler, (1996). *Passwords Strengths and Weaknesses*. Accessed: Dec. 20, 2018. [Online]. Available: https://www.garykessler.net/library/password.html

[37] W.-J. Tsaur, "A flexible user authentication scheme for multi-server Internet services," in *Proc. Netw.-ICN*, 2001, pp. 174–183. doi: 10.1007/3-540-47728-4_18.

[38] D. He, Y. Chen, and J. Chen, "Cryptanalysis and improvement of an extended chaotic maps-based key agreement protocol," *Nonlinear Dyn.*, vol. 69, pp. 1149–1157, Aug. 2012. doi: 10.1007/s11071-012-0335-0.

[39] H.-Y. Lin, "Traceable anonymous authentication and key exchange protocol for privacy-aware cloud environments," *IEEE Syst. J.*, vol. 13, no. 2, pp. 1608–1617, Jun. 2019. doi: 10.1109/JSYST.2018.2828022.

[40] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, May 2002. doi: 10.1109/TC.2002.1004593.

[41] Q. Xie, D. S. Wong, G. Wang, X. Tan, K. Chen, and L. Fang, "Provably secure dynamic ID-based anonymous two-factor authenticated key exchange protocol with extended security model," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1382–1392, Jun. 2017. doi: 10.1109/TIFS.2017.2659640.

[42] L. Zhang, Y. Zhang, H. Luo, and S. Tang, "Privacy protection for e-health systems by means of dynamic authentication and three-factor key agreement," *IEEE Trans. Ind. Electron.*, vol. 65, no. 3, pp. 2795–2805, Mar. 2018. doi: 10.1109/TIE.2017.2739683.

[43] E.-J. Yoon and K.-Y. Yoo, "Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem," *J. Supercomput.*, vol. 63, no. 1, pp. 235–255, Jan. 2013. doi: 10.1007/s11227-010-0512-1.

[44] F. Rehman, S. Akram, and M. A. Shah, "The framework for efficient passphrase-based multifactor authentication in cloud computing," in *Proc. ICAC*, 2016, pp. 37–41. doi: 10.1109/IConAC.2016.7604891.

[45] *SMS is Deprecated*. Accessed: Dec. 20, 2018. [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63b.html-out-of-band

[46] M.-C. Chuang and M. C. Chen, "An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics," *Expert Syst. Appl.*, vol. 41, no. 4, pp. 1411–1418, Mar. 2014. doi: 10.1016/j.eswa.2013.08.040.

[47] R. Zhang, Y. Xiao, H. Ma, and S. Sun, "Efficient multi-factor authenticated key exchange scheme for mobile communications," *IEEE Trans. Dependable Secure Comput.*, vol. 16, no. 4, pp. 625–634, Jul./Aug. 2019. doi: 10.1109/TDSC.2017.2700305.

[48] C.-I. Fan and Y.-H. Lin, "Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics," *IEEE Trans. Dependable Secure Computing*, vol. 4, no. 4, pp. 933–945, Dec. 2009. doi: 10.1109/TIFS.2009.2031942.

[49] D. Yang and B. Yang, "A biometric password-based multi-server authentication scheme with smart card," in *Proc. ICCDA*, vol. 1, 2010, pp. V5-554–V5-559. doi: 10.1109/ICCDA.2010.5541128.

[50] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. 31, no. 4, pp. 469–472, Jul. 1985. doi: 10.1109/TIT.1985.1057074.

[51] D. He and D. Wang, "Robust biometrics-based authentication scheme for multiserver environment," *IEEE Syst. J.*, vol. 9, no. 3, pp. 816–823, Sep. 2015. doi: 10.1109/JSYST.2014.2301517.

[52] D. He, "Security flaws in a biometrics-based multi-server authentication with key agreement scheme," IACR Cryptol. ePrint Arch., NV, USA, Tech. Rep. 2011/365, 2011, p. 365.

[53] H. Lin, F. Wen, and C. Du, "An improved anonymous multi-server authenticated key agreement scheme using smart cards and biometrics," *Wireless Pers. Commun.*, vol. 84, no. 4, pp. 2351–2362, 2015. doi: 10.1007/s11277-015-2708-4.

[54] S. Kumari and H. Om, "Cryptanalysis and improvement of an anonymous multi-server authenticated key agreement scheme," *Wireless Pers. Commun.*, vol. 96, pp. 2513–2537, May 2017. doi: 10.1007/s11277-017-4310-4.

[55] J. Ding, "Cryptographic systems using pairing with errors," U.S. Patent 9 246 675 B2, Jan. 26, 2016.

[56] J. Ding, X. Xie, and X. Lin, "A simple provably secure key exchange scheme based on the learning with errors problem," IACR Cryptol. ePrint Arch., NV, USA, Tech. Rep. 2012/688, 2012, p. 688.

[57] C. Peikert, "Lattice cryptography for the Internet," in *Proc. PQCrypto*. Cham, Switzerland: Springer, vol. 8772, 2014, pp. 197–219. doi: 10.1007/978-3-319-11659-4_12.

[58] J. W. Bos, C. Costello, D. Stebila, and M. Naehrig, "Post-quantum key exchange for the TLS protocol from the ring learning with errors problem," in *Proc. IEEE SP*, San Jose, CA, USA, May 2015, pp. 553–570. doi: 10.1109/SP.2015.40.

[59] D, Xu, D. He, K.-K. R. Choo, and J. Chen, "Provably secure three-party password authenticated key exchange protocol based on ring learning with error," IACR Cryptol. ePrint Arch., NV, USA, Tech. Rep. 2017/360, 2017, p. 360.

[60] J. Bos, L. Ducas, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, E. Kiltz, and D. Stehle, "CRYSTALS-Kyber: A CCA-Secure Module-Lattice-Based KEM," in *Proc. EuroSP*, vol. 1, 2018, pp. 353–367. doi: 10.1109/EuroSP.2018.00032.

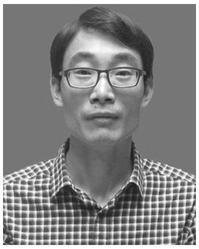
HAILONG YAO received the M.S. degree in communication and information system from the School of Electronic and Information Engineering, Lanzhou Jiaotong University, in 2013. He is currently pursuing the Ph.D. degree with Northwest Normal University. He is currently a Lecturer with Lanzhou City University. His research interests include cryptography and privacy security in distributed systems.

CAIFEN WANG received the Ph.D. degree in cryptography from the School of Communication Engineering, Xidian University, in 2003. She is currently a Professor with Shenzhen Technology University. She has been selected as the Director of the China Cryptography Society and a member of the Special Committee of Cryptography Algorithms. Her main research interests include cryptography and information security, in particular, applied cryptography and security in cloud computing.

XINGBING FU received the Ph.D. degree from the University of Electronic Science and Technology of China (UESTC), in 2016. He is currently a lecturer. His research interests include cloud computing and cryptography.

CHAO LIU received the B.E. degree in computer science and technology from Huaqiao University, China, in 2013, and the M.S. degree in computer science and engineering from Northwest Normal University, China, in 2018. He is currently pursuing the Ph.D. degree with the University of Maryland at Baltimore, Baltimore, USA. His research interests include cryptography, blockchain, distributed systems, and information security.

BIN WU received the B.E. degree in mathematics and applied mathematics and the M.S. degree in homology algebra from Northwest Normal University, China, in 2008 and 2018, respectively, where she is currently pursuing the Ph.D. degree. Her research interests include cryptography and information security.



FAGEN LI received the Ph.D. degree in cryptography from Xidian University, Xi'an, China, in 2007. His research interests include cryptography and network security, especially in signcryption schemes, signature schemes, and key agreement protocols.