IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received January 22, 2020, accepted January 27, 2020, date of publication January 30, 2020, date of current version February 11, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2970537

A Probably Secure Bi-GISIS Based Modified AKE Scheme With Reusable Keys

SEDAT AKLEYLEK AND KÜBRA SEYHAN
Department of Computer Engineering, Ondokuz Mayıs University, 55139 Samsun, Turkey
Corresponding author: Sedat Akleylek (sedat.akleylek@bil.omu.edu.tr)

This study was partially supported by TUBITAK under grant EEEAG-117E636.

ABSTRACT In this paper, we propose a novel authenticated key exchange scheme based on the Bi-GISIS problem for the post-quantum world. The security of the proposed scheme is based on the hardness assumption of the Bi-GISIS problem. The reusable key property is provided for the proposed scheme in the random oracle model by using the bilateral pasteurization method. To obtain an authenticated key exchange scheme, we use the implicit authentication steps. The security analysis of the proposed scheme is presented in the Bellare-Rogaway security model, where weak perfect forward secrecy is provided. We also give novel perspective to the Bi-GISIS based authenticated key exchange problem.

INDEX TERMS Lattice-based cryptography, authenticated key exchange, Bi-GISIS problem, reusable keys.

I. INTRODUCTION

Authenticated key exchange (AKE) schemes aim to obtain a shared secret key by including authentication steps in the communication between two parties in the insecure channel. Authentication steps allow these schemes to become resistant to various attacks such as man-in-the-middle [1]. The security of cryptosystems is based on computationally difficult problems. Such as the integer factorization problem and the discrete logarithm problem. That cannot be solved in polynomial time by using traditional computers. However, an algorithm, proposed by Shor in 1994 [2], solved these problems in polynomial time in a quantum computer. As a result of this algorithm, traditional AKE schemes are insecure in the post-quantum world. Lattice-based cryptosystem family is one of the fundamental systems that are believed to be safe in the post-quantum. The security of these systems is based on hard lattice problems that are difficult to solve in polynomial time for both current and post-quantum computing systems. The main hard lattice problems are shortest vector problem (SVP), closest vector problem (CVP), short integer solution (SIS), inhomogeneous short integer solution (ISIS), learning with errors (LWE), and ring variant of learning with errors (RLWE) [3]. There are also alternative hard lattice problems proposed by reducing the hardness of these main problems. For example, the bilateral generalization inhomogeneous short integer solution (Bi-GISIS) problem was described in [4].

Basic information security concepts such as confidentiality and authentication, are guaranteed by AKE schemes. To provide confidentiality, the session key is prevented from being obtained by adversaries, while authentication is provided by preventing adversaries from imitating the communication [5]. There are two different ways of authentication for key exchange (KE) schemes: implicit and explicit [6]. In explicit authentication, signature schemes and message authentication codes (MAC) are used. However, in the implicit authentication there is no need to use additional structures such as those in the explicit authentication. Instead, ephemeral-static public/private keys and hash functions are used. While static key values are needed to achieve the weak perfect forward secrecy (wPFS), ephemeral keys and hash functions are used to provide authentication [7]. There are several studies to construct quantum resistant AKE schemes with explicit authentication in [3], [8], and implicit authentication in [7], [9].

A. MOTIVATION AND CONTRIBUTION

The security of the AKE scheme given in [7] is based on the hardness assumption of the RLWE problem. Unlike other proposed AKE schemes, the proposed scheme contains reusable key property in the random oracle model (ROM). This property is provided by the bilateral pasteurization method and then the same key can be used in several

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

executions of the AKE scheme. Moreover, adapting reusable key property to different key exchange schemes is needed for the post-quantum world.

In this paper, we modify the KE scheme described in [4] to provide a novel solution the open problem given in [4]. The security of the proposed scheme is based on the hardness assumption of the Bi-GISIS problem whose security can be reduced to the module variant of learning with errors (MLWE) problem. In the modified scheme, we use the bilateral pasteurization method to achieve the reusable key property. With the modified scheme, the same key is guaranteed to be reused in multiple executions. Our main aim is to construct an authenticated version of a KE scheme given in [4]. We prefer to use implicit authentication steps to achieve this. We also explain the security analysis of the proposed scheme in the ROM under the Bellare-Rogaway (BR) security model, which provides wPFS.

B. ORGANIZATION

The rest of this paper is organized as follows. In Section II, we provide mathematical background. In Section III, we explain the proposed scheme step-by-step and then give the correctness of the proposed Bi-GISIS based AKE scheme. Then, we present a detailed security analysis of the AKE scheme under the BR model. In Section IV, we compare the proposed scheme with the previous ones. Conclusion of this paper is given in Section V.

II. PRELIMINARIES

In this section, we give mathematical background to construct an AKE with reusable keys.

Bilateral generalization inhomogenous short integer solution problem is recalled in Definition 1.

Definition 1 (Bi-GISIS [4]): Let $A \in \Re_q^{m\times m}$ be a random matrix with rank m. Given x_1, x_2^T such that

$$\begin{aligned} x_1 &= As_1 + e_1 \mod q \\ x_2^T &= s_2^T A + e_2^T \mod q \end{aligned}$$

where $s_1, s_2^T, e_1, e_2^T \xleftarrow{r} D_{\Re^m,\sigma}$, the aim is to find the secret vectors s_1, s_2^T.

In Definition 2, the decisional variant of bilateral generalization inhomogenous short integer solution problem (DBi-GISIS) is given.

Definition 2 (DBi-GISIS [4]): The aim is to decide the distribution of $K = \{A, x_1, x_2^T\}$. There are two cases: K is sampled either

i) $x_1 = As_1 + e_1 \mod q$, $x_2^T = s_2^T A + e_2^T \mod q \leftarrow$*Bi-GISIS, or*

ii) $K \xleftarrow{r} U(\Re_q^{m\times m}) \times U(\Re_q^m) \times U(\Re_q^m)$.

In Definition 3, neg function is provided. It's needed in the assumption of the DBi-GISIS problem and the security analysis of the proposed scheme.

Definition 3 (Neg Function [4]): neg: $\mathbb{N} \rightarrow R$ function can be defined as for every $c > 0$ if there exists an $n_0 \in \mathbb{N}$ such that neg $(n) < \frac{1}{n^c}$ for every $n > n_0$, then neg is a negligible function.

The hardness assumption of the DBi-GISIS is detailed in Definition 4.

*Definition 4 (DBi-GISIS Assumption [4]): Let $A \in \Re_q^{m\times m}$ be a random matrix, $\{A, x_1, x_2^T\} \leftarrow$ Bi-GISIS where $s_1, s_2^T, e_1, e_2^T \xleftarrow{r} D_{\Re^m,\sigma}$, and $c_1, c_2^T \xleftarrow{r} U(\Re_q^m)$. Then, any probabilistic polynomial algorithm (**PPA**) satisfies*

$$|Pr[\boldsymbol{PPA}(A, x_1, x_2^T) = 1] - Pr[\boldsymbol{PPA}(A, c_1, c_2^T) = 1]| < neg(n).$$

The hardness assumption of the DBi-GISIS problem is explained with Lemma 1. The idea is the same used in [4] (in Lemma 18).

Lemma 1: Let the DBi-GISIS assumption be satisfied,

$$\begin{aligned} K_1 &= \{A, x_1, x_2^T\} \xleftarrow{r} \text{Bi-GISIS, and} \\ K_2 &= \{A, x_1', x_2'^T\} \xleftarrow{r} U(\Re_q^{m\times m}) \times U(\Re_q^m) \times U(\Re_q^m). \end{aligned}$$

*Then, there exists no **PPA** distinguishing between K_1 and K_2 with non-negligible advantage.*

The equivalent hard problem to the DBi-GISIS is given in Lemma 2. The idea is the same used in [4] (in Lemma 19).

Lemma 2: Assume that the decisional module variant of learning with errors (M-DLWE) [10] is computationally hard problem. Then, the assumption DBi-GISIS, which is equivalent to M-DLWE, is satisfied.

By combining Lemma 1 and Lemma 2, Corollary 1 defines the hardness assumption of the Bi-GISIS problem.

Corollary 1: As long as the hardness assumption of the DBi-GISIS is satisfied, the security of the Bi-GISIS problem relies on the hardness assumption DBi-GISIS, which is equivalent the M-DLWE problem.

In Definition 5, MSB reconciliation function that is used to reconcile errors in the proposed AKE scheme is given.

Definition 5 (MSB Reconciliation Function [4]): Given $u \in \mathbb{Z}_q$, then

$$r = MSB(u) : \begin{cases} r = 0, & \text{if } \frac{q}{4} < |u| < \frac{q}{2} \\ r = 1, & \text{otherwise} \end{cases}$$

The main aim is to generate the same shared secret key in the proposed AKE scheme. To achieve this, the most significant bit (r) of the coefficient is selected.

Remark 1: MSB reconciliation function is defined for $u \in \mathbb{Z}_q$. However, in the proposed AKE, we use $x \in \Re_q^m$. MSB function outputs each coefficient, i.e., $x_i \in \mathbb{Z}_q^n$ for $i \in [m]$ is computed seperately.

The reusable key idea is given in Definition 6.

*Definition 6 (Reusable Key [7]): Assume that the same keys are generated/used in the several executions of the scheme. If an adversary (**ADV**) cannot obtain any information about the secret keys by using previous ones, then the scheme has reusable key property.*

The pasteurization method is used to ensure that the reusable key property is achieved in KE protocols [7]. By using this method, the probability of distinguishing the

Notations		
SS	:	Static secret key.
ET	:	Error term.
SP	:	Static public key.
ES	:	Ephemeral secret key.
EP	:	Ephemeral public key.
SSK	:	Shared secret key.
ROM	:	Random oracle model.
wPFS	:	Weak perfect forward secrecy.
R	:	Real numbers.
$\Re$	:	$\mathbb{Z}[x]/(x^n+1)$.
$\Re_q$	:	$\mathbb{Z}_q[x]/(x^n+1)$.
$\Re_q^{m\times m}$	:	A random matrix from $\Re_q$ with rank of m.
$\|\|x\|\|$	:	Euclidean norm of vector x.
x^T	:	Transpose of vector x.
$x \leftarrow^r U(X)$	:	Vector x is chosen uniformly at random from X.
θ	:	A distribution that is arbitrary over $\Re_q^m$.
ϑ	:	A distribution that is statistically close to the uniform distribution over $\Re_q^m$.
$\mathbb{Z}_q$	:	$\mathbb{Z}/q\mathbb{Z}$.
$D_{\Re^m,\sigma}$	:	Discrete Gaussian distribution with σ over $\Re^m$.
$D^{\text{Bi-GISIS}}_{s_1,s_2^T,D_{R^m}}$	:	The distribution of Bi-GISIS.
$\sigma=\alpha(nl/\log(nl))^{\frac{1}{4}}$	:	Standard deviation.
$m\geq 2$	:	Module dimension.
$i\in[n]$	:	$i\in\{1,\ldots,n\}$.
δ	:	Positive real.
$\lambda=O(n)$	:	Security parameter.
H_1	:	$H_1:\{0,1\}^*\rightarrow D_{\Re^m,\sigma}$.
H_2	:	$H_2:\{0,1\}^*\rightarrow \{0,1\}^\lambda$.
β	:	Norm bound $\beta=\sqrt{n}\sigma$.

difference between RLWE samples and uniformly random values is negligible in the presence of an adversary [11]. The core idea of the proposed method is that if an **ADV** controls the protocol, he/she cannot obtain any information about the secret key. If for any PPT adversary the advantage is negligible, then the proposed scheme is called secure under this [12].

In Definition 7, the modified or namely bilateral pasteurization method is explained to provide reusable key property for the Bi-GISIS based schemes.

Definition 7 (Bilateral Pasteurization Method - Bi-P): Let $A \in \Re_q^{m\times m}$ be a random matrix, $\{x_1, x_2^T\}$ be sampled from the Bi-GISIS distribution described in Definition 1, H_1 be a cryptographic hash function and $g_2, g_1^T \leftarrow^r D_{\Re^m,\sigma}$. Then, the bilateral pasteurization is defined as

$$\begin{aligned}\overleftrightarrow{x_1} &= x_1 + AH_1(x_1) + g_2\\ \overleftrightarrow{x_2}^T &= x_2^T + H_1(x_2)^T A + g_1^T.\end{aligned} \quad (1)$$

As a result of being non-commutativity of matrix multiplication, the terms $AH_1(x_1)$ and $H_1(x_2)^T A$ are different from each other. This method yields two cases.

- If $\{x_1, x_2^T\} \in$ Bi-GISIS, then $\{\overleftrightarrow{x_1}, \overleftrightarrow{x_2}^T\} \in$ Bi-GISIS.
- If $\{x_1, x_2^T\} \notin$ Bi-GISIS, then $\{\overleftrightarrow{x_1}, \overleftrightarrow{x_2}^T\} \notin$ Bi-GISIS.

The main idea of the Bi-P method is that nobody can obtain any information about the secret keys by using $\{\overleftrightarrow{x_1}, \overleftrightarrow{x_2}^T\}$. In the second case, the distribution $\{\overleftrightarrow{x_1}, \overleftrightarrow{x_2}^T\} \notin$ Bi-GISIS is statistically close to uniformly distribution. To provide this, we propose the extended versions of Lemma 3 and Lemma 4 given in [13].

Lemma 3: Let $x \leftarrow^r \theta$, $y \leftarrow^r \vartheta$. Then, $p = x + y$ is statistically close to the uniform distribution:

$$Pr[p = x + y] \leq \frac{1}{q^{mn}}$$

Lemma 4: Let q be a prime number, $A \in \Re_q^{m\times m}$ be a uniformly random matrix, and $p \in \Re_q^m$. Given $(A, b_1 = As_1 + e_1\text{-}b_2^T = s_2^T A + e_2^T) \leftarrow^r D^{Bi\text{-}GISIS}_{s_1,s_2^T,D_{\Re^m,\sigma}}$, then the multiplication of the probabilities of b_1 and b_2^T:

$$Pr[b_1 = p] \cdot Pr[b_2^T = p] \leq \frac{1}{q^{2mn}}$$

By combining Lemma 3 and Lemma 4, we explain the probability of the Bi-GISIS distribution in Corollary 2.

Corollary 2: If $Pr[As_1 + e_1 = p] \cdot Pr[s_2^T A + e_2^T = p] = \frac{1}{q^{2\,mn}} + neg(\lambda)$, then the distribution $D^{Bi\text{-}GISIS}_{s_1,s_2^T,D_{\Re^m,\sigma}}$, which is statistically close to uniform distribution over $\Re_q^m$, is obtained.

	Alice		Bob
		$A \in \Re_q^{m\times m}$	
SS:	$s_1 \leftarrow^r D_{\Re^m,\sigma}$		$s_2^T \leftarrow^r D_{\Re^m,\sigma}$
ET:	$e_1 \leftarrow^r D_{\Re^m,\sigma}$		$e_2^T \leftarrow^r D_{\Re^m,\sigma}$
SP:	$p_1 = As_1 + e_1$		$p_2^T = s_2^T A + e_2^T$
ES:	$r_1 \leftarrow^r D_{\Re^m,\sigma}$		$r_2^T \leftarrow^r D_{\Re^m,\sigma}$
ET:	$g_1^T, f_1, h_1 \leftarrow^r D_{\Re^m,\sigma}$		$g_2, f_2^T, h_2^T \leftarrow^r D_{\Re^m,\sigma}$
EP:	$x_1 = Ar_1 + f_1$	$\xrightarrow{x_1}$	$x_2^T = r_2^T A + f_2^T$
	$c = H_1(\bar{A}, \bar{B}, x_1)$		$c = H_1(\bar{A}, \bar{B}, x_1)$
		$\xleftarrow{x_2^T}$	$d^T = H_1(\bar{A}, \bar{B}, x_1, x_2^T)$
	$d^T = H_1(\bar{A}, \bar{B}, x_1, x_2^T)$		
Bi-P:	$\overleftrightarrow{x_2}^T = x_2^T + d^T A + g_1^T$		$\overleftrightarrow{x_1} = x_1 + Ac + g_2$
	$k_1 = (p_2^T + \overleftrightarrow{x_2}^T)(s_1 + r_1 + c) - (p_2^T s_1) + h_1$		$k_2 = (s_2^T + r_2^T + d^T)(p_1 + \overleftrightarrow{x_1}) - (s_2^T p_1) + h_2^T$
	$\psi_1 = \text{MSB}(k_1)$		$\psi_2 = \text{MSB}(k_2)$
SSK:	$sk_1 = H_2(\bar{A}, \bar{B}, x_1, x_2^T, \psi_1)$		$sk_2 = H_2(\bar{A}, \bar{B}, x_1, x_2^T, \psi_2)$

FIGURE 1. **Bi-GISIS based Authenticated Key Exchange Scheme with Reusable Keys.**

The distribution of the Bi-P method is given in Corollary 3. It's obtained by combining Lemma 3, Corollary 2 and Definition 7.

Corollary 3: Let H_1 be a ROM that the output of H_1 is sampled from $D_{\Re^m,\sigma}$, $x_1, x_2^T \leftarrow^r \theta$ and $e_1, e_2^T \leftarrow^r D_{\Re^m,\sigma}$. Then, the components of the Bi-P method $\overleftrightarrow{x_1} = x_1 + AH_1(x_1) + e_1$ and $\overleftrightarrow{x_2}^T = x_2^T + H_1(x_2)^T A + e_2^T$ are statistically close to uniform distribution in the ROM.

By using Corollary 3, we conclude that if **ADV** controls a party in the scheme, he/she shouldn't obtain any information about the secret keys. Due to the hardness assumption of the Bi-GISIS problem, an adversary cannot distinguish between a statistically uniform distribution and the Bi-GISIS distribution.

In Definition 8, fresh session is recalled.

Definition 8 (Fresh Session [8]): Let $\widehat{sid}$ be a session matching sid. The sid, an accomplished session, is called fresh, either sessionKR(sid) and sessionKR($\widehat{sid}$) shouldn't query or if $\widehat{sid}$ doesn't exist, then staticKR(A) and staticKR(B) shouldn't query.

III. BI-GISIS BASED AUTHENTICATED KEY EXCHANGE SCHEME WITH REUSABLE KEY

In this section, we explain the Bi-GISIS based AKE scheme with reusable key in the ROM and give the correctness of the proposed scheme. Then, we provide a detailed security analysis in the Bellare-Rogaway (BR) [14] security model.

To construct a novel AKE scheme, we modify the KE scheme given in [4]. By using the Bi-P approach given in Definition 7, we provide reusable keys for the modified scheme. The security of our scheme is just based on the hardness assumption of the Bi-GISIS problem. The proposed scheme uses hash functions, static keys and ephemeral keys to provide the implicit authentication. In Figure 1, the proposed AKE scheme with reusable keys is summarized. In the proposed scheme, the first step of the implicit authentication is the usage of static/ephemeral private and public key pairs. Static public and private key pairs, generated once in each execution of the proposed scheme, contain authentication information about the parties. Ephemeral public and private key pairs, which are reconstructed each execution of the proposed scheme, used in exchange information between the parties. The second step of the implicit authentication is provided by the hash functions H_1 and H_2. The reusable key property of the proposed scheme is ensured by the Bi-P method. To obtain the same shared secret key, the MSB reconciliation function is used. Briefly, the same authenticated shared secret key ($sk_1 = sk_2$) is obtained by using all of these components, which are described in Figure 1.

The correctness of the proposed AKE scheme is given in Section III-A.

A. CORRECTNESS

We give the correctness of the proposed scheme in Equation (2).

$$\begin{aligned}
k_1 &= (p_2^T + \overleftrightarrow{x_2}^T)(s_1 + r_1 + c) - (p_2^T s_1) + h_1 \\
&= (s_2^T A + e_2^T + x_2^T + d^T A + g_1^T)(s_1 + r_1 + c) \\
&\quad - (s_2^T A + e_2^T) s_1 + h_1 \\
&= (s_2^T A + e_2^T + r_2^T A + f_2^T + d^T A + g_1^T)(s_1 + r_1 + c) \\
&\quad - (s_2^T A s_1 + e_2^T s_1) + h_1 \\
&= s_2^T A s_1 + s_2^T A r_1 + s_2^T A c + e_2^T s_1 + e_2^T r_1 + e_2^T c \\
&\quad + r_2^T A s_1 + r_2^T A r_1 + r_2^T A c + f_2^T s_1 + f_2^T r_1 + f_2^T c \\
&\quad + d^T A s_1 + d^T A r_1 + d^T A c + g_1^T s_1 + g_1^T r_1 + g_1^T c \\
&\quad - s_2^T A s_1 - e_2^T s_1 + h_1 \\
k_2 &= (s_2^T + r_2^T + d^T)(p_1 + \overleftrightarrow{x_1}) - (s_2^T p_1) + h_2^T
\end{aligned}$$

$$
\begin{aligned}
&= (s_2^T + r_2^T + d^T)(As_1 + e_1 + x_1 + Ac + g_2) \\
&\quad - s_2^T(As_1 + e_1) + h_2^T \\
&= (s_2^T + r_2^T + d^T)(As_1 + e_1 + Ar_1 + f_1 + Ac + g_2) \\
&\quad - (s_2^T As_1 + s_2^T e_1) + h_2^T \\
&= s_2^T As_1 + r_2^T As_1 + d^T As_1 + s_2^T e_1 + r_2^T e_1 + d^T e_1 \\
&\quad + s_2^T Ar_1 + r_2^T Ar_1 + d^T Ar_1 + s_2^T f_1 + r_2^T f_1 + d^T f_1 \\
&= s_2^T Ac + r_2^T Ac + d^T Ac + s_2^T g_2 + r_2^T g_2 + d^T g_2 \\
&\quad - s_2^T As_1 - s_2^T e_1 + h_2^T \qquad (2)
\end{aligned}
$$

Remark 2: Let $i \in \{1, 2\}$. Then, $\{e_i, s_i, r_i, f_i\}$ and $\{c, d^T\}$ give the same property because of the hash function H_1. We use the idea detailed in [4] for the computation of shared secret keys. In other words, for $i \in [m]$ $\|e_{2,i}\| < \sqrt{n}\sigma = \beta$ and $\|r_i\| < \sqrt{n}\sigma = \beta$, then, we have the following:

$$
\begin{aligned}
||e_2^T r|| &= ||\sum_{i=1}^{m} e_{2,i} r_i|| \leq \sum_{i=1}^{m} ||e_{2,i} r_i|| \\
&\leq \sum_{i=1}^{m} n||e_{2,i}||||r_i|| \leq mn\beta^2 \\
&\Rightarrow ||e_2^T r|| \approx mn\beta^2
\end{aligned}
$$

By combining Remark 2, Definition 5, and Equation (2) then,

$$
\begin{aligned}
k_1 - k_2 = &(\overbrace{e_2^T r_1}^{mn\beta^2} + \overbrace{e_2^T c}^{mn\beta^2} + \overbrace{f_2^T s_1}^{mn\beta^2} + \overbrace{f_2^T r_1}^{mn\beta^2} + \overbrace{f_2^T c}^{mn\beta^2} + \overbrace{g_1^T s_1}^{mn\beta^2} \\
&+ \overbrace{g_1^T r_1}^{mn\beta^2} + \overbrace{g_1^T c}^{mn\beta^2} + \overbrace{h_1}^{\beta}) - (\overbrace{r_2^T e_1}^{mn\beta^2} + \overbrace{d^T e_1}^{mn\beta^2} + \overbrace{s_2^T f_1}^{mn\beta^2} \\
&+ \overbrace{r_2^T f_1}^{mn\beta^2} + \overbrace{d^T f_1}^{mn\beta^2} + \overbrace{s_2^T g_2}^{mn\beta^2} + \overbrace{r_2^T g_2}^{mn\beta^2} + \overbrace{d^T g_2}^{mn\beta^2} + \overbrace{h_2^T}^{\beta}) \\
&\Rightarrow \|k_1 - k_2\| \leq 16mn\beta^2 + 2\beta \qquad (3)
\end{aligned}
$$

In conclusion, if $\|k_1 - k_2\| \leq 16mn\beta^2 + 2\beta$, then the probability of having the same shared secret key is at most $O(n2^{-\lambda})$ in the proposed AKE scheme.

B. SECURITY ANALYSIS

We provide the security analysis in the BR model with wPFS in the ROM. To present the security analysis of proposed scheme, we construct a hybrid BR model based on [7]–[9]. This model aims to show that it provides wPFS in the ROM. With the reusable key property ensured by the Bi-P approach, any adversary cannot obtain any information about the static secret keys in each execution of the proposed AKE scheme. In the two-pass AKE schemes, if a passive adversary controls the communication, then previous session keys are protected with wPFS. To provide wPFS in the proposed AKE scheme, we present the security proofs and examine possible cases for the session key received from the test session in the BR security model.

- The owner of the test session sid = (II, 1, A*, B*, x_1^*, x_2^{T*}) is the initiator (1).
  - TYPE **ADV**$_1$: For sid, x_2^{T*} is generated with the answer(II, 2, B*, A*, x_1^*) query.
  - TYPE **ADV**$_2$: For sid, x_2^{T*} isn't generated with the answer(II, 2, B*, A*, x_1^*) query.
- The owner of the test session sid = (II, 2, B*, A*, x_1^*, x_2^{T*}) is the responder (2).
  - TYPE **ADV**$_3$: For sid, x_1^* isn't generated with start(II, 1, A*, B*) query.
  - TYPE **ADV**$_4$: For sid, x_1^* is generated with the start(II, 1, A*, B*) query. In addition, A* either completes the session by using x_2^{T*} or cannot.
  - TYPE **ADV**$_5$: For sid, x_1^* is generated with the start(II, 1, A*, B*) query. In addition, A* completes the session by using another $x_2^{T'}$ such that $x_2^{T'} \neq x_2^{T*}$.

In Figure 2, the main components of the security model for the proposed AKE scheme is presented.

Theorem 1 provides the main structure of the security proof.

Theorem 1: Let n, $\lambda = O(n)$, $m \geq 2$ be the lattice-dimension, the security parameter, and the constant, respectively. Let $\sqrt{n}\sigma = \beta$, $q = O(2^{\lambda} mn\beta^2)$, and $\|k_1 - k_2\| \leq 16mn\beta^2 + 2\beta$. Then, the hardness assumption of the Bi-GISIS, given in Corollary 1, is satisfied. Moreover, the proposed AKE scheme with reusable key property is secure in the BR security model in the ROM.

The detailed proof of Theorem 1 will be explained in Section III-B1 and Section III-B2.

1) THE OWNER OF TEST SESSION SID IS THE INITIATOR

We start with the initiator. Let the owner of sid* = (II, 1, A*, B*, x_1^*, x_2^{T*}) be the initiator.

a: TYPE ADV$_1$

In this type, by considering the fresh session definition (Definition 8), an adversary **ADV** should provide the following information for wPFS:

- **ADV** can obtain the static secret key values of both parties by using the staticKR query.
- **ADV** can monitor the communication between the parties.

Lemma 5 presents the security proof of ADV$_1$.

*Lemma 5: Let **ADV** be an adversary of type ADV$_1$. The hardness assumption of the Bi-GISIS is satisfied with the parameters $\lambda = O(n)$, $\sqrt{n}\sigma = \beta$, $q = O(2^{\lambda} mn\beta^2)$, and $\|k_1 - k_2\| \leq 16mn\beta^2 + 2\beta$. Then, the advantage of **ADV** is negligible in the ROM.*

Proof: The proof of Lemma 5 is discussed by considering all choices called Game$_{1,i}$, where $i \in \{0, 1, \ldots, 5\}$. □

Game$_{1,0}$:

- Simulator (S) chooses $A \xleftarrow{r} \Re_q^{m\times m}$. By using A, static public keys are honestly generated.
- S expects that **ADV** chooses sid* = (II, 1, A*, B*, x_1^*, x_2^{T*}) as a test session. For this session:
  - A*, B* $\xleftarrow{r}$ $\{P_1, \ldots, P_N\}$.

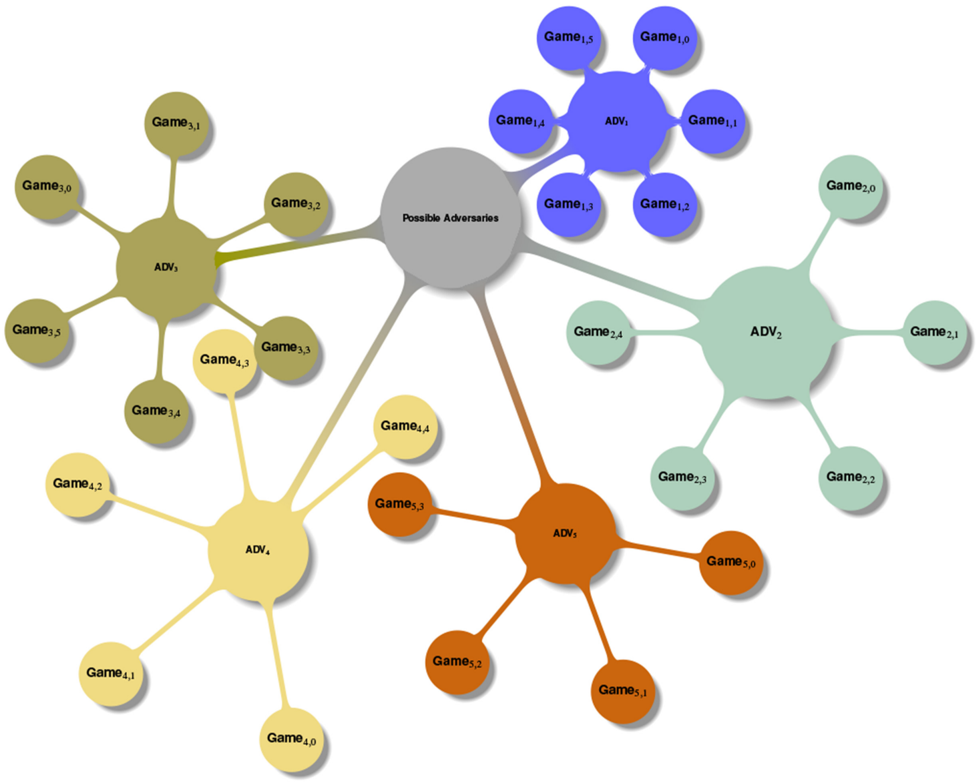

FIGURE 2. The BR Security Model for the Proposed Scheme.

- $s_1^*, s_2^{T*} \xleftarrow{r} \{1, \ldots, t\}$.
- x_1^* is generated from the s_1^*-th session of A* with the start(II, 1, A*, B*) query.
- x_2^{T*} is generated from the s_2^{T*}-th session of B* with the answer(II, 2, B*, A*, x_1^*) query.

- S works with **ADV** and impersonates the oracle in the following way:
  1. Hash Functions H_1 and H_2: Let f be a query for random oracles, h be the corresponding response given to the random oracles, L_1 and L_2 be the list tables of (f, h) pair.
     * If the query f is performed to H_1, then S checks to see whether there is a (f, h) pair in the table L_1.
       · If there is a pair, then it returns h for **ADV**.
       · Otherwise, S chooses uniformly random $h \xleftarrow{r} D_{\Re^m,\sigma}$ and returns h for **ADV**. Then, a pair (f, h) is stored in the table L_1.
     * If the query f is performed to H_2, then S checks to see whether there is a (f, h) pair in the table L_2.
       · If there is a pair, then it returns h for **ADV**.
       · Otherwise, S chooses uniformly random $h \xleftarrow{r} D_{\Re^m,\sigma}$ and returns h for **ADV**. Then, a pair (f, h) is stored in the table L_2.
  2. For the start, the answer and the complete queries, we give the details by using games.
  3. When the query sessionKR is performed, then **ADV** returns sid queried in sessionKR.
  4. When the query staticKR is performed, then **ADV** returns the static secret key of the input of queried in staticKR.
  5. test(sid): Let the test session sid = (II, 1, A, B, x_1, x_2^T) be queried by **ADV**.
     * S cancels the execution in the following cases:
       1) If (A, B) $\neq$ (A*, B*) or
       2) If x_1 isn't generated by the s_1^*-th session A* or
       3) If x_2^T isn't generated by the s_2^{T*}-th session B*.
     * Otherwise, S chooses $\wp \xleftarrow{r} \{0, 1\}$. Two cases occur.
       · If $\wp = 0$, then the output of S is shared with random secret key $sk_1' \xleftarrow{r} \{0, 1\}^\lambda$.
       · Otherwise, the output of S is sk_1, which is the real session key of sid.

The Analysis of Game$_{1,0}$: The probability that S can cancel the execution in Game$_{1,0}$ is $\frac{1}{t^2N^2}$.

Proof: S randomly chooses A*,B*, s_1^*, s_2^{T*} as follows. Let A*, B*$\xleftarrow{r}$ $\{P_1, \ldots, P_N\}$. A* and B* are randomly selected from N elements. The right session part is one of N possible elements.

Let $s_1^*, s_2^{T*} \xleftarrow{r} \{1, \ldots, t\}$. s_1^* and s_2^{T*} are randomly selected from t elements. The right party is one of t possible elements. All of these choices are independent events for **ADV**. Therefore, the probability of canceling the execution is computed as $\frac{1}{N} \cdot \frac{1}{N} \cdot \frac{1}{t} \cdot \frac{1}{t}$. □

Game$_{1,1}$: The oracles described in Game$_{1,0}$ are impersonated by S, except for the complete.

- When the complete(II, 1, A, B, x_1, x_2^T) is queried over S,
  - S sets $sk_1 = sk_2$, when the following conditions completely satisfied.
    1) (A, B) = (A*, B*).
    2) The session is the s_1^*-th session of A.
    3) x_2^{T*} is generated by the session of s_2^{T*}-th of B.
  - Otherwise, S impersonates the oracle given in Game$_{1,0}$.

The Analysis of Game$_{1,1}$: The probability of distinguishing the difference between Game$_{1,0}$ and Game$_{1,1}$ is negligible for all **ADV**s.

Proof: There is only one operation ($sk_1 = sk_2$) in Game$_{1,1}$. Since this operation does not affect the integrity of the scheme, there is no difference between Game$_{1,0}$ and Game$_{1,1}$ in terms of parameters and queries. □

Game$_{1,2}$: The oracles described in Game$_{1,1}$ are impersonated by S, except for the start.

- When the start(II, 1, A, B) is queried over S,
  - $x_1 \xleftarrow{r} \Re_q^m$ is selected instead of $x_1 = Ar_1 + f_1$ by S, when the following conditions are completely satisfied.
    1) (A, B) = (A*, B*).
    2) The session is the s_1^*-th session of A.

The Analysis of Game$_{1,2}$: As long as the hardness assumption of the Bi-GISIS is satisfied, then the probability of distinguishing the difference between Game$_{1,1}$ and Game$_{1,2}$ is negligible for all **ADV**s.

Proof: According to the hardness assumption of the DBi-GISIS problem, there is no polynomial time algorithm except for negligible probability that distinguishes between $(A, x_1 = Ar_1 + f_1, x_2^T)$ sampled in the Bi-GISIS and $(A, x_1' \xleftarrow{r} \Re_q^m, x_2'^T)$ sampled uniformly at random. Under the hardness assumption of the Bi-GISIS, we conclude that Game$_{1,2}$ is computationally indistinguishable from Game$_{1,1}$ except for negligible probability. □

Game$_{1,3}$: The oracles described in Game$_{1,1}$ are impersonated by S, except for the complete.

- When the complete(II, 1, A, B, x_1, x_2^T) is queried over S,
  - $k_1 \xleftarrow{r} \Re_q^m$ is randomly selected by S, when the following conditions are completely satisfied.
    1) (A, B) = (A*, B*).
    2) The session is the s_1^*-th session of A.
    3) x_2^T isn't generated by the session of s_2^{T*}-th of B.

The Analysis of Game$_{1,3}$: As long as the hardness assumption of the Bi-GISIS is satisfied, then the probability of distinguishing the difference between Game$_{1,2}$ and Game$_{1,3}$ is negligible for all **ADV**s.

Proof: In this game, since x_2^T isn't generated with the answer query by the session s_2^T-th of B, there is no information about the distribution of x_2^T. However, in the Bi-P approach the distribution of $\overleftrightarrow{x_2}^T$ obtained independently from x_2^T is known. This distribution, which is given in Corollary 3, is statistically close to uniform distribution. By rewriting the key material of A, we obtain Equation (4).

$$\begin{aligned} k_1 &= (p_2^T + \overleftrightarrow{x_2}^T)(s_1 + r_1 + c) - (p_2^T s_1) + h_1 \\ &= \overleftrightarrow{x_2}^T(s_1 + r_1 + c) + p_2^T(r_1 + c) + h_1 \end{aligned} \tag{4}$$

As long as $(s_1 + r_1 + c)$ and h_1 are sampled from $D_{\Re^m,\sigma}$ and $\overleftrightarrow{x_2}^T$ is uniform in $\Re_q^m$, then $\overleftrightarrow{x_2}^T(s_1 + r_1 + c) + h_1$ cannot be distinguished from uniformly random sample in $\Re_q^m$ due to the hardness assumption of the Bi-GISIS. Therefore, Game$_{1,2}$, in which k_1 is generated by using the Bi-GISIS sample, is computationally indistinguishable from Game$_{1,3}$, in which k_1 is generated by using random sample, except for negligible probability. □

Game$_{1,4}$: S chooses $w_1 \xleftarrow{r} \Re_q^m$ and computes $k_1 = w_1 + p_2^T(r_1 + c)$.

The Analysis of Game$_{1,4}$: As long as the hardness assumption of the Bi-GISIS is satisfied, then the probability of distinguishing the difference between Game$_{1,2}$ and Game$_{1,4}$ is negligible for all **ADV**s.

By using the same idea given in the analysis of Game$_{1,2}$, as long as $w_1 \xleftarrow{r} \Re_q^m$, then k_1 is uniformly at random over $\Re_q^m$. Thus, Game$_{1,4}$ is computationally indistinguishable from Game$_{1,2}$ except for negligible probability.

Game$_{1,5}$: The oracles described in Game$_{1,3}$ are impersonated by S, except for the answer.

- When the answer(II, 2, B, A, x_1) is queried over S,
  - $x_2^T, k_2 \xleftarrow{r} \Re_q^m$ are randomly selected and x_2^T is sent to the other party by S, when the following conditions are completely satisfied.
    1) (A, B) = (A*, B*).
    2) The session is the s_2^{T*}-th session of B*.
    3) x_1 is generated by the session of s_1^*-th of A*.
  - Otherwise, S impersonated the answer given in Game$_{1,3}$.

The Analysis of Game$_{1,5}$: As long as the hardness assumption of the Bi-GISIS is satisfied, then the probability of distinguishing the difference between Game$_{1,3}$ and Game$_{1,5}$ is negligible for all **ADV**s.

Proof: By rewriting $k_2 = (s_2^T + r_2^T + d^T)(p_1 + \overleftrightarrow{x_1}) - (s_2^T p_1) + h_2^T$, we obtain $k_2 = (s_2^T + r_2^T + d^T)(\overleftrightarrow{x_1}) + (s_2^T + d^T)p_1 + h_2^T$. By using the same proof idea given in the analysis of Game$_{1,3}$, we conclude that the probability of distinguishing the difference between Game$_{1,3}$ and Game$_{1,5}$ is negligible. □

-

b: TYPE ADV$_2$

In this type, the test session doesn't have a matching session. Therefore, wPFS is not provided for ADV$_2$. Lemma 6 presents the security proof of ADV$_2$.

*Lemma 6: Let **ADV** be an adversary whose type is ADV_2. The hardness assumption of the Bi-GISIS is satisfied with the parameters $\lambda = O(n)$, $\sqrt{n}\sigma = \beta$, $q = O(2^{\lambda} mn\beta^2)$, and $\|k_1 - k_2\| \leq 16mn\beta^2 + 2\beta$. Then, the advantage of **ADV** is negligible in the ROM.*

Proof: The proof of Lemma 6 is explained with for all $\mathrm{Game}_{2,i}$, where $i \in \{0, 1, \ldots, 4\}$. □

$\mathrm{Game}_{2,0}$:

- S chooses $A \xleftarrow{r} \Re_q^{m\times m}$. By using A, static public keys are honestly generated.
- S expects that **ADV** chooses sid* = (II, 1, A*, B*, x_1^*, x_2^{T*}) as a test session. For this session:
  - A*, B*$\xleftarrow{r} \{P_1, \ldots, P_N\}$.
  - $s_1^* \xleftarrow{r} \{1, \ldots, t\}$.
  - x_1^* is generated from the s_1^*-th session of A* with the start(II, 1, A*, B*) query.
- S works with **ADV** and impersonates the oracles given in $\mathrm{Game}_{1,0}$ except for test query.
  1. test(sid): Let the test session sid = (II, 1, A, B, x_1, x_2^T) be queried by **ADV**.
     - ∗ S cancels the execution in the following cases.
       1) If (A, B) ≠ (A*, B*) or
       2) If x_1 isn't generated by the s_1^*-th session A*.
     - ∗ Otherwise, S chooses $\wp \xleftarrow{r} \{0, 1\}$. Two cases occur:
       - · If $\wp = 0$, then the output of S is shared with random secret key $sk_1' \xleftarrow{r} \{0, 1\}^{\lambda}$.
       - · Otherwise, the output of S is sk_1, which is the real session key of sid.

The Analysis of $\mathrm{Game}_{2,0}$: The probability that S can cancel the execution in $\mathrm{Game}_{2,0}$ is $\frac{1}{tN^2}$.

Proof: In this game, S randomly chooses A*,B*, s_1^*. By using the same idea given in the analysis of $\mathrm{Game}_{1,0}$, we conclude that the probability of cancelling the execution is computed as $\frac{1}{N} \cdot \frac{1}{N} \cdot \frac{1}{t}$. □

$\mathrm{Game}_{2,1}$: The oracles described in $\mathrm{Game}_{2,0}$ are impersonated by S, except for the answer.

- When the answer(II, 2, B, A, x_1) is queried over S,
  - $k_2 = (s_1^T + r_2^T + d^T)(\overleftrightarrow{x_1}) + (r_2^T + d^T)p_1 + h_2^T$ is computed by S, when the following conditions are completely satisfied.
    1) B = B*.
    2) The session is the s_2^*-th session of B*.
  - Otherwise, S impersonates the oracle the answer given in $\mathrm{Game}_{3,1}$, which is described in Section III-B2.

The Analysis of $\mathrm{Game}_{2,1}$: The probability of distinguishing the difference between $\mathrm{Game}_{2,0}$ and $\mathrm{Game}_{2,1}$ is negligible for all **ADV**s.

Proof: In this game, S knows all the static secret keys (s_1, s_2^T). The correctness of scheme is ensured in S with $k_2 = (s_1^T + r_2^T + d^T)(\overleftrightarrow{x_1}) + (r_2^T + d^T)p_1 + h_2^T$, which we obtained by rewriting k_2. Then, $\mathrm{Game}_{2,0}$, where k_2 is generated by using s_2^T, is computationally indistinguishable from $\mathrm{Game}_{2,1}$, where k_2 is generated by using s_1^T, except for negligible probability. □

$\mathrm{Game}_{2,2}$: The oracles described in $\mathrm{Game}_{2,1}$ are imitated by S, except for the start and the complete.

- When the complete(II, 1, A, B, x_1, x_2^T) is queried over S,
  - $k_1 = \overleftrightarrow{x_2}^T(s_2+r_1+c)+p_2^T(r_1+c)+h_1$ is computed by S, when the following conditions are completely satisfied.
    1) A = B*.
    2) The session is the s_2^*-th session of B*.
  - Otherwise, S impersonates the oracle complete given in $\mathrm{Game}_{2,1}$.

The Analysis of $\mathrm{Game}_{2,2}$: The probability of distinguishing the difference between $\mathrm{Game}_{2,1}$ and $\mathrm{Game}_{2,2}$ is negligible for all **ADV**s.

Proof: In this game, S knows all the static secret keys (s_1, s_2^T). By using the same idea given in the analysis of $\mathrm{Game}_{2,1}$, we conclude that $\mathrm{Game}_{2,2}$, in which k_1 is generated by using s_2, is computationally indistinguishable from $\mathrm{Game}_{2,1}$, in which k_1 is generated by using s_1, except for negligible probability. □

$\mathrm{Game}_{2,3}$: S impersonates the oracles given in $\mathrm{Game}_{2,2}$ except for the query to replace the static secret key of B*, which is p_2^{T*}, with the uniformly random sample, which is $u_2^T \xleftarrow{r} \Re_q^m$.

The Analysis of $\mathrm{Game}_{2,3}$: As long as the hardness assumption of the Bi-GISIS is satisfied, then the probability of distinguishing the difference between $\mathrm{Game}_{2,2}$ and $\mathrm{Game}_{2,3}$ is negligible for all **ADV**s.

Proof: As long as the hardness assumption of the Bi-GISIS is satisfied, p_2^{T*} shouldn't be distinguished from $u_2^T \xleftarrow{r} \Re_q^m$. There doesn't exist any polynomial time algorithm that distinguishes between $\mathrm{Game}_{2,2}$, where p_2^{T*} is an example of Bi-GISIS, and $\mathrm{Game}_{2,3}$, where p_2^{T*} is uniformly random sample. □

$\mathrm{Game}_{2,4}$: The oracles described in $\mathrm{Game}_{2,3}$ are impersonated by S, except for the complete.

- When the complete(II, 2, B, A, x_1) is queried over S,
  - $k_1 \xleftarrow{r} \Re_q^m$ is selected by S, when the following conditions are completely satisfied.
    1) (A, B) = (A*, B*).
    2) The session is the s_1^*-th session of A*.
    3) x_2^{T*} isn't generated by using the answer(II, 2, B*, A*, x_1).
  - Otherwise, S impersonates the oracle complete given in $\mathrm{Game}_{2,3}$.

The Analysis of $\mathrm{Game}_{2,4}$: As long as the hardness assumption of the Bi-GISIS is satisfied, then the probability of distinguishing the difference between $\mathrm{Game}_{2,3}$ and $\mathrm{Game}_{2,4}$ is negligible for all **ADV**s.

Proof: In the calculation of $k_1 = \overleftrightarrow{x_2}^T(s_2 + r_1 + c) + p_2^{T*}(r_1+c)+h_1$, since p_2^{T*}, $h_1 \xleftarrow{r} \Re_q^m$ and $r_1+c \xleftarrow{r} D_{\Re^m,\sigma}$, then $p_2^{T*}(r_1+c)+h_1$ is a Bi-GISIS sample. Hence, $\mathrm{Game}_{2,3}$, where k_1 is calculated by using p_2^{T*}, is computationally indistinguishable from $Game_{2,4}$, where k_1 is selected from uniformly random samples, except for negligible probability. □

2) THE OWNER OF TEST SESSION SID IS THE RESPONDER

Let the owner of sid* = (II, 2, B*, A*, x_1^*, x_2^{T*}) be the responder.

a: TYPE ADV_3

In this type, the test session doesn't have a matching session. Therefore, wPFS is not provided for ADV_3. Lemma 7 presents the security proof of ADV_3.

*Lemma 7: Let **ADV** be an adversary whose type is ADV_3. The hardness assumption of the Bi-GISIS is satisfied with $\lambda = O(n)$, $\sqrt{n}\sigma = \beta$, $q = O(2^{\lambda} mn\beta^2)$, and $\|k_1 - k_2\| \leq 16mn\beta^2 + 2\beta$. Then, the advantage of **ADV** is negligible in the ROM.*

Proof: The proof of Lemma 7 is given with for all $Game_{3,i}$, where $i \in \{0, 1, \ldots, 5\}$. □

$Game_{3,0}$:

- S chooses $A \xleftarrow{r} \mathfrak{R}_q^{m\times m}$. By using A, static public keys are honestly generated.
- S expects that **ADV** chooses sid* = (II, 2, B*, A*, x_1^*, x_2^{T*}) as a test session. For this session:
  - A*, B*$\xleftarrow{r} \{P_1, \ldots, P_N\}$.
  - $s_2^{T*} \xleftarrow{r} \{1, \ldots, t\}$.
  - x_2^{T*} is generated from the s_2^{T*}-th session of B* with the answer(II, 2, B*, A*, x_1^*) query.
- S works with **ADV** and impersonates the oracles given in $Game_{1,0}$ except for test query.
  1. test(sid): Let the test session sid = (II, 2, B, A, x_1, x_2^T) be queried by **ADV**.
     - ∗ S cancels the execution in the following cases.
       1) If (A, B) ≠ (A*, B*) or
       2) If x_2^T isn't generated by the s_2^{T*}-th session B*.
     - ∗ Otherwise, S chooses $\wp \xleftarrow{r} \{0, 1\}$. Two cases occur.:
       - · If $\wp = 0$, then the output of S is shared with random secret key $sk_1' \xleftarrow{r} \{0, 1\}^{\lambda}$.
       - · Otherwise, the output of S is sk_1, which is the real session key of sid.

The Analysis of $Game_{3,0}$: The probability that S can cancel the execution in $Game_{3,0}$ is $\frac{1}{tN^2}$.

Proof: In this game, S randomly chooses A*, B*, s_2^{T*}. By using the same idea given in the analysis of $Game_{1,0}$, we conclude that the probability of cancelling the execution is calculated as $\frac{1}{N} \cdot \frac{1}{N} \cdot \frac{1}{t}$. □

$Game_{3,1}$: The oracles, which is described in $Game_{3,0}$ are impersonated by S, except for the start and the complete.

- When the complete(II, 1, A, B, x_1, x_2^T) is queried over S,
  - $k_1 = \overleftrightarrow{x_2}^T(s_2+r_1+c)+p_2^T(r_1+c)+h_1$ is computes by S, when the following conditions are completely satisfied.
    1) A=A*.
    2) The session is the s_1^*-th session of A*.
  - Otherwise, S impersonates the oracle complete given in $Game_{3,0}$.

The Analysis of $Game_{3,1}$: The probability of distinguishing the difference between $Game_{3,0}$ and $Game_{3,1}$ is negligible for all **ADV**s.

Proof: We use the same idea given in the analysis of $Game_{2,2}$. □

$Game_{3,2}$: The oracles described in $Game_{3,1}$ is impersonated by S, except for the answer.

- When the answer(II, 2, B, A, x_1) is queried over S,
  - $k_2 = (s_1^T + r_2^T + d^T)(\overleftrightarrow{x_1}) + p_1(r_2^T + d^T) + h_2^T$ is computed by S, when the following conditions are completely satisfied.
    1) B = A*.
    2) The session is the s_1^*-th session of A*.
  - Otherwise, S impersonates the oracle answer given in $Game_{3,1}$.

The Analysis of $Game_{3,2}$: The probability of distinguishing the difference between $Game_{3,1}$ and $Game_{3,2}$ is negligible for all **ADV**s.

Proof: We use the same idea given in the analysis of $Game_{2,1}$. □

$Game_{3,3}$: S impersonates the oracles given in $Game_{3,2}$ except for the query to replace the static secret key of A*, which is p_1^*, with the uniformly random sample, which is $u_1 \xleftarrow{r} \mathfrak{R}_q^m$.

The Analysis of $Game_{3,3}$: As long as the hardness assumption of the Bi-GISIS is satisfied, then the probability of distinguishing the difference between $Game_{3,2}$ and $Game_{3,3}$ is negligible for all **ADV**s.

Proof: As long as the hardness assumption of the Bi-GISIS is satisfied, p_1^* shouldn't be distinguished from $u_1 \xleftarrow{r} \mathfrak{R}_q^m$. In other words, there doesn't exist any polynomial time algorithm that distinguishes between $Game_{3,2}$, where p_1^* is an example of the Bi-GISIS, and $Game_{3,3}$, where p_1^* is uniformly random sample. □

$Game_{3,4}$: The oracles described in $Game_{3,3}$ is impersonated by S, except for the answer.

- When the answer(II, 2, B, A, x_1) is queried over S,
  - $k_2 \xleftarrow{r} \mathfrak{R}_q^m$ is selected by S, when the following conditions are completely satisfied.
    1) (A, B) = (A*, B*).
    2) The session is the s_2^{T*}-th session of B*.
    3) x_1 isn't generated by using the start(II, 1, A*, B*).
  - Otherwise, S impersonates the oracle answer given in $Game_{3,3}$.

The Analysis of $Game_{3,4}$: As long as the hardness assumption of the Bi-GISIS is satisfied, then the probability of distinguishing the difference between $Game_{3,3}$ and $Game_{3,4}$ is negligible for all **ADV**s.

Proof: In the calculation of $k_2 = (s_1^T + r_2^T + d^T)(\overleftrightarrow{x_1}) + p_1^*(r_2^T + d^T) + h_2^T$, since $p_1^* \xleftarrow{r} \mathfrak{R}_q^m$ and $(r_2^T + d^T), h_2^T \xleftarrow{r} D_{\mathfrak{R}^m,\sigma}$, then $(r_2^T + d^T)p_1^* + h_2^T$ is a Bi-GISIS sample.

Hence, $\text{Game}_{3,3}$, where k_2 is calculated by using p_1^*, is computationally indistinguishable from the $\text{Game}_{3,4}$, where k_2 is selected from uniformly random samples, except for negligible probability. □

$\text{Game}_{3,5}$: S chooses $w_2^T \xleftarrow{r} \mathfrak{R}_q^m$ and computes $k_2 = w_2^T + (s_1^T + r_2^T + d^T)(\overleftrightarrow{x_1})$. As long as the hardness assumption of the Bi-GISIS is satisfied, then for all **ADV**s. the probability distinguishing $\text{Game}_{3,4}$ and $\text{Game}_{3,5}$ is negligible.

The Analysis of $\text{Game}_{3,5}$: As long as $w_2^T \xleftarrow{r} \mathfrak{R}_q^m$, then k_2 be uniformly at random over $\mathfrak{R}_q^m$. So, for all **ADV**s. the probability distinguishing the difference between $\text{Game}_{3,4}$ and $\text{Game}_{3,5}$ is negligible.

b: TYPE ADV_4

In this type to achieve wPFS by considering the fresh session definition (Definition 8), **ADV** should satisfy the following properties:

- **ADV** can obtain static secret key values of both parties by using the staticKR query.
- **ADV** can monitor the communication between the parties.

Lemma 8 presents the security proof of ADV_4.

*Lemma 8: Let **ADV** be an adversary whose type is ADV_4. The hardness assumption of the Bi-GISIS is satisfied with $\lambda = O(n)$, $\sqrt{n}\sigma = \beta$, $q = O(2^\lambda mn\beta^2)$, and $\|k_1 - k_2\| \leq 16mn\beta^2 + 2\beta$. Then, the advantage of **ADV** is negligible in the ROM.*

Proof: The proof of Lemma 8 is explained with for all $\text{Game}_{4,i}$, where $i \in \{0, 1, \ldots, 4\}$. □

$\text{Game}_{4,0}$:

- S chooses $A \xleftarrow{r} \mathfrak{R}_q^{m \times m}$. By using A, static public keys are honestly generated.
- S expects that **ADV** chooses sid* = (II, 2, B*, A*, x_1^*, x_2^T*) as a test session. For this session:
  - A*, B*$\xleftarrow{r}$ $\{P_1, \ldots, P_N\}$.
  - s_1^*, s_2^T* $\xleftarrow{r}$ $\{1, \ldots, t\}$.
  - x_1^* is generated from the s_1^*-th session of A* with the start(II, 1, A*, B*) query.
  - x_2^T* is generated from the s_2^T*-th session of B* with the answer(II, 2, B*, A*, x_1^*) query.
- S works with **ADV** and impersonates the oracles given in $\text{Game}_{1,0}$ except for test query.
  1. test(sid): Let the test session sid = (II, 2, B, A, x_1, x_2^T) be queried by **ADV**.
     * S cancels the execution in the following cases.
       1) If (A, B) $\neq$ (A*, B*) or
       2) If x_1 isn't generated by the s_1^*-th session A* or
       3) If x_2^T isn't generated by the s_2^T*-th session B*.
     * Otherwise, S chooses $\wp \xleftarrow{r} \{0, 1\}$. Two cases occur:
       · If $\wp = 0$, then the output of S is shared with random secret key $sk_1' \xleftarrow{r} \{0, 1\}^\lambda$.
       · Otherwise, the output S is sk_1, which is the real session key of sid.

The Analysis of $\text{Game}_{4,0}$: The probability that S can cancel the execution in $\text{Game}_{4,0}$ is $\frac{1}{t^2N^2}$. *Proof:* S randomly chooses A*, B*, s_1^*, s_2^T* as follows. By using the same idea given in the analysis of $\text{Game}_{1,0}$, we conclude that the probability of cancelling the execution is computed as $\frac{1}{N} \cdot \frac{1}{N} \cdot \frac{1}{t} \cdot \frac{1}{t}$. □

$\text{Game}_{4,1}$: The oracles described in $\text{Game}_{4,0}$ are impersonated by S, except for the complete.

- When the complete(II, 1, A, B, x_1, x_2^T) is queried over S,
  - S sets $sk_1 = sk_2$, after the following conditions are completely satisfied.
    1) (A, B) = (A*, B*).
    2) The session is the s_1^*-th session of A*.
    3) x_2^T* is generated by the session of s_2^T*-th of B.
  - Otherwise, S impersonates the oracle complete given in $\text{Game}_{4,0}$.

The Analysis of $\text{Game}_{4,1}$: The probability of distinguishing the difference between $\text{Game}_{4,0}$ and $\text{Game}_{4,1}$ is negligible for all **ADV**s.

Proof: There is only one operation ($sk_1 = sk_2$) in $\text{Game}_{4,1}$. Since $\text{Game}_{4,1}$ does not deal with the integrity, there is no difference between $\text{Game}_{4,0}$ and $\text{Game}_{4,1}$ in terms of parameters and queries. □

$\text{Game}_{4,2}$: The oracles described in $\text{Game}_{4,1}$ are impersonated by S, except for the start.

- When the start(II, 1, A, B) is queried over S,
  - $x_1 \xleftarrow{r} \mathfrak{R}_q^m$ is selected instead of $x_1 = Ar_1 + f_1$ by S, when the following conditions are completely satisfied.
    1) (A, B) = (A*, B*).
    2) The session is the s_1^*-th session of A*.

The Analysis of $\text{Game}_{4,2}$: As long as the hardness assumption of the Bi-GISIS is satisfied, then the probability of distinguishing the difference between $\text{Game}_{4,1}$ and $\text{Game}_{4,2}$ is negligible for all **ADV**s.

Proof: We use the same idea given in the analysis of $\text{Game}_{1,2}$. □

$\text{Game}_{4,3}$: The oracles described in $\text{Game}_{4,2}$ are impersonated by S, except for the complete.

- When the complete(II, 1, A, B, x_1, x_2^T) is queried over S,
  - $k_1 \xleftarrow{r} \mathfrak{R}_q^m$ is randomly selected by S, when the following conditions are completely satisfied.
    1) (A, B) = (A*, B*).
    2) The session is the s_1^*-th session of A.
    3) x_2^T* isn't generated by the session of s_2^T*-th of B.

The Analysis of $\text{Game}_{4,3}$: As long as the hardness assumption of the Bi-GISIS is satisfied, then the probability of distinguishing the difference between $\text{Game}_{4,2}$ and $\text{Game}_{4,3}$ is negligible for all **ADV**s.

Proof: We use the same idea given in the analysis of $\text{Game}_{1,3}$. □

$\text{Game}_{4,4}$: The oracles described in $\text{Game}_{4,3}$ are impersonated by S, except for the answer.

- When the answer(II, 2, A, B, x_1) is queried over S,
  - $x_2^T, k_2 \xleftarrow{r} \Re_q^m$ are randomly selected and x_2^T is sent to the other party by S,when the following conditions are completely satisfied.
    1) (A, B) = (A*, B*).
    2) The session is the s_2^T*-th session of B*.
    3) x_1 is generated by the session of s_1^*-th of A*.
  - Otherwise, S impersonates the answer query given in Game$_{4,3}$.

The Analysis of Game$_{4,4}$: As long as the hardness assumption of the Bi-GISIS is satisfied, then the probability of distinguishing the difference between Game$_{4,3}$ and Game$_{4,4}$ is negligible for all **ADV**s.

Proof: We use the same idea given in the analysis of Game$_{1,5}$. □

c: TYPE ADV$_5$

In this type, the test session doesn't have a matching session. Therefore, wPFS is not provided for ADV$_5$. Lemma 9 presents the security proof of ADV$_5$.

*Lemma 9: Let **ADV** be an adversary whose type is ADV$_5$. The hardness assumption of the Bi-GISIS is satisfied with $\lambda = O(n)$, $\sqrt{n}\sigma = \beta$, $q = O(2^{\lambda} mn\beta^2)$, and $\|k_1 - k_2\| \leq 16mn\beta^2 + 2\beta$. Then, the advantage of **ADV** is negligible in the ROM.*

Proof: The proof of Lemma 9 is explained with for all Game$_{5,i}$, where $i \in \{0, 1, \dots, 3\}$. □

Game$_{5,0}$:

- S chooses $A \xleftarrow{r} \Re_q^{m\times m}$. By using A, static public keys are generated honestly.
- S expects that **ADV** chooses sid* = (II, 2, B*, A*, x_1^*, x_2^T*) as a test session. For this session:
  - A*, B*$\xleftarrow{r} \{P_1, \dots, P_N\}$.
  - $s_1^*, s_2^T* \xleftarrow{r} \{1, \dots, t\}$.
  - x_1^* is generated from the s_1^*-th session of A* with the start(II, 1, A*, B*) query.
  - x_2^T* is generated from the s_2^T*-th session of B* with the answer(II, 2, B*, A*, x_1^*) query.
- S works with **ADV** and impersonates the oracles given in Game$_{1,0}$ except for test query.
  1. test(sid): Let the test session sid = (II, 1, A*, B*, x_1^*, x_2^T*) be queried by **ADV**.
     ∗ S cancels the execution in the following cases.
       1) If (A, B) ≠ (A*, B*) or
       2) If x_1 isn't generated by the s_1^*-th session A* or
       3) If x_2^T isn't generated by the s_2^T*-th session B*.
     ∗ Otherwise, S chooses $\wp \xleftarrow{r} \{0, 1\}$. Two cases occur:
       · If $\wp = 0$, then the output of S is random shared secret key $sk_1' \xleftarrow{r} \{0, 1\}^{\lambda}$.
       · Otherwise, the output of S is sk_1, which is the real session key of sid.

The Analysis of Game$_{5,0}$: The probability that S can cancel the execution in Game$_{5,0}$ is $\frac{1}{t^2N^2}$.

Proof: In this game, S randomly chooses A*, B*, s_1^*, s_2^T*. By using the same idea given in the analysis of Game$_{1,0}$, we conclude that the probability of cancelling the execution is computed as $\frac{1}{N} \cdot \frac{1}{N} \cdot \frac{1}{t} \cdot \frac{1}{t}$. □

Game$_{5,1}$: The oracles described in Game$_{5,0}$ are impersonated by S, except for the complete.

- When the start(II, 1, A, B) is queried over S,
  - $x_1 \xleftarrow{r} \Re_q^m$ is selected instead of $x_1 = Ar_1 + f_1$ by S, when the following conditions are completely satisfied.
    1) (A, B) = (A*, B*).
    2) The session is the s_1^*-th session of A.
  - Otherwise, S impersonates the answer query given in Game$_{5,0}$.

The Analysis of Game$_{5,1}$: As long as the hardness assumption of the Bi-GISIS is satisfied, then the probability of distinguishing the difference between Game$_{5,1}$ and Game$_{5,0}$ is negligible for all **ADV**s.

Proof: We use the same idea given in the analysis of Game$_{1,2}$. □

Game$_{5,2}$: The oracles described in Game$_{5,1}$ are impersonated by S, except for the answer.

- When the complete(II, 1, A, B, x_1, x_2^T) is queried over S,
  - $k_1 \xleftarrow{r} \Re_q^m$ is randomly selected by S, when the following conditions are completely satisfied.
    1) (A, B) = (A*, B*).
    2) The session is the s_1^*-th session of A*.
    3) x_2^T* isn't generated by the session of s_2^T*-th of B*.

The Analysis of Game$_{5,2}$: As long as the hardness assumption of the Bi-GISIS is satisfied, then the probability of distinguishing the difference between Game$_{5,1}$ and Game$_{5,2}$ is negligible for all **ADV**s.

Proof: We use the same idea given in the analysis of Game$_{1,3}$. □

Game$_{5,3}$: The oracles described in Game$_{5,2}$ are impersonated by S, except for the answer.

- When the complete(II, 1, A, B, x_1, x_2^T) is queried over S,
  - $k_2 \xleftarrow{r} \Re_q^m$ is randomly selected and x_2^T is sent to the other party by S, when the following conditions are completely satisfied.
    1) (A, B) = (A*, B*).
    2) The session is the s_2^T*-th session of B*
  - Otherwise, S impersonates the complete query given in Game$_{1,2}$.

The Analysis of Game$_{5,3}$: As long as the hardness assumption of the Bi-GISIS is satisfied, then the probability of distinguishing the difference between Game$_{5,2}$ and Game$_{5,3}$ is negligible for all **ADV**s.

Proof: We use the same idea given in the analysis of Game$_{1,5}$. □

TABLE 1. A comparison for selected lattice-based KE/AKE schemes.

	Hardness Assumption	Authentication	Reusable Key	Number of Multiplications	Security Model	Number of Hash Functions	ROM
[1]	Bi-GISIS	×	×	MM:4	×	×	×
[8]	RLWE	E	×	PM:12	BR, wPFS	2	✓
[9]	LWE	I	×	MM:8	BR, wPFS	1	✓
[7]	RLWE	I	✓	PM:10	BR, wPFS	2	✓
Proposed AKE	Bi-GISIS	I	✓	MM:10	BR, wPFS	2	✓

E: Explicit, I: Implicit, PM: Polynomial Multiplication, MM: Matrix Multiplication

IV. COMPARISON

In Table 1, we compare the proposed scheme with the previous ones. This comparison summarizes the properties of the AKE schemes in terms of hardness assumption, security model, authentication concept, the number of required hash functions, the number of required core arithmetic operations such as multiplications and reusable key property.

The proposed AKE is a solution to the open problem defined in [4]. The security of the proposed scheme is based on the hardness of the Bi-GISIS problem. The reusable key property is added to the proposed AKE by using the bilateral pasteurization method. The comparison is presented by focusing the hardness assumption and reusable key property. The security of the proposed scheme depends on the hardness of the Bi-GISIS problem equivalent to the MLWE problem. By using the implicit authentication and ROM, it provides wPFS in the BR security model. As a result of the reusable key property, the number of matrix multiplications in the proposed scheme is higher than the others. There is a scheme with the reusable key property is given in [7]. Note that the hardness assumptions of these schemes are different and this causes different requirements.

Remark 3: Note that the scheme given in [9] and the proposed AKE cannot be fairly compared since their hardness assumptions are different. The number of matrix multiplications in the proposed scheme is higher than [9] since the reusable key property has a penalty: increasing the number of multiplications. With this property, the increased number of multiplications can be ignored since reusing the keys several executions gives much more benefits.

Remark 4: The main differences from [8] are the hardness assumption and the authentication property. Compared with [8], the proposed scheme offers an authentication without any additional structure. The proposed scheme provides an alternative to quantum-resistant AKE schemes by including the reusable key property.

V. CONCLUSION

In this paper, we construct a novel AKE scheme for the post-quantum world which is a solution to the future work of [4]. To provide authentication, we add implicit authentication steps for the Bi-GISIS based KE scheme given in [4]. In addition, we use the bilateral pasteurization method to achieve reusable key property. With the help of this, the same shared secret key becomes available for the multiple executions of the proposed scheme. We explain the security in the ROM under the BR security model to achieve wPFS. As a future work, our aim is to determine the set of parameters for any security level and then give the computational complexity analysis for efficient implementations. In addition, password authenticated key exchange (PAKE) with reusable keys will be studied.

APPENDIX

BELLARE-ROGAWAY SECURITY MODEL

In [7], BR security model [14] is adapted for two-pass authenticated key exchange scheme. In this version of BR model, an adversary can read, transform, insert and prevent messages over the network.

SESSION

A single execution of the scheme is called session. In the session, some parameters have special meanings.

- II: In the session of AKE, there are two parts.
- 1: Initiator.
- 2: Responder.
- M_A: The message, which is sent from A to B.
- M_B: The message, which is sent from B to A.
- N: Maximum honest user numbers in the AKE scheme.
- t: Maximum session numbers for every part in the AKE scheme.

In the two-pass AKE scheme, a session consists of the following stages:

1. The owner of the session is A, which activates the session.
    - The representation of the session is sid = (II, 1, A, B, M_A, M_B).
    - The message form that activates the session is (II, 1, A, B).
    - The message M_A is generated.

2. The owner of the session is B, which activates the session.
   - The representation of the session is sid = (II, 2, B, A, M_A, M_B).
   - The message form that activates the session is (II, 2, A, B).
   - If B receives the message M_A as (II, 2, B, A, M_A), then B takes the role of 2. The message M_B is generated to sending A.
   - Finally, B calculates its secret shared key by using the reconciliation function.
3. The session owner is A again.
   - When A receives the message M_B as (II, 1, A, B, M_A, M_B), calculates its secret shared key, which is the same as B's secret shared key, by using the reconciliation function.

ORACLE

There are six oracles that **ADV** has access to.

1. start(II, 1, A, B): **ADV** activates A as the initiator. The output of this oracle is message M_A.
2. answer(II, 2, B, A, M_A): By using M_A, **ADV** activates B as the responder. The output of this oracle is message M_B.
3. complete(II, 2, A, B, M_A, M_B): In order to complete the session whose activation is realized by using the start query, the message M_B is sent to A.
4. sessionKR(sid): If there is a session key of sid, then **ADV** returns this sid.
5. staticKR(A): The output of this oracle is A's static secret key.
6. test(sid): In the fresh session, this oracle is allowed to be used once to avoid some attacks. $\wp \rightarrow_r \{0, 1\}$ is chosen by **ADV**. Then, two cases occur.
   - If $\wp = 1$, then **ADV** returns the real session key of sid.
   - Otherwise, **ADV** returns the random session key.

ACKNOWLEDGMENT

The authors would like to express their gratitude to the anonymous reviewers for their invaluable suggestions in putting the present study into its final form.

REFERENCES

[1] C. Paar and J. Pelzl, "Public-key cryptosystems based on the discrete logarithm problem," in *Understanding Cryptography: A Textbook for Students and Practitioners*, 2nd ed. Berlin, Germany: Springer, 2009, pp. 205–208.

[2] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, Washington, DC, USA, Nov. 1994, pp. 124–134, doi: 10.1109/SFCS.1994.365700.

[3] C. Peikert, "Lattice cryptography for the Internet," in *PQCrypto* (Lecture Notes in Computer Science), vol. 8772, no. 4. 2014, pp. 197–219, doi: 10.1007/978-3-319-11659-4_12.

[4] Z. Jing, C. Gu, Z. Yu, P. Shi, and C. Gao, "Cryptanalysis of lattice-based key exchange on small integer solution problem and its improvement," *Cluster Comput.*, vol. 22, no. S1, pp. 1717–1727, Jan. 2019, doi: 10.1007/s10586-018-2293-x.

[5] C. D. de Saint Guilhem, M. Fischlin, and B. Warinschi, "Authentication in key-exchange: Definitions, relations and composition," Cryptol. ePrint Arch. (IACR), Tech. Rep. 2019/1203, 2019.

[6] C. Boyd, A. Mathuria, and D. Stebila, "Protocols for authentication and key establishment," in *Information Security and Cryptography*, 2nd ed. Berlin, Germany: Springer, 2020, pp. 1–52.

[7] J. Ding, P. Branco, and K. Schmitt, "Key exchange and authenticated key exchange with reusable keys based on RLWE assumption," Cryptol. ePrint Arch. (IACR), Tech. Rep. 2019/665, 2019.

[8] J. Zhang, Z. Zhang, J. Ding, M. Snook, Ö. Dagdelen, "Authenticated key exchange from ideal lattices," in *Advances in Cryptology-EUROCRYPT* (Lecture Notes in Computer Science), vol. 9057, E. Oswald and M. Fischlin, Eds. Berlin, Germany: Springer, 2015, pp. 719–751, doi: 10.1007/978-3-662-46803-6_24.

[9] L. Zhou and F. Lv, "A simple provably secure AKE from the LWE problem," *Math. Problems Eng.*, vol. 2017, Apr. 2017, Art. no. 1740572, doi: 10.1155/2017/1740572.

[10] A. Langlois and D. Stehlé, "Worst-case to average-case reductions for module lattices," *Des., Codes Cryptogr.*, vol. 75, no. 3, pp. 565–599, Jun. 2015, doi: 10.1007/s10623-014-9938-4.

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

[12] J. Ding, X. Gao, T. Takagi, and Y. Wang, "One sample ring-LWE with rounding and its application to key exchange," n *Applied Cryptography and Network Security* (Lecture Notes in Computer Science), vol. 11464, R. Deng, V. Gauthier-Umaña, M. Ochoa, and M. Yung, Eds. Cham, Switzerland: Springer, 2019, pp. 323–343, doi: 10.1007/978-3-030-21568-2_16.

[13] J. Ding, R. Saraswathy, S. Alsayigh, and C. Clough, "How to validate the secret of a ring learning with errors (RLWE) key," Cryptol. ePrint Arch. (IACR), Tech. Rep. 2018/081, 2018.

[14] M. Bellare and P. Rogaway, "Entity authentication and key distribution," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 773. Berlin, Germany: Springer, 1994, pp. 232–249, doi: 10.1007/3-540-48329-2_21.

SEDAT AKLEYLEK received the B.Sc. degree in mathematics majored in computer science from Ege University, Izmir, Turkey, in 2004, and the M.Sc. and Ph.D. degrees in cryptography from Middle East Technical University, Ankara, Turkey, in 2008 and 2010, respectively. He has been an Associate Professor with the Department of Computer Engineering, Ondokuz Mayıs University, Samsun, Turkey, since 2016. His research interests include in the areas of post-quantum cryptography, algorithms and complexity, and architectures for computations in finite fields.

KÜBRA SEYHAN received the B.Sc. degree in computer engineering from Karadeniz Technical University, Trabzon, Turkey, in 2016, and the M.Sc. degree in computer engineering from Ondokuz Mayıs University, Samsun, Turkey, in 2020. She is currently a Research Assistant with the Department of Computer Engineering, Ondokuz Mayıs University. Her research interest includes post-quantum cryptography and algorithms.