SCIS 2018 2018 Symposium on
Cryptography and Information Security
Niigata, Japan, Jan. 23 - 26, 2018
The Institute of Electronics,
Information and Communication Engineers

AtLast: Another Three-party Lattice-based PAKE Scheme

Rakyong Choi * Hyeongcheol An † Kwangjo Kim *

Abstract: Password-based Authenticated Key Exchange (PAKE) protocol assumes that the parties share a low-entropy, easy-to-remember password to achieve the authentication with a high-entropy session key. PAKE protocols can be employed to hand-held devices for access control of sensitive personal data remotely. For communication with more than one user, the user needs to remember all passwords between other users. To resolve this problem, a three-party PAKE (3PAKE) protocol, where user only shares a password with a server, is introduced.
In this paper, we construct a novel lattice-based three-party PAKE protocol, AtLast, based on the hardness of ring-LWE assumption, with a simple design and extend Ding *et al.*'s PAKE protocol with implicit server authentication, RLWE-PPK protocol, to three-party setting by modifying the generic approach by Abdalla *et al.* Then, we compare our protocol with Xu *et al.*'s three-party PAKE protocol, RLWE-3PAKE, over lattices.

Keywords: Password-based Authenticated Key Exchange (PAKE) protocol, Ring Learning with Errors (ring-LWE) problem, RLWE-PPK protocol

1 Introduction

1.1 Background and Motivation

One of fundamental problems in cryptography is how to make a secure communication over a public unreliable channel that might be controlled by the adversary. A possible solution for this issue is to guarantee authenticity and privacy using the mutual session key from key exchange and authenticated key exchange protocols.

A key exchange protocol is a cryptographic primitive to establish the mutual session key for communication between two parties over an insecure channel and an authenticated key exchange protocol is a key exchange protocol with authentication process to prevent attacks like the man-in-the-middle attack by providing mutual authentication between parties.

In cryptography, Password-based Authenticated Key Exchange (PAKE) protocol assumes a more realistic scenario where secret keys are not uniformly distributed over a large space with a high-entropy, but chosen from a human-memorable set with a low-entropy.

Passwords are normally easier to remember for users than cryptographically secure keys. Though, in the scenario that a user communicates with more than one user, he/she needs to remember all passwords between them. Thus, in this paper, we consider a three-party PAKE (3PAKE) protocol where user only shares a password with a trusted third party, *e.g.* a server.

On the other hand, as the quantum computer becomes realistic in the near future, constructing protocols using post-quantum cryptography against quantum computing attack is currently one of challenging issues in cryptography. Indeed, the security of all public-key algorithms based on classical hard problems will no longer be assured as soon as an adequate quantum computer exists.

It is clear that the effort to develop quantum-resistant technologies is intensifying. In the US, the National Security Agency (NSA) planned to transition from its Suite B cryptographic tools to quantum-resistant algorithms. The National Institute of Standards and Technology (NIST) requested to submit post-quantum cryptographic algorithms for standards.

Most known 3PAKE protocols put their security on classical hard problems such as Diffie-Hellman problem and are unsuitable in an upcoming post-quantum world.

Searching for 3PAKE protocols that can be based on provably secure lattice assumptions is important. In the current literature, to the best of our knowledge, only one single three-party PAKE protocol stands out precisely for this reason. Xu *et al.* [1] extends Ding *et al.*'s PAKE protocol on ring-LWE [2] to three-party setting. But unfortunately, their protocol is very complicated and not very efficient.

Thus, in this paper, we design a simpler three-party PAKE protocol based on lattice.

1.2 Outline of the Paper

In Section 2, we overview the previous PAKE protocols and lattice-based key exchange protocols. Section 3 gives a notation and background knowledge such as the definition and hard problems of lattices.

In Section 4, we discuss two lattice-based PAKE pro-

* School of Computing, KAIST. 291, Daehak-ro, Yuseong-gu, Daejeon, South Korea 34141. {thepride, kkj}@kaist.ac.kr
† Graduate School of Information Security, School of Computing, KAIST. 291, Daehak-ro, Yuseong-gu, Daejeon, South Korea 34141. anh1026@kaist.ac.kr

tocols which are deeply related to our work. Then, we give the design and analysis of new lattice-based three-party PAKE protocol named as AtLast, in Section 5.

Finally, we give a concluding remark with future work in Section 6.

2 Previous Work

2.1 PAKE Protocol

The first PAKE protocol was first suggested by Bellovin and Merritt [3] without formal security analysis. PAKE protocol is beneficial for its simple use but is always vulnerable against the so-called dictionary attacks. In dictionary attacks, the adversary tries all possible combination of secret keys in a small set of values like dictionary, to break the security of a scheme. This attack is not very effective in the case of high-entropy keys but it becomes very damaging when the secret key is a password with low-entropy since the attacker has a non-negligible chance of finding the valid secret key.

Dictionary attacks are divided into two types: on-line and off-line dictionary attacks. To address this problem, several protocols are designed to be secure even when the secret key is a password. The goal of these protocols is to restrict the adversaries success to on-line guessing attacks and prevent off-line dictionary attacks. The security of these systems relies on a policy invalidating or blocking the use of a password if a certain number of failed attempts has occurred.

To prevent this kind of attacks, Bellare *et al.* [4] and Boyko *et al.* [5] independently suggested the first provably secure PAKE protocols.

In PAKE protocols, they are generally listed into two types as balanced PAKE and augmented PAKE. A balanced protocol assumes two party use the same password to authenticate a shared key for communication. This is generic for any communication, including client-server and client-client. As an example of balanced PAKE protocol, Encrypted Key Exchange (EKE) [3], Password Authenticated Key exchange (PAK) and Password-Protected Key exchange (PPK) [5], Simple Password Exponential Key Exchange (SPEKE) [6], Simple Password-Authenticated Key Exchange (SPAKE) [7], and Password Authenticated Key Exchange by Juggling (J-PAKE) [8] are well-known.

On the other hand, an augmented one is more suitable to the client-server case, in which the server does not store password-equivalent data. This means that an attacker that stole the server data still cannot impersonate as the client unless they first perform a brute force search for the password. Examples include augmented EKE [9] and PAK-Z [10].

2.2 3PAKE Protocol

The 3PAKE protocols are divided into two categories as implicit server authentication and explicit server authentication. A 3PAKE protocol with implicit server authentication can only have mutual authentication between two users, *i.e.,* the server does not authenticate a user while executing the protocol.

In contrast, a 3PAKE protocol with explicit server authentication must have mutual authentication between a server and users. Thus, a 3PAKE protocol with explicit server authentication normally has more complicated than the one with implicit server authentication.

In 2005, Abdalla *et al.* [11] proposed a formal security model (AFP model) for 3PAKE protocols. In their work, they provide a new model for 3PAKE protocols by modifying the BR model [12] and BPR model [4] and call it the Real-Or-Random (ROR) model. However, resistance to undetectable on-line dictionary attack is not taken into consideration in the AFP model. The authors of AFP model count this attack in the number of queries for message modifications which are limited to certain numbers. Hence, undetectable on-line dictionary attacks are not discriminated from detectable on-line dictionary attacks.

To improve the AFP model, Wang and Hu [13] provided a stronger security model (WH model) of 3PAKE protocol.

However, Yoneyama [14] pointed out that each model has its drawbacks. For example, the AFP model and WH model do not consider the notion of forward secrecy and WH model do not offer key privacy for the server. In addition, resistance to undetectable on-line dictionary attacks is not taken into consideration in the AFP model as stated above. To address these problems, Yoneyama extended the eCK model proposed by LaMacchia *et al.* [15] to the 3-party password-based situation, deriving the 3eCK model. The major difference between the 3eCK model and previous models is in an adversary's oracle queries and capabilities in the target session.

2.3 Key Exchange Protocol from Lattice

Ding *et al.* [16] suggested the first lattice-based key exchange protocol in 2012. Following this research, numerous work studied key exchange and authenticated key exchange protocols based on Learning with Errors (LWE) problem and its variant [17–22].

Peikert [17] gave efficient and practical lattice-based protocols for key transport and authenticated key exchange that are suitable as "drop-in" replacement for current Internet standards. Bos *et al.* [18] designed the more efficient protocol to be implemented in the TLS protocol and NewHope protocol [19] improved the performance this protocol with higher security level.

Frodo protocol [20] was suggested to remove the risk to have more structure in the hardness problem, ring structure in the case of lattice-based key exchange protocols. It was designed to rest its security on LWE problem instead of ring-LWE problem.

Zhang *et al.* [21] designed an authenticated key exchange based on lattice similar to HMQV [23].

Kyber protocol [22] is yet another authenticated key exchange protocol recently proposed by Bos *et al.* This protocol is based on a variant of LWE problem called

Module-LWE to enhance the performance and proves the security with the Quantum-accessible Random Oracle Model (QaROM) instead of classical Random Oracle Model (ROM).

There are only a small number of PAKE protocols based on lattice at the time of this research. One of these lattice-based PAKE protocols is that of Katz and Vaikuntanathan [24]. This protocol is proven secure in the standard model security, but it is not so efficient due to its Common Reference String (CRS)-based design. Recently, Zhang and Yu [25] suggested a new CRS-based PAKE framework from public key encryption with associated approximate smooth projective hashing.

But CRS-based protocols use complicated cryptographic tools to achieve standard-model security while ROM-based protocols have very simple and elegant designs. Compared to those CRS-based protocols [24,25], Ding *et al.*'s PAKE protocol [2] is more efficient since it is proven secure based on ROM.

Recently, Xu *et al.* [1] proposed the first lattice-based 3PAKE protocol extending RLWE-PAK protocol by Ding *et al.* [2], but this protocol is quite complicated since it is the 3PAKE protocol with explicit server authentication.

3 Preliminaries

3.1 Notation

We denote vectors as bold small letters (*e.g.*, $\mathbf{x}$, $\mathbf{y}$) and matrices as bold capital letters (*e.g.*, $\mathbf{A}$, $\mathbf{B}$).

Let $\mathbb{R}$ and $\mathbb{Z}$ express the set of real numbers and the set of integers, respectively and italic letters express real numbers (*e.g.*, a, b, c).

For any integer $q \geq 2$, $\mathbb{Z}_q$ denotes the ring of integers modulo q and $\mathbb{Z}_q^{n\times m}$ denotes the set of $n \times m$ matrices with entries in $\mathbb{Z}_q$.

For a ring $\mathcal{R}$ of degree n over $\mathbb{Z}$, we denote its quotient ring as $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$ and its ring element as bold italic letters (*e.g.*, $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$).

When $\mathbf{A} \in \mathbb{Z}_q^{n\times m_1}$, $\mathbf{B} \in \mathbb{Z}_q^{n\times m_2}$, we write the concatenation of $\mathbf{A}$ and $\mathbf{B}$ as $[\mathbf{A} \mid \mathbf{B}] \in \mathbb{Z}_q^{n\times(m_1+m_2)}$.

Let $f(a, b)$ be a function f on a and b. We say a function $f : \mathbb{Z} \to \mathbb{R}^+$ is *negligible* when $f = O(n^{-c})$ for all $c > 0$ and denoted by $\mathrm{negl}(n)$. A function $g(m) = \lceil m \rfloor$ is the ceiling function from $\mathbb{R}$ to $\mathbb{Z}$ such that $g(m)$ is the smallest integer which is greater than or equal to m.

3.2 Hard Problems on Lattices

Briefly, lattices are a fascinating tool in modern cryptography and a lattice Λ can be defined as a discrete subgroup of $\mathbb{R}^m$ with its basis $\mathcal{S}$. A basis $\mathcal{S}$ of Λ is a set of linearly independent vectors $\mathcal{S} = \{\mathbf{b}_1, \mathbf{b}_2, \cdots, \mathbf{b}_m\}$ which spans the lattice Λ and $\mathbf{S} = (\mathbf{b}_1|\mathbf{b}_2|\cdots|\mathbf{b}_m)$ is a basis matrix of lattice Λ.

Integer lattices are defined as a subgroup of $\mathbb{Z}^m$ instead of $\mathbb{R}^m$. For a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, we can denote lattices as a set $\Lambda_q^{\mathbf{u}}(\mathbf{A}) = \{\mathbf{e} \in \mathbb{Z}^m | \mathbf{A}\cdot\mathbf{e} = \mathbf{u} \bmod q\}$ and as a set $\Lambda_q^{\perp}(\mathbf{A}) = \{\mathbf{e} \in \mathbb{Z}^m | \mathbf{A}\cdot\mathbf{e} = \mathbf{0} \bmod q\}$ when $\mathbf{u} = \mathbf{0}$.

Lattice-based cryptography has a lot of advantages that their security is based on the average-case hardness problems like Small Integer Solution (SIS) problem and Learning With Errors (LWE) problem, which remain secure against quantum computing attacks and can be reduced to the worst-case hardness problem in lattices like Shortest Vector Problem (SVP) and Closest Vector Problem (CVP).

Among them, LWE problem is introduced by Regev [26] in 2005 and ring-LWE problem is introduced by Lyubashevsky *et al.* [27] in 2010. Both are shown to be quantum-resistant mathematical hard problem against quantum adversary.

We give a formal definition of these problems in the below:

Definition 1. (LWE problem)
For a matrix $\mathbf{A} \in \mathbb{Z}_q^{m\times n}$ with $m \geq n \log q$, a vector $\mathbf{b} \in \mathbb{Z}_q^m$ where $\mathbf{b} = \mathbf{A}\cdot\mathbf{s} + \mathbf{e} \mod q$ and a small vector $\mathbf{e} \leftarrow_\chi \mathbb{Z}_q^m$, it is hard to find a secret vector $\mathbf{s} \in \mathbb{Z}_q^n$.

Error distribution χ over $\mathbb{Z}_q$ is usually either Gaussian distribution or binomial distribution.

LWE problem can be also interpreted as a set of m independent samples $(\mathbf{a}_i, b_i) = (\langle \mathbf{s}, \mathbf{a}_i\rangle + e_i \mod q)$. If we switch the space to the ideal lattice, the computation behaves like a ring.

Definition 2. (ring-LWE problem)
In a ring $\mathcal{R}_q$, given a pair of ring elements $(\boldsymbol{a}, \boldsymbol{b})$ where $\boldsymbol{b} = \boldsymbol{a}\cdot\boldsymbol{s} + \boldsymbol{e} \mod q$ and a small vector $\boldsymbol{e} \leftarrow_\chi \mathcal{R}_q$, it is hard to find a secret vector $\boldsymbol{s} \in \mathcal{R}_q$.

We say that all instances from Definitions 1 and 2 are from LWE distribution and ring-LWE distribution, respectively.

Decisional version of LWE (ring-LWE) problem is, for m independent LWE (ring-LWE) instances, to distinguish whether the set of instances are from uniform distribution or LWE (ring-LWE) distribution.

4 Previous Lattice-based PAKE

4.1 RLWE-PAK and RLWE-PPK

Ding *et al.* [2] generalized the Diffie-Hellman like protocols, PAK and PPK, by Boyko *et al.* [5] in lattice-based setting.

In their protocol, Cha and Mod functions are used. For a set $E = \{-\lceil\frac{q}{4}\rfloor, \cdots, \lceil\frac{q}{4}\rfloor\}$

Cha is the characteristic function where

$$\mathsf{Cha}(a) = \begin{cases} 0, & \text{if } a \in E = \{-\lceil\frac{q}{4}\rfloor, \cdots, \lceil\frac{q}{4}\rfloor\} \\ 1, & \text{otherwise.} \end{cases}$$

and $\mathsf{Mod}_2 : \mathbb{Z}_q \times \{0,1\} \to \{0,1\}$ is defined as:

$$\mathsf{Mod}_2(v, b) = \left(v + b\cdot\frac{q-1}{2}\right) \bmod q \bmod 2$$

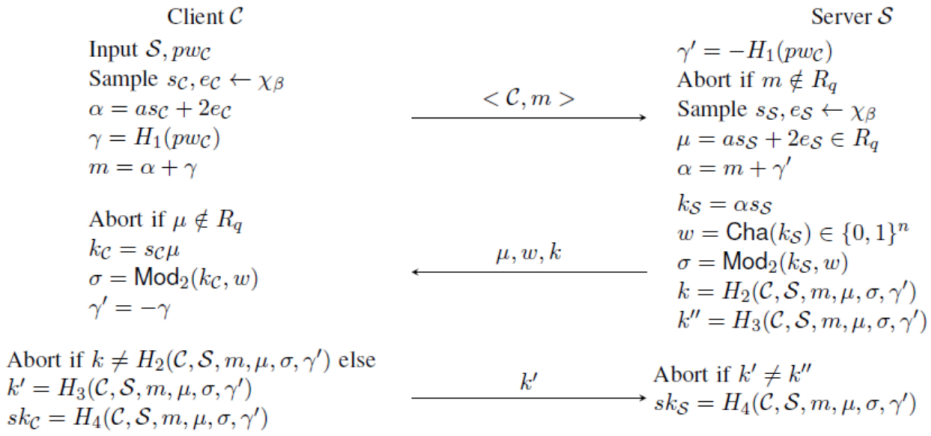

Figure 1: RLWE-PAK Protocol [2]

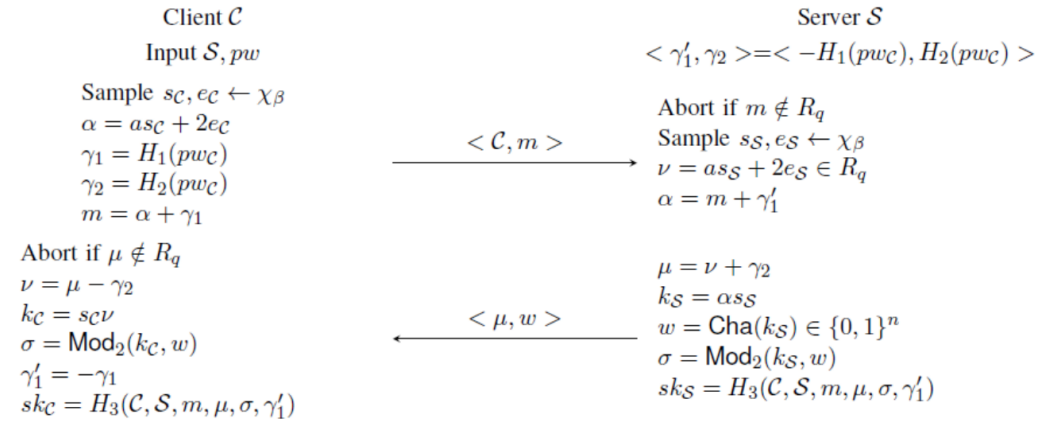

Figure 2: RLWE-PPK Protocol [2]

They defined the new lattice-based hardness assumption called Pairing with Errors (PWE) problem which can be reduced to RLWE problem.

Definition 3. (PWE problem)
In a ring $\mathcal{R}_q$, given a tuple of ring elements $(\boldsymbol{a}, \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{k}) \in \mathcal{R}_q^4$ where $(\boldsymbol{a}, \boldsymbol{x}) \in \mathcal{R}_q^2$ are uniformly chosen, $\boldsymbol{y} = \boldsymbol{a} \cdot \boldsymbol{s} + 2\boldsymbol{e}$ with $\boldsymbol{e} \leftarrow_\chi \mathcal{R}_q$ is a ring-LWE sample, and $\omega = \mathsf{Cha}(\boldsymbol{x} \cdot \boldsymbol{s} + \boldsymbol{g})$ for some $\boldsymbol{g} \leftarrow_\chi \mathcal{R}_q$ and , it is hard to find $\sigma = \mathsf{Mod}_2(\boldsymbol{x} \cdot \boldsymbol{s} + \boldsymbol{g}, \omega)$.

Figures 1 and 2 show the description of lattice-based PAKE protocols with explicit server authentication and implicit server authentication, respectively.

4.2 RLWE-3PAKE

Xu *et al.* [1] introduced the first lattice-based 3PAKE protocol extending Ding *et al.*'s RLWE-PAK protocol. They assume that the server $\mathcal{S}$ is fully trustful and clients $\mathcal{A}$ and $\mathcal{B}$ seek to have server's help to establish a shared session key.

Then, they implemented their RLWE-3PAKE protocol with the similar security parameter used in NewHope protocol [19] and compared the result with another 3PAKE protocol based on elliptic curve.

5 AtLast Protocol

5.1 System Model

The 3PAKE protocols are divided into two categories as implicit server authentication and explicit server authentication. A 3PAKE protocol with implicit server authentication can only have mutual authentication between two users, *i.e.,* the server does not authenticate a user while executing the protocol. In contrast, a 3PAKE protocol with explicit server authentication must have mutual authentication between a server and users. Thus, a 3PAKE protocol with explicit server authentication normally has more complicated than the one with implicit server authentication.

In our protocol, we assume that the server is honest but curious so that the server should not be able to gain any information on the value of that session key during the protocol. To achieve this property, we design a 3PAKE protocol with implicit server authentication.

5.2 Our Construction

We design a novel 3PAKE protocol based on lattice, AtLast, as shown in Figure 3 by extending RLWE-PPK protocol.

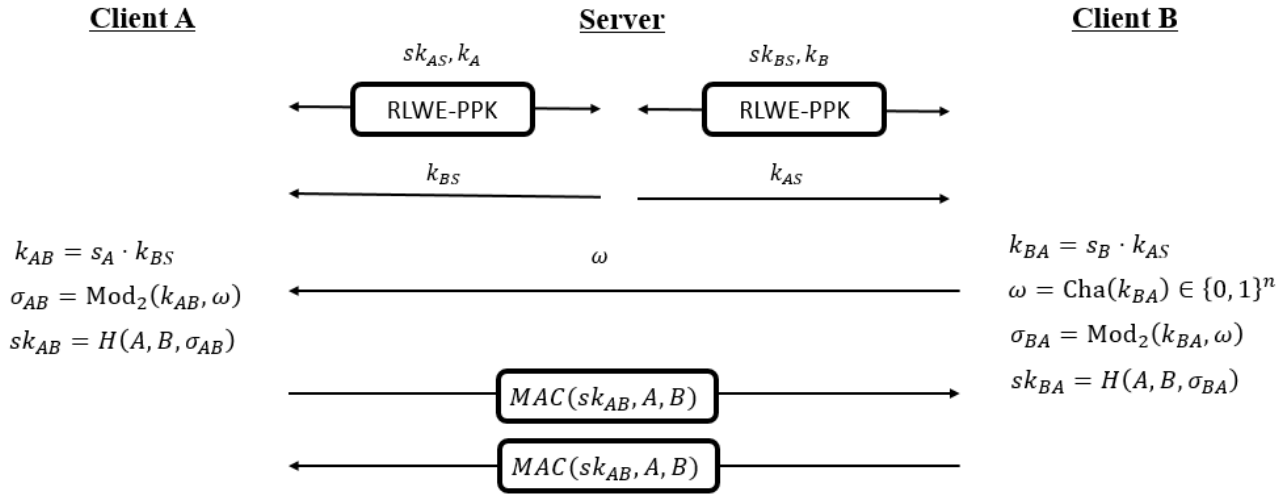

Figure 3: Our AtLast Protocol

During the RLWE-PPK key exchange process between server and each client, we assume that server uses the same secret key $\boldsymbol{s}_S$, while the public keys for each process are different as $\nu_A = \boldsymbol{a} \cdot \boldsymbol{s}_S + \boldsymbol{e}_{SA}$ and $\nu_B = \boldsymbol{a} \cdot \boldsymbol{s}_S + \boldsymbol{e}_{SB}$.

Then, we compute $\boldsymbol{k}_{AB} = \boldsymbol{s}_A \cdot \boldsymbol{k}_{BS} = \boldsymbol{s}_A \cdot \boldsymbol{s}_S\{\boldsymbol{a} \cdot \boldsymbol{s}_B + 2\boldsymbol{e}_B\}$ and $\boldsymbol{k}_{BA} = \boldsymbol{s}_B \cdot \boldsymbol{k}_{AS} = \boldsymbol{s}_B \cdot \boldsymbol{s}_S\{\boldsymbol{a} \cdot \boldsymbol{s}_A + 2\boldsymbol{e}_A\}$ for client $\mathcal{A}$ and $\mathcal{B}$, respectively.

After that, similar to the process of RLWE-PPK protocol, we apply Cha and Mod_2 to have the mutual key to establish the shared secret key between two clients and use MAC function for mutual authentication between them.

5.3 Security Requirements

To check the security of AtLast protocol, we have to prove the following security requirements of 3PAKE protocols.

1. **Session key security**
   If two uncorrupted clients in the proposed protocol complete matching sessions, they have the same key and the probability that the adversary guesses whether the key is from the protocol or from random is negligible.

2. **Known key security**
   Even after an adversary $\mathcal{A}$ has acquired one particular session key, other session keys are still secure.

3. **Forward secrecy**
   Even if a client's password is leaked to the adversary, the adversary is not able to acquire previous session keys, even though the adversary actively interfered, or tried to act as a man-in-the-middle attack.

4. **Weak perfect forward secrecy (wPFS)**
   Even though client's long-term keys are compromised, the secrecy of previously established session-keys is guaranteed, but only for sessions in which the adversary did not actively interfere.

5. **Key privacy**
   In the proposed protocol, the server should not be able to gain any information on the value of the session key, even though the server's help is mandatory to establish a session key between two clients in the protocol.

6. **Resistance to three classes of password guessing attacks**
   To ensure the security of the password, the protocol should resist undetectable online password guessing attacks, detectable online password guessing attacks, and offline password guessing attacks.

7. **Resistance to other various attacks**
   The protocol should withstand other attacks such as user impersonation, modification and man-in-the-middle attacks.

Among these security requirements, we show the validity of our protocol for some security requirements.

We assume that the adversary $\mathcal{A}$ can make queries to any instance as the former security modelling of key exchange protocols [4, 12, 28]. $\mathcal{A}$ can send messages to a client, run the protocol to get the appropriate session key, reveal the some session key, corrupt some clients, *etc.*

In the following proof sketch of our protocol, we assume the following conjecture.

Conjecture 1. *If RLWE-PAK protocol based on ring-LWE is secure in the ROM, our AtLast protocol is also secure in the ROM.*

Session key security

In our proposed protocol, the server and clients authenticate each other via the shared password.

Thus, anyone who does not have the password of clients (*e.g.* pw_A for Client $\mathcal{A}$) cannot compute the right computation for $(\gamma_1, \gamma_2) = (H_1(pw_A), H_2(pw_A))$.

Hence, he/she cannot be authenticated by the other client and the proposed 3PAKE protocol provides mutual authentication between the server and the client like the original RLWE-PPK protocol.

On the other hand, since unauthorized client will not be authenticated by the server and unable to interact with other legitimate client, our protocol provides session key security.

Known key security

The clients use ephemeral keys to establish the session key. Thus, a session key has no relation to other session keys. Though the adversary $\mathcal{A}$ has one session key, other session keys will remain secure. Therefore, our protocol provides known key security.

Forward secrecy and wPFS

Since our protocol provides known key security and the session key is independent of the password, leakage of the password does not make the adversary have previously established session keys unless the adversary interfered the protocol directly. Therefore, our protocol provides weak perfect forward secrecy.

Key privacy

In our protocol, the server cannot compute the value of the session key, even though the server provides ephemeral keys while establishing a session key between two clients in the protocol. Thus, our protocol satisfies the key privacy property.

6 Conclusion and Future Work

In this paper, we designed a novel 3PAKE protocol with implicit server authentication based on the RLWE-PPK [2] and sketch the security requirements of the proposed protocol. Though RLWE-3PAKE protocol assumed that the server is fully trustful, we assume more realistic scenario that the server might be not fully trustful.

Our approach is based on the generic construction by Abdalla *et al.* [11] in Figure 4 since we use MAC protocol for further authentication between two clients but we modify the construction to adjust it to the lattice-based cryptography

Compared to RLWE-3PAKE protocol by Xu *et al.* [1], our protocol is conceptually simpler lattice-based 3PAKE protocol than the protocol by Xu *et al.* [1]. But, we only gave the proof sketch of some of security requirements and missed the proof for the resistance to password guessing attacks and other various attacks.

As future work, we plan to extend the proposed protocol to a group-oriented setting (*i.e.* lattice-based group PAKE protocol) and multi-party setting (*i.e.* lattice-based multi-party PAKE protocol).

In addition, we will give the formal security proof for both classical and quantum adversaries from Random Oracle Model (ROM) and Quantum-accessible Random Oracle Model (QaROM) and embed our protocol to internet protocols like TLS protocol.

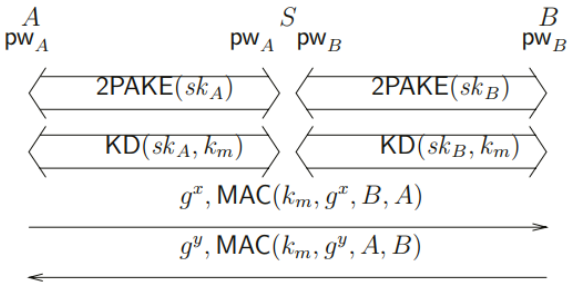

Figure 4: A generic construction by Abdalla *et al.* [11]

Acknowledgement

This work was partly supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No. 2017-0-00555, Towards Provable-secure Multi-party Authenticated Key Exchange Protocol based on Lattices in a Quantum World) and National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. NRF-2015R1A2A2A01006812, Design and Security Analysis of Novel Lattice-based Fully Homomorphic Signatures Robust to Quantum Computing Attack).

References

[1] 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 Cryptology ePrint Archive 2017/360*, 2017.

[2] J. Ding, S. Alsayigh, J. Lancrenon, R. Saraswathy, and M. Snook, "Provably secure password authenticated key exchange based on rlwe for the post-quantum world," in *Cryptographers' Track at the RSA Conference*, pp. 183–204, Springer, 2017.

[3] S. M. Bellovin and M. Merritt, "Encrypted key exchange: Password-based protocols secure against dictionary attacks," in *IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 72–84, IEEE, 1992.

[4] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks," in *Advances in Cryptology–EUROCRYPT 2000*, pp. 139–155, Springer, 2000.

[5] V. Boyko, P. MacKenzie, and S. Patel, "Provably secure password-authenticated key exchange using diffie-hellman," in *Advances in Cryptology–EUROCRYPT 2000*, pp. 156–171, Springer, 2000.

[6] D. P. Jablon, "Strong password-only authenticated key exchange," *ACM SIGCOMM Computer Communication Review*, vol. 26, no. 5, pp. 5–26, 1996.

[7] M. Abdalla and D. Pointcheval, "Simple password-based encrypted key exchange protocols," in *Cryptographers' Track at the RSA Conference*, vol. 3376, pp. 191–208, Springer, 2005.

[8] F. Hao and P. Y. Ryan, "Password authenticated key exchange by juggling," in *International Workshop on Security Protocols*, pp. 159–171, Springer, 2008.

[9] S. M. Bellovin and M. Merritt, "Augmented encrypted key exchange: a password-based protocol secure against dictionary attacks and password file compromise," in *ACM Conference on Computer and Communications Security*, pp. 244–250, ACM, 1993.

[10] P. MacKenzie, "The PAK suite: Protocols for password-authenticated key exchange," in *Contributions to IEEE P1363.2*, 2002.

[11] M. Abdalla, P.-A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *International Workshop on Public Key Cryptography*, pp. 65–84, Springer, 2005.

[12] M. Bellare and P. Rogaway, "Entity authentication and key distribution," in *Advances in Cryptology–CRYPTO'93*, pp. 232–249, Springer, 1993.

[13] W. Wang and L. Hu, "Efficient and provably secure generic construction of three-party password-based authenticated key exchange protocols," in *INDOCRYPT*, pp. 118–132, Springer, 2006.

[14] K. Yoneyama, "Password-based authenticated key exchange without centralized trusted setup," in *International Conference on Applied Cryptography and Network Security*, pp. 19–36, Springer, 2014.

[15] B. LaMacchia, K. Lauter, and A. Mityagin, "Stronger security of authenticated key exchange," in *International Conference on Provable Security*, pp. 1–16, Springer, 2007.

[16] J. Ding, X. Xie, and X. Lin, "A simple provably secure key exchange scheme based on the learning with errors problem," *IACR Cryptology ePrint Archive 2012/688*, 2012.

[17] C. Peikert, "Lattice cryptography for the internet," in *International Workshop on Post-Quantum Cryptography*, pp. 197–219, Springer, 2014.

[18] J. W. Bos, C. Costello, M. Naehrig, and D. Stebila, "Post-quantum key exchange for the tls protocol from the ring learning with errors problem," in *IEEE Symposium on Security and Privacy*, pp. 553–570, IEEE, 2015.

[19] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, "Post-quantum key exchange-a new hope," in *USENIX Security Symposium*, pp. 327–343, 2016.

[20] J. Bos, C. Costello, L. Ducas, I. Mironov, M. Naehrig, V. Nikolaenko, A. Raghunathan, and D. Stebila, "Frodo: Take off the ring! practical, quantum-secure key exchange from LWE," in *ACM SIGSAC Conference on Computer and Communications Security*, pp. 1006–1018, ACM, 2016.

[21] J. Zhang, Z. Zhang, J. Ding, M. Snook, and Ö. Dagdelen, "Authenticated key exchange from ideal lattices," in *Advances in Cryptology–EUROCRYPT 2015*, pp. 719–751, 2015.

[22] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, and D. Stehlé, "CRYSTALS–Kyber: a CCA-secure module-lattice-based KEM," *IACR Cryptology ePrint Archive 2017/634*, 2017.

[23] H. Krawczyk, "HMQV: A high-performance secure Diffie-Hellman protocol (extended abstract)," in *Advances in Cryptology–CRYPTO 2005*, pp. 546–566, Springer, 2005.

[24] J. Katz and V. Vaikuntanathan, "Smooth projective hashing and password-based authenticated key exchange from lattices," in *Advances in Cryptology–ASIACRYPT 2009*, vol. 5912, pp. 636–652, Springer, 2009.

[25] J. Zhang and Y. Yu, "Two-round PAKE from approximate SPH and instantiations from lattices," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 37–67, Springer, 2017.

[26] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in *Annual ACM symposium on Theory of computing*, pp. 84–93, ACM, 2005.

[27] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 1–23, Springer, 2010.

[28] M. Bellare and P. Rogaway, "Provably secure session key distribution: the three party case," in *Annual ACM symposium on Theory of computing*, pp. 57–66, ACM, 1995.