Two-party authenticated key exchange protocol using lattice-based cryptography

Xiaopeng Yang and Wenping Ma

Abstract

Authenticated key exchange (AKE) protocol is an important cryptographic primitive that assists communicating entities, who are communicating over an insecure network, to establish a shared session key to be used for protecting their subsequent communication. Lattice-based cryptographic primitives are believed to provide resilience against attacks from quantum computers. An efficient AKE protocol with smaller module over ideal lattices is constructed in this paper, which nicely inherits the design idea of the excellent high performance secure Diffie-Hellman protocol. Under the hard assumption of ring learning with errors (RLWE) hard assumption, the security of the proposed protocol is proved in the Bellare-Rogaway model, which achieves weak Perfect Forward Secrecy (wPFS) additionally.

Index Terms

Lattice-based Cryptography, Authenticated Key Exchange

I. Introduction

Key exchange (KE) is an elementary cryptographic original that permits any two parties to negotiate a session key over an open network. The key exchange protocols fall into two categories: The fist one is key exchange protocol without authentication; the other one is authenticated key exchange (AKE) protocol. For AKE, each party owns certain public information (e.g., a static public key), which is issued by a trusted

The authors are with the State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China(e-mail: xp_yang89xidian@126.com, wp_ma@mail.xidian.edu.cn)

third party, such as public key infrastructure (PKI), or certification authority, and the homologous secret information (e.g., a static secret key). During the execution of the agreement, each party firstly generates his ephemeral secret key and concomitant ephemeral public key, and exchanges the ephemeral public key. Then, each participant computes certain session state. Finally, each party derives a common session key by using a robust extractor. How to evaluate the security of a cryptographic protocol is an important study of cryptography. Bellare and Rogaway firstly proposed a security model of AKE called Bellare-Rogaway model [1], which is based on the indistinguishability between the real session key and any random key uniformly chosen from the same distribution. This model is the most widely used security model, which is robust enough for many practical applications. Constructing efficient AKE protocols is among the core content of research for cryptography. Especially, with the development of quantum computing technology, it is inspiring to design new alternatives which are recognized to have resistance to quantum attacks.

With the present development of quantum technologies, the computing power grows more powerful and brings new challenges for the traditional cryptosystem. To meet these challenges, lattices have emerged in recent years as a rich treasurehouse from which to construct varieties of cryptographic primitives. Especially, building efficient and practical AKE protocols from lattices is of great importance. Moreover, lattice-based cryptography has several fascinating features. From a security perspective, the best attacks for quantum adversaries on the potential problems require exponential time in the primary security parameter. In addition, strong average-case/worst-case security reductions support security proofs in lattice-based cryptography. Lattice-based cryptography computations should be greatly simple, fast and parallelizable in the name of efficiency. Most of lattice-based cryptographic constructions are based directly upon one of the two average-case problems that have been shown to enjoy worst-case hardness guarantees: the small integer solution (SIS) problem and learning with errors (LWE) problem.

A. Related work

To our best knowledge, there are six main papers which concentrate on building KE protocol from RLWE [2]–[7]. In 15th IACR international conference, Fujioka *et al.* proposed a universal construction of

AKE from key encapsulation mechanism (KEM), which is proven to be secure in the Canetti-Krawczyk plus secure model [2]. Ding *et al.* proposed a simple provably secure KE from LWE [3]. In order to eliminate the noises from RLWE, they use a signal function. Meanwhile, they give an multiparty KE protocol. Fujioka *et al.* constructed a post-quantum AKE from lattices [4]. Their design ideas derived from the construction of secrete sharing from KEMs. Zhang *et al.* proposed an AKE from ideal lattices [5]. After deeply digging into the properties of modular rounding function and the cross rounding function, Peikert proposed a simple reconciliation mechanism, and then constructed a passively secure KEM [6]. Using this KEM, he further constructed a provably secure AKE which may be an improvement on the current AKE from signatures. Bos proposed a KE protocol, and then extended it to the Transport Layer Security (TLS) protocol [7].

B. Theoretic thereunder and idealistic base

The HMQV protocol uses the commutativity of cyclic group (i.e., $(g^a)^b = g^{ab} = (g^b)^a$) successfully [8]. But the cryptographic algorithms based on LWE problem supports the "approximate" commutativity, which is different from the cryptographic algorithms based on the discrete logarithm. More specifically, let R_q be a polynomial ring, and let χ be a certain distribution over R_q. For a public parameter $\mathbf{a} \leftarrow_{\mathcal{R}} R_q$ that is chosen from R_q at random, party i and party j chooses $\mathbf{s}_i, \mathbf{e}_i \leftarrow_{\mathcal{R}} \chi$ and $\mathbf{s}_j, \mathbf{e}_j \leftarrow_{\mathcal{R}} \chi$, secretly and respectively. Then, party i and party j computes $\mathbf{b}_i = \mathbf{a} \cdot \mathbf{s}_i + \mathbf{e}_i$ and $\mathbf{b}_j = \mathbf{a} \cdot \mathbf{s}_j + \mathbf{e}_j$, respectively. Utilizing the secret vector $\mathbf{s}_i$ and $\mathbf{s}_j$ which respectively grasps, party i and party j computes $\mathbf{s}_i \cdot \mathbf{b}_j$ and $\mathbf{s}_j \cdot \mathbf{b}_i$ respectively, an approximate formula $\mathbf{s}_i \cdot \mathbf{b}_j = \mathbf{s}_i \cdot \mathbf{a} \cdot \mathbf{s}_j + \mathbf{s}_i \cdot \mathbf{e}_j \approx \mathbf{s}_j \cdot \mathbf{a} \cdot \mathbf{s}_i + \mathbf{s}_j \cdot \mathbf{e}_i = \mathbf{s}_j \cdot \mathbf{b}_i$ holds with an overwhelming probability. Thus, we obtain $\mathbf{s}_i \cdot \mathbf{b}_j - \mathbf{s}_j \cdot \mathbf{b}_i = \mathbf{s}_i \cdot \mathbf{e}_j - \mathbf{s}_j \cdot \mathbf{e}_i$. If the error size $\|\mathbf{s}_i \cdot \mathbf{e}_j - \mathbf{s}_j \cdot \mathbf{e}_i\|$ is within limits, then party i and party j can eliminate this noise to compute the shared secret vector $\mathbf{s}_i \cdot \mathbf{a} \cdot \mathbf{s}_j$. Since this shared secret vector only involves the secret vectors $\mathbf{s}_i$ and $\mathbf{s}_j$ mastered by party i and party j respectively, only party i and party j can obtain the shared secret vector. The above mentioned property offers the possibility of building key exchange protocols from lattices.

C. Cryptanalysis of AKE of Zhang et al

We review the characteristic function and the modular function constructed in [5] as follows.

Definition 1. For $v \in \mathbb{Z}_q = \{-\frac{q-1}{2}, \ldots, \frac{q-1}{2}\}$, where q is odd prime number, define the characteristic function $Cha(v) : \mathbb{Z}_q \to \mathbb{Z}_2$ as follows:

$$Cha(v) = \begin{cases} 0 & \text{if} \quad v \in E = \{-\lfloor \frac{q}{4} \rfloor, \ldots, \lfloor \frac{q}{4} \rceil\}; \\ 1 & \quad v \in \{-\frac{q-1}{2}, \ldots, \frac{q-1}{2}\} - E. \end{cases} \tag{1}$$

Definition 2. For $v \in \mathbb{Z}_q$ and $b \in \mathbb{Z}_2$, define the modular function as follows:

$$Mod_2(v, b) = (v + b \cdot \frac{q}{2})(\mod q \mod 2) \tag{2}$$

As mentioned above, we have explained the theoretic thereunder and idealistic base for constructing a two-party key exchange protocol. But for key exchange protocol, that is far from enough. We need to consider how to eliminate the noise $(\mathbf{s}_i \cdot \mathbf{e}_j - \mathbf{s}_j \cdot \mathbf{e}_i)$, such that two party can recover $\mathbf{s}_i \cdot \mathbf{a} \cdot \mathbf{s}_j$ correctly. For negotiating $\mathbf{s}_i \cdot \mathbf{a} \cdot \mathbf{s}_j$, two party in [5] obtain bit-by-bit via computing $Mod_2(v, b)$. Take a bit for example as follows: Let q be a odd prime, given $b = Cha(v) \in \mathbb{Z}_2$, for $w = v + 2e$, where e is an error vector which satisfies $|e| < \frac{q}{2}$, then $Mod_2(v, Cha(v)) = Mod_2(w, Cha(v))$. That is, when the distance between w and v is within certain limits (i.e., $w = v + 2e$), then party i and party j can compute a shared bit b by using the modular function $Mod_2(v, b)$ based on w and v respectively, given a common semaphore (i.e., the characteristic function $Cha(v)$): $Mod_2(v, Cha(v)) = \overline{b} = Mod_2(w, Cha(v))$. We will list three main defects of [5] as follows.

An important requirement needs to be satisfied: each bit of the shared secret key should be uniformly distributed to prevent any adversary can guess correctly each secret shared bit with an non-negligible probability. Although we have explained that party i and party j can compute a shared bit $Mod_2(v, Cha(v)) = \overline{b}$ by using the modular function $Mod_2(v, b)$ based on w and v respectively, we are not sure whether $Pr[\overline{b} = 0] = Pr[\overline{b} = 1] = \frac{1}{2}$ holds or not? The answer to this question is no. Specifically, when q is odd prime, given $w, v \in_{\mathcal{R}} \mathbb{Z}_q$, if $Cha(v) = 0$, then the deviation that $Mod_2(w, Cha(v))$ outputs 0 or 1 is $\frac{1}{2|E|}$.

If $Cha(v) = 1$, then the deviation that $Mod_2(w, Cha(v))$ outputs 0 or 1 is $\frac{1}{|E|-1}$. In [5], although the uniformly distributed key material is hashed by using certain hash function to obtain an almost uniformly distributed key, NIST [13] pointed that if the length of the cryptographic hash function is κ, then the source string has at least 2κ min-entropy. The min-entropy of source string in [5] is $0.97n$. The AKE scheme [5] only can generate $0.485n$ bits secret key via using the standard cryptographic hash function SHA-2.

For the same reason as above, the output distribution of modular function is not statistically indistinguishable with the uniform distribution, given characteristic function. Because of this, it is insecure that the adversary may obtain some relevant information of session key by querying session state. Only when modulus q is a value of sub-exponential magnitude (i.e., $q = 2^{\omega(\log_2 n)}$), the output distribution of modular function is statistically indistinguishable with the uniform distribution, given characteristic function. But in this case, the computational costs and communication costs will go up.

Zhang *et al.* [5] adopt the power basis to represent each element over the residue ring $R_q = \mathbb{Z}_q[x]/(x^n + 1)$, where $n = 2^\kappa$. Since the size of the power basis is large over the residue ring R_q, the size of each element under the representation of the power basis is also large, so bringing more traffic and larger computing cost.

The hash function $\mathbf{H}_1 : \{0,1\}^* \rightarrow \chi_r = \mathcal{D}_{\mathbb{Z}^n,r}$ used in [5] maps any bit string to a discrete sampling result over an integer lattice. Zhang *et al.* [5] use a hash function such as SHA-2 to get a uniformly random string, but unfortunately, they have not given any explicit method to sample a noise from the Gaussian distribution by using this uniformly random string. In addition, this operation does not exist in any current literature or public invention. The crucial difference between our $\mathbf{H}_1$ and $\mathbf{H}_1$ used in [5] is that we give a concrete method to sample a noise from the Gaussian distribution by using hash function SHA-2 while they have not do. Actually, Zhang *et al.* [5] have not explicitly explained which hash function is used as $\mathbf{H}_2$. They just have mentioned that $\mathbf{H}_2$ is modeled as random oracle. In addition, $\mathbf{H}_2$ is not the focus of their attention. We use hash function SHA-2 to serve as $\mathbf{H}_2$.

D. Our results and approaches

Table I. Our AKE protocol

RLWE parameter: $q, m, n = \varphi(m), \mathbf{a} \leftarrow_{\mathcal{R}} U(R_q), \chi_{s_1}$		
Party i		Party j
$\mathbf{s}_i, \mathbf{e}_i \leftarrow_{\mathcal{R}} \chi_{s_1}$		$\mathbf{s}_j, \mathbf{e}_j \leftarrow_{\mathcal{R}} \chi_{s_1}$
$\mathbf{P}_i = \mathbf{a} \cdot \mathbf{s}_i + \mathbf{e}_i$		$\mathbf{P}_j = \mathbf{a} \cdot \mathbf{s}_j + \mathbf{e}_j$
$\mathbf{r}_i, \mathbf{f}_i \leftarrow_{\mathcal{R}} \chi_{s_1}$		$\mathbf{r}_j, \mathbf{f}_j \leftarrow_{\mathcal{R}} \chi_{s_1}$
$\mathbf{X}_i = \mathbf{a} \cdot \mathbf{r}_i + \mathbf{f}_i$	$\xrightarrow{\mathbf{X}_i, i}$	$\mathbf{Y}_j = \mathbf{a} \cdot \mathbf{r}_j + \mathbf{f}_j$
$d = \mathbf{H}_1(\mathbf{X}_i, j, i)$		$d = \mathbf{H}_1(\mathbf{X}_i, j, i)$
		$e = \mathbf{H}_1(\mathbf{X}_i, \mathbf{Y}_j, j, i)$
		$\sigma_j = g \cdot (\mathbf{X}_i + d \cdot \mathbf{P}_i) \cdot (\mathbf{r}_j + e \cdot \mathbf{s}_j)$
		$\overline{\mathbf{v}}_j \leftarrow \mathbf{dbl}(\sigma_j)$
	$\xleftarrow{\mathbf{Y}_j, \mathbf{v}_j, i, j}$	
$e = \mathbf{H}_1(\mathbf{X}_i, \mathbf{Y}_j, j, i)$		$\mathbf{v}_j = \langle \overline{\mathbf{v}}_j \rangle_2$
$\sigma_i = g \cdot (\mathbf{Y}_j + e \cdot \mathbf{P}_j) \cdot (\mathbf{r}_i + d \cdot \mathbf{s}_i)$		$\tau_j = \lfloor \overline{\mathbf{v}}_j \rceil_2$
$\tau_i = \mathbf{rec}(\sigma_i, \mathbf{v}_j)$		$sid = (i, j, \mathbf{X}_i, \mathbf{Y}_j, \mathbf{v}_j)$
$sid = (i, j, \mathbf{X}_i, \mathbf{Y}_j, \mathbf{v}_j)$		$SK_j = \mathbf{H}_2(sid, \tau_j)$
$SK_i = \mathbf{H}_2(sid, \tau_i)$		

Note: $\mathbf{H}_1 : \{0,1\}^* \rightarrow \chi_s$. $\mathbf{H}_2 : \{0,1\}^* \rightarrow \{0,1\}^\kappa$. $g = \prod_p (1 - \zeta_p)$, where p runs all odd primes dividing m. Particularly, $g = 2$, if m is a power of 2.

Fig. 1. Our AKE protocol

Table 1 shows our AKE protocol. We combine the reconciliation mechanism and representation method for elements over R_q under the decoding basis to realize a secure two-party AKE protocol. The core innovations of this paper is threefold:

First, we use the reconciliation mechanism as our robust extractor, thus remedying the above-mentioned deficiency.

Second, we adopt the decoding basis to represent elements over R_q to obtain smaller-sized element representation and lower computing costs. Specifically, modulus q that is used in our construction is only taken a value of polynomial magnitude (i.e., $q = \widetilde{O}(n^2)$), which vastly decreases computational costs and communication costs.

Let K be the m order cyclotomic field with $n = \varphi(m)$, By using the canonical imbedding, we construct a new method that maps any bit string to certain element, which follows the discrete gaussian distribution $\chi = \lfloor \Psi \rceil$ over $R = \mathbb{Z}[\zeta_m]$. Our specific method is described as follows:

Let n dimensional continuous Gaussian distribution to be generated, and let $2m$ be fixed parameter. Let $h : \{0,1\}^k \rightarrow \{0,1\}^{2mn}$ be a hash function such as SHA-2.

Divide the range of the hash function h into n groups, each of which contains $2m$ bits. We might as

well let the i-th group $(a_0, a_1, \ldots, a_{m-1}, a_m, \ldots, a_{2m-1})$. Then, convert into two integers: $A_{i,1} = a_0 + 2 \cdot a_1 + 2^2 \cdot a_2 + \cdots + 2^{m-1} \cdot a_{m-1}$, $A_{i,2} = a_m + 2 \cdot a_{m+1} + 2^2 \cdot a_{m+2} + \cdots + 2^{m-1} \cdot a_{2m-1}$. Let $u_{i,1} = \frac{1}{A_{i,1}}$ and $u_{i,2} = \frac{1}{A_{i,2}}$, compute $X_i = \sqrt{-2 \ln u_{i,1}} \cdot \cos(2\pi \cdot u_{i,1})$ and $Y_i = \sqrt{-2 \ln u_{i,2}} \cdot \cos(2\pi \cdot u_{i,2})$. Thus, (X_i, Y_i) is a bidimensional joint Gaussian random variable with mean 0 and variance 1.

For generating a Gaussian random variable with variance $\frac{s}{\sqrt{2}}$, just need to compute $(\frac{s}{\sqrt{2}} \cdot X_i, \frac{s}{\sqrt{2}} \cdot Y_i)$. Set $a_i = \frac{s}{\sqrt{2}} \cdot X_i$, $b_i = \frac{s}{\sqrt{2}} \cdot Y_i$, where $1 \leq i \leq \frac{n}{2}$.

Construct complex random variable $a_i + \sqrt{-1} \cdot b_i$ for $1 \leq i \leq \frac{n}{2}$. Set $x_i = a_i + b_i$, for $1 \leq i \leq \frac{n}{2}$, and set $x_i = a_i - b_i$, for $\frac{n}{2} \leq i \leq n$. Then, vector $(x_1, x_2, \ldots, x_n)$ is a vector over the conjugate symmetric hyperplane $H = \{\mathbf{x} \in \mathbb{C}^{\mathbb{Z}_m^*} | x_i = \overline{x_{m-i}}, \forall i \in \mathbb{Z}_m^*\}$.

Let σ be the canonical imbedding. $\overline{\mathbf{x}} = \sigma^{-1}(x_1, x_2, \ldots, x_n) \in \mathbb{Q}^n$ is a random variable that follows the continuous Gaussian distribution over K. Round each component of $\overline{\mathbf{x}}$ to the nearest integer, such that we obtain a vector $\mathbf{x}$ with integer coefficient.

Let $\overrightarrow{b}$ represent the power basis of $R = \mathbb{Z}[\zeta_m]$. Output $x = \langle \overrightarrow{b}, \mathbf{x} \rangle \in R = \mathbb{Z}[\zeta_m]$, which follows the discrete gaussian distribution $\chi = \lfloor \Psi \rceil$ over $R = \mathbb{Z}[\zeta_m]$.

E. Organization

The rest of this paper is organized as follows. Section 2 presents the preliminaries. The improved two-party AKE protocol is described in section 3. We analyze the security of the improved protocol in section 3. Finally, section 4 concludes this paper.

II. PRELIMINARIES

A. Abbreviations and notations

In this paper, $\mathbb{C}, \mathbb{R}, \mathbb{Z}, \mathbb{Q}$ denote the set of complex numbers, the set of real numbers, the set of integers and the set of rational numbers, respectively. For $x \in \mathbb{R}$, define $\lfloor x \rceil = \lfloor x + \frac{1}{2} \rfloor \in \mathbb{Z}$. For $q \geq 1$, define $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$. Let λ be the security parameter, if a polynomial time algorithm (PT) A runs in PT of λ, then it is efficient. If a function $f(\lambda) = o(\lambda^{-c})$, where $c > 0$, then it is negligible. We make use of the Landau

notations. For the algorithm A, if $|Pr[A(X)] - Pr[A(Y)]| \leq negl(\lambda)$, then these two distributions are computationally indistinguishable. We say X and Y are statistically indistinguishable over the distribution D, if $\frac{1}{2}\sum_{d\in D}|X(d) - Y(d)| \leq negl(\lambda)$. Let $\mathbf{rad}(m)$ denote the product of all distinct primes dividing m.

B. Security model

We use N to represent the maximum number of honest users participating in AKE protocol. Each users is denoted by a unique $i \in \{1, \cdots, N\}$, and has a pair of static public key and static secret key, where static public key is issued by the identity authentication center. An execution of the protocol is called a session. A session is activated by an incoming message in the form of (Π, I, i, j) or $(\Pi, R, j, i, \mathbf{X}_i)$, where Π is protocol identifier, I or R are role identifiers, and i or j are user identifiers. If user i receives a message in the form of $((\Pi, I, i, j))$, then user i is called the session initiator. User i outputs $\mathbf{X}_i$ and sends it to user j. If user j receives a message in the form of $(\Pi, R, j, i, \mathbf{X}_i)$, then user j is called the session responsor. User j outputs $\mathbf{Y}_j$ and sends it to user i. After exchanging two-way messages, two parties compute a session key. If the session is activated at i, and i is the initiator, then we use $sid = (\Pi, I, i, j, \mathbf{X}_i)$ or $sid = (\Pi, I, i, j, \mathbf{X}_i, \mathbf{Y}_j)$ to represent this session. Similarly, if the session is activated at j, and j is the responsor, then we use $sid = (\Pi, R, j, i, \mathbf{X}_i, \mathbf{Y}_j)$ to represent this session. For session identifier $sid = (\Pi, *, i, j, *, *)$, the third symbol represents session owner, and the fourth represents session peer. When the session owner has computed its session key, then this session is called completed. The matched session of $sid = (\Pi, I, i, j, \mathbf{X}_i, \mathbf{Y}_j)$ is $\overline{sid} = (\Pi, R, j, i, \mathbf{X}_i, \mathbf{Y}_j)$.

The adversary $\mathcal{A}$ is modeled as a probabilistic polynomial time (PPT) Turing machine, which can control the whole communication network. The endowed abilities of $\mathcal{A}$ is summarized as follows:

$\mathbf{Send}_0(\Pi, I, i, j)$: $\mathcal{A}$ activates party i as the initiator. The oracle returns $\mathbf{X}_i$ to $\mathcal{A}$.

$\mathbf{Send}_1(\Pi, R, j, i, \mathbf{X}_i)$: Using $\mathbf{X}_i$, $\mathcal{A}$ activates party j as the responsor. The oracle returns $\mathbf{Y}_j$ to $\mathcal{A}$.

$\mathbf{Send}_2(\Pi, R, i, j, \mathbf{X}_i, \mathbf{Y}_j)$: $\mathcal{A}$ sends $\mathbf{Y}_j$ to party i to finish the session, which has been activated by $\mathbf{Send}_0(\Pi, I, i, j)$.

$\mathbf{SessionKeyReveal}(sid)$: The oracle returns the session key, if it is finished.

$\mathbf{Corrupt}(i)$: The oracle returns the static secret key of party i to $\mathcal{A}$. Once the static secret key of party i is revealed, this party is called dishonest. Otherwise, this party is called honest.

$\mathbf{Test}(sid^*)$: The oracle chooses $b \in_{\mathcal{R}} \{0,1\}$ at random. If $b=0$, then oracle chooses a session key uniformly at random. If $b=1$, then it returns the session key of sid^*. We allow $\mathcal{A}$ makes only one query for a fresh session sid^*.

Definition 3. (Freshness) Let $sid^* = (\Pi, I, i^*, j^*, \mathbf{X}_i, \mathbf{Y}_j)$ or $((\Pi, R, j^*, i^*, \mathbf{X}_i, \mathbf{Y}_j)$ be a completed session. Assume its matched session exists, then sid^* is called a fresh session, if the following conditions hold:

$\mathcal{A}$ does not make a $\mathbf{SessionKeyReveal}(sid^*)$.

$\mathcal{A}$ does not make a $\mathbf{SessionKeyReveal}(\overline{sid}^*)$.

i^* and j^* are honest. That is, $\mathcal{A}$ does not make a $\mathbf{Corrupt}(i^*)$ or $\mathbf{Corrupt}(j^*)$.

$\mathcal{A}$ can make the above-mentioned queries to the oracle in any order. When $\mathcal{A}$ outputs a guess b' for b, this game ends. If $b'=b$, then we say $\mathcal{A}$ wins this game. Define the advantage of $\mathcal{A}$ as follows:

$$Adv_{\Pi,\mathcal{A}} = Pr[b'=b] - \frac{1}{2} \tag{3}$$

Definition 4. (Security) We say an AKE protocol is secure, if the following conditions hold: If two honest parties has finished matched session, then they has computed a same session key with an overwhelming probability. For any PPT adversary, $Adv_{\Pi,\mathcal{A}}$ is negligible.

Definition 5. (weak forward secrecy, wPFS) $\mathcal{A}$ can make $\mathbf{SessionKeyReveal}$ and $\mathbf{Corrupt}$ queries, but cannot make $\mathbf{State}$ query. In addition, if $\mathcal{A}$ has sent $\mathbf{Corrupt}(i)$ query, then there exists an instance $\Pi_j^{k'}$, which matches instance Π_i^k.

C. Cyclotomic number field and its codifferent

For a positive integer m, let ζ_m represent the primitive m-th root of unity. The minimal polynomial of ζ_m is called the m-th cyclotomic polynomial, which has complex roots ω_m^j, where $\omega_m = \exp(\frac{2\pi i}{m})$. Let $K = \mathbb{Q}(\zeta_m)$ and $R = \mathbb{Z}[\zeta_m]$ represent the m-th cyclotomic field and the m-th cyclotomic ring, respectively.

The power basis of $R = \mathbb{Z}[\zeta_m]$ is defined as $\overrightarrow{\mathbf{b}} = \{\zeta_m^j | 0 \leq j \leq \varphi(m)\}$. The powerful basis $\overrightarrow{\mathbf{p}}$ of $K = \mathbb{Q}(\zeta_m)$ and $R = \mathbb{Z}[\zeta_m]$ is defined as follows: For a prime power m, the powerful basis is the power basis $\overrightarrow{\mathbf{b}} = \{\zeta_m^j | 0 \leq j \leq \varphi(m)\}$; For $m = \prod_\ell m_\ell$, define $\overrightarrow{\mathbf{p}} = \bigotimes_\ell \overrightarrow{\mathbf{p}}_\ell$, that is, $\overrightarrow{\mathbf{p}}$ is the tensor product of $\overrightarrow{\mathbf{p}}_\ell$ of each $\mathbb{Q}(\zeta_{m_\ell})$.

1) Canonical embedding: Let $s_1 + 2s_2 = n$, there exists a hyperplane $H = \{(x_1, x_2, \ldots, x_n) \in \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2} | x_{s_1+s_2+j} = \overline{x_{s_1+j}}, \forall j \in [s_2]\} \subset \mathbb{C}^n$. Let us have a look at the characteristic of each element in H: $(x_1, x_2, \cdots, x_{s_1})$ are real numbers, and $x_{s_1+s_2+j} = \overline{x_{s_1+j}}$. We mainly consider the following space. Two coordinates of $(a+b\cdot\sqrt{-1}, a-b\cdot\sqrt{-1})$ are conjugate complex numbers, where $a, b \in \mathbb{R}$. $\{(a+b\cdot\sqrt{-1}, a-b\cdot\sqrt{-1}) | a, b \in \mathbb{R}\}$ is a two-dimensional vector space. Take a set of basis $(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}), (\frac{1}{\sqrt{2}}\cdot\sqrt{-1}, \frac{-1}{\sqrt{2}}\cdot\sqrt{-1})$. Obviously, $(a + b\cdot\sqrt{-1}, a - b\cdot\sqrt{-1}) = \sqrt{2}\cdot a\cdot(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}) + \sqrt{2}\cdot b\cdot(\frac{1}{\sqrt{2}}\cdot\sqrt{-1}, \frac{-1}{\sqrt{2}}\cdot\sqrt{-1})$. Thus, a set of basis of H can be expressed as $\{e_1, e_2, \cdots, e_{s_1}, \frac{1}{\sqrt{2}}(e_{s_1+j} + e_{s_1+s_2+j}), \frac{1}{\sqrt{2}}(e_{s_1+j} - e_{s_1+s_2+j}) | 1 \leq j \leq s_2\}$. If we consider the canonical embedding of cyclotomic number field, then $s_1 = 0$, $s_2 = \frac{\varphi(m)}{2}$. If the i-th root and the $(s_2 + i)$-th root are conjugate, then we have

$$\mathbf{T} = \frac{1}{\sqrt{2}} \begin{pmatrix} \mathbf{I}_{\frac{\varphi(m)}{2}} & \sqrt{-1}\cdot\mathbf{I}_{\frac{\varphi(m)}{2}} \\ \mathbf{I}_{\frac{\varphi(m)}{2}} & -\sqrt{-1}\cdot\mathbf{I}_{\frac{\varphi(m)}{2}} \end{pmatrix}$$

, where each column is a basis. If the $(s_1 + i)$-th root and the $(s_1 + 2s_2 - i)$-th root are conjugate, then we have

$$\mathbf{B} = \frac{1}{\sqrt{2}} \begin{pmatrix} \mathbf{I} & \sqrt{-1}\cdot\mathbf{J} \\ \mathbf{J} & -\sqrt{-1}\cdot\mathbf{I} \end{pmatrix}$$

, where $\mathbf{I}$ is a $s_2 \times s_2$ order unit matrix, $\mathbf{J}$ is a $s_2 \times s_2$ order inverse unit matrix, that is, the first column of $\mathbf{J}$ is the last column of $\mathbf{I}$, while the last column of $\mathbf{I}$ is the first column of $\mathbf{J}$. Certainly, matrices $\mathbf{I}$ and $\mathbf{J}$ may be considered as a unitary transformation from n dimensional real space to the hyperplane H. If there exist s_1 real roots during embedding process, then under these two embedded modes, the generator

$$\begin{array}{ccc} \mathbb{Q}(\zeta_m) & \xrightarrow{\text{coefficients embedding}} & \mathbb{Q}^n:\ \mathbf{a}=(a_1,a_2,\cdots,a_{n-1}) \\ \overrightarrow{\mathbf{p}}=\{\bigotimes_\ell \overrightarrow{\mathbf{p}}_\ell\} \Big\updownarrow \overrightarrow{\mathbf{b}}=(\zeta_m^j)_{0\le j\le\varphi(m)} & & \mathbf{a}=\mathbf{CRT}_m^{-1}\cdot\sigma(a) \Big\updownarrow \sigma(a)=\mathbf{CRT}_m\cdot\mathbf{a} \\ \bigotimes_\ell K_\ell & \xrightarrow{\text{canonical embedding}} & \sigma(a)\in H \end{array}$$

Fig. 2. The coefficients embedding and the canonical embedding connect algebraic elements, rational subspace, and complex subspace.

matrix of H is

$$\begin{pmatrix} \mathbf{I}_{s_1} & \mathbf{0} \\ \mathbf{0} & \mathbf{T} \end{pmatrix} \text{or} \begin{pmatrix} \mathbf{I}_{s_1} & \mathbf{0} \\ \mathbf{0} & \mathbf{B} \end{pmatrix}$$

Let $\sigma_i|_{\mathbb{Q}} : K \to \mathbb{C}$ via $\zeta_m \mapsto \omega_m^i$ be the ring homomorphism, the canonical embedding is defined as $\sigma(a) = (\sigma_i(a))_{i\in\mathbb{Z}_m^*}$, for each $a \in K$. The norm is defined as $\|a\|_2 = (\sum_{i\in\mathbb{Z}_m^*} |\sigma_i(a)|^2)^{1/2}$, $\|a\|_\infty = \max_{i\in\mathbb{Z}_m^*} |\sigma_i(a)|$. For m-th cyclotomic number field, where $n = \varphi(m)$, let $\mathbf{a}$ represent the coefficient embedding of $K = \mathbb{Q}(\zeta_m)$, that is, $a = \langle \overrightarrow{\mathbf{b}}, \mathbf{a}\rangle = \overrightarrow{\mathbf{b}}^T \cdot \mathbf{a}$. According the definition of the canonical embedding above mentioned, the relation between the coefficient embedding ($a \in K$ represented by the power basis $\overrightarrow{\mathbf{b}}$) and the canonical embedding ($a \in K$ represented by the powerful basis $\overrightarrow{\mathbf{p}}$) is $\sigma(a) = (\sigma_j(a))_{j\in\mathbf{Z}_m^*} = \mathbf{CRT}_m \cdot \mathbf{a}$, where $\mathbf{CRT}_m$ is the $n = \varphi(m)$ dimensional Vandermonde matrix:

$$\mathbf{CRT}_m = \begin{pmatrix} 1 & \zeta_m^{j_1} & \zeta_m^{2j_1} & \cdots & \zeta_m^{(n-1)j_1} \\ \vdots & & & \ddots & \vdots \\ 1 & \zeta_m^{j_i} & \zeta_m^{2j_i} & \cdots & \zeta_m^{(n-1)j_i} \\ \vdots & & & \ddots & \vdots \\ 1 & \zeta_m^{j_{\varphi(m)}} & \zeta_m^{2j_{\varphi(m)}} & \cdots & \zeta_m^{(n-1)j_{\varphi(m)}} \end{pmatrix} \tag{4}$$

Figure 1. describes that how the coefficients embedding and the canonical embedding connect algebraic elements, rational subspace, and complex subspace.

2) Codifferent: For m-th cyclotomic algebraic integral ring $R = \mathbb{Z}[\zeta_m]$, if m is even, then let $\widehat{m} = m/2$. If m is odd, then let $\widehat{m} = m$. Define $g = \prod_p(1-\zeta_p)$, where p runs all odd primes dividing m. Let $t = \widehat{m}/g$, $R^\vee = \langle g/\widehat{m}\rangle = \langle t^{-1}\rangle$, where $\langle g/\widehat{m}\rangle$ represents the codifferent finitely generated by $g/\widehat{m}$, whose coefficients are taken from the cyclotomic algebraic integral ring $R = \mathbb{Z}[\zeta_m]$. $t = \widehat{m}/g$ is an algebraic integral element in the cyclotomic field $K = \mathbb{Q}(\zeta_m)$, that is, $t = \widehat{m}/g \in R = \mathbb{Z}[\zeta_m]$. More specifically, $\widehat{m}$

is divisible by $g = \prod_p (1-\zeta_p)$. Since $t = \widehat{m}/g \in K$, but $t = \widehat{m}/g \notin R$, then $R^\vee = t^{-1}R = \langle t^{-1} \rangle = \langle g/\widehat{m} \rangle$ is not a subset of R. The codifferent is interpreted as a fractional ideal of algebraic integral ring$R$. Since $R^\vee = t^{-1}R$, then it is also a principal fractional ideal. The relationship between it and R are as follows: $R^\vee = t^{-1}R$, $\widehat{m}R^\vee \subseteq R$, $(R^\vee)^\vee = R$.

The significance of the codifferent lies in that it depicts the relationship between the dual ideal of a fractional ideal $I(\subseteq K)$ and inverse of $I(\subseteq K)$ in algebraic integral ring. Specifically, for any fractional ideal $I(\subseteq K)$, its dual ideal is $I^\vee = I^{-1} \cdot R$, where $R^\vee$ is the codifferent above defined, $I^{-1} = \{d \in K | d \cdot I \subset K\}$.

Definition 6. The decoding basis of the codifferent of $R^\vee$ is defined as $\overrightarrow{\mathbf{d}} = \tau(\overrightarrow{\mathbf{p}})^\vee$, i.e., the dual of the conjugate of the powerful basis of R, where τ is the conjugate map of K, $\tau(\zeta_m) = \zeta_m^{-1} = \zeta_m^{m-1}$.

In the applications of cryptographic protocols, we should clarify the relationship between the basis of the algebraic integral ring $R = \mathbb{Z}[\zeta_m] = \mathbb{Z}[x]/(\Phi(x))$ under the algebraic field and the basis of the codifferent $R^\vee$ under canonical embedding. Specially, between the powerful basis $\overrightarrow{\mathbf{p}}$ of $R = \mathbb{Z}[\zeta_m] = \mathbb{Z}[x]/(\Phi(x))$, the integral basis of the codifferent $R^\vee$, and the decoding basis $\overrightarrow{\mathbf{d}}$ of the codifferent $R^\vee$, these transformational relationships can guarantee the property of integral basis, which is the basic of efficient computing power on the computer. Fortunately, there exist these transformational relationships as follows: If a powerful basis of R is $\overrightarrow{\mathbf{p}}$, let $R^\vee = t^{-1} \cdot R = \langle t^{-1} \rangle = \langle g/\widehat{m} \rangle$ be the codifferent of $K = \mathbf{Q}(\zeta_m)$, then $t^{-1} \cdot \overrightarrow{\mathbf{p}}$ and the decoding basis $\overrightarrow{\mathbf{d}} = \tau(\overrightarrow{\mathbf{p}})^\vee$ are integral basis of the codifferent $R^\vee$, respectively. That is, when each element in $R^\vee$ is represented by this basis, its coefficient is integral. Figure 2. shows these transformational relationships between the basis of the algebraic integral ring $R = \mathbb{Z}[\zeta_m] = \mathbb{Z}[x]/(\Phi(x))$ under the algebraic field and the basis of the codifferent $R^\vee$ under canonical embedding.

D. Continuous/discrete RLWE distribution

Definition 7. Denote continuous Gaussian distribution on $R_q^\vee$ by $\Psi = \mathcal{D}_s = s^{-n} \cdot \rho_s(\mathbf{x})$. For each $\mathbf{a} \in_{\mathcal{R}} R_q$, $\mathbf{s} \in_{\mathcal{R}} R_q^\vee$ chosen uniformly ar random, error vector $\mathbf{e}$ chosen from the continuous Gaussian distribution

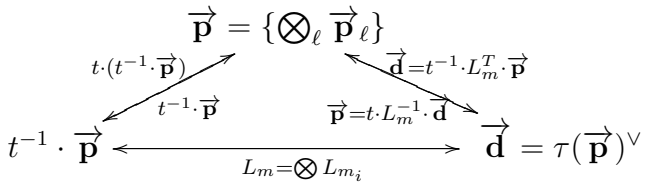

Fig. 3. Transformational relationships

ψ over $R_q^\vee$, output $(\mathbf{a}, \mathbf{b} = \mathbf{a}\cdot\mathbf{s} + \mathbf{e} \in R_q^\vee)$, we denote the RLWE Distribution over $R_q \times (K_\mathbb{R}/R_q^\vee)$ by $A_{\mathbf{s},\Psi}$. For any PPT adversary, it cannot differentiate the distribution $A_{\mathbf{s},\Psi}$ from the uniform distribution over $R_q \times (K_\mathbb{R}/R_q^\vee)$ with non-negligible probability. We call it $\mathrm{RLWE}_{q,\Psi}$ hard problem, or $\mathrm{RLWE}_{q,\Psi}$ hard assumption.

Since the coefficients of the error vectors, which are chosen from the continuous Gaussian distribution, are rational numbers, and since the rational numbers are represented with floating-point numbers in computer, this involves precision problem (i.e., according to the security parameter, those digits after the decimal point of those coefficients should be round to several bits. [17]) Therefore, in the constructions of cryptographic schemes, the error vectors are chosen from the discrete distribution $\chi = \lfloor\Psi\rceil$, where $\chi = \lfloor\cdot\rceil$ is a discretization method. One of the simplest discretization method is "rounding to the nearest integer". On the other hand, the secret vector $\mathbf{s} \in R_q^\vee$ is random, which is chosen form the RLWE distribution $A_{\mathbf{s},\Psi}$. [11] and [22] respectively point out that when $\mathbf{s} \in R_q^\vee$ is chosen from the same distribution Ψ as the error vector $\mathbf{e} \in R_q^\vee$, $\mathrm{RLWE}_{q,\Psi}$ still keeps its hardness. Moreover, when the secret vector $\mathbf{s} \in R_q^\vee$ is chosen from the distribution Ψ, we can make its size shorter. Obviously, it is very useful to cryptographic applications. Combining the above-mentioned two aspects, we can obtain the general $\mathrm{RLWE}_{q,\chi}$ hard problem as follows:

Definition 8. We denote the discrete Gaussian distribution over $R_q^\vee$ by $\chi = \lfloor\Psi\rceil = \lfloor\mathcal{D}_s = s^{-n}\cdot\rho_s(\mathbf{x})\rceil$. For $\mathbf{a} \in_\mathcal{R} R_q$ randomly chosen from the distribution χ, the secret vector $\mathbf{s} \in R_q^\vee$ chosen from χ, and the error vector $\mathbf{e} \in R_q^\vee$ chosen from the distribution χ, i.e., $\mathbf{s}, \mathbf{e} \leftarrow \chi = \lfloor\Psi\rceil$, output $(\mathbf{a}, \mathbf{b} = \mathbf{a}\cdot\mathbf{s} + \mathbf{e} \mod R_q^\vee)$, it is called the distribution $A_{\mathbf{s},\chi}$ over $R_q \times (K_\mathbb{R}/R_q^\vee)$. Similarly, for any PPT adversary, it cannot differentiate the distribution $A_{\mathbf{s},\chi}$ from the uniform distribution over $R_q \times (K_\mathbb{R}/R_q^\vee)$ with non-negligible

probability. We call it $\mathrm{RLWE}_{q,\chi}$ hard problem, or $\mathrm{RLWE}_{q,\chi}$ hard assumption.

For the relationship between $\mathrm{RLWE}_{q,\Psi}$ and $\mathrm{RLWE}_{q,\chi}$, [11] points out that if $\mathrm{RLWE}_{q,\Psi}$ problem is hard, then $\mathrm{RLWE}_{q,\chi}$ problem is hard, given the same number of samples $(\mathbf{a}_i, \mathbf{b}_i)$, for $i \in \mathbb{Z}^+$. Thus, we can adopt $\mathrm{RLWE}_{q,\chi}$ hard problem to design and construct varies of cryptographic schemes, actively and steadily. The following theorem elaborates the reduction from the average-case problem $\mathrm{RLWE}_{q,\chi}$ to the worst-case problem Ideal-SIVP.

Theorem II.1. *Let R be the mth cyclotomic ring of dimension $n = \varphi(m)$. Let $\gamma = \gamma(n) < \sqrt{\frac{\log n}{n}}$. Let $q = q(n)$ be a polynomial-bounded prime that satisfies $q \equiv 1 \mod m$, $\gamma \cdot q \geq \omega(\sqrt{\log n})$. There exists a polynomial time (PT) quantum reduction from solving $\widetilde{O}(\sqrt{n}/\gamma)$-approximating SIVP on ideal lattice over R to solving Ring-$\mathrm{DLWE}_{q,\chi}$, given $\lambda - 1$ samples from χ, where $\chi = \lfloor \Psi \rceil$, $\Psi = (\widehat{m}/g) \cdot \mathcal{D}_{\xi \cdot q}$, and $\xi = \gamma \cdot (n\lambda / \log(n\lambda))^{1/4}$.*

E. Gaussian distribution, subgaussian variables, and discrete gaussian sampling

Randomness is the base of the security of cryptographic algorithms, lattice-based public key cryptography is no exception. Being different from the traditional public key algorithms based on number theory, the introduction of randomness on lattice mainly is achieved by Gaussian sampling algorithm [19], [20]. Integer lattice (i.e., lattice basis consists of integer vectors) is the simplest lattice, and is the first lattice used in the designs of cryptographic algorithms [21], [22]. On the n dimensional integer lattice, the Gaussian function is defined on the real vector subspace $\mathbb{R}^n$. Now we research the ideal lattices over the cyclotomic field. Accordingly, the Gaussian function is defined on the real vector subspace $\mathbb{C}^n$.

1) Gaussian distribution: Since each root of m order cyclotomic polynomial $\Phi_m(x)$, which is defined over the cyclotomic number field $K = \mathbb{Q}[x]/(\Phi_m(x))$, is in the form of complex root ω_m^j, where $\omega_m = \exp(\frac{2\pi i}{m})$, $i \in \mathbb{Z}_m^*$, and the complex roots appear in pairs and mutually dual, the Gaussian function over the cyclotomic number field is not only defined over n dimensional complex vector subspace $\mathbb{C}^n$, but also is more accurately defined over a conjugate symmetric hyperplane $H = \{\mathbf{x} \in \mathbb{C}^{\mathbb{Z}_m^*} | x_i = \overline{x_{m-i}}, \forall i \in \mathbb{Z}_m^*\}$.

It can be proved that n dimensional real vector space $\mathbb{R}^n$ is isomorphic to the hyperplane H via a linear transformation defined by a unitary matrix

$$\mathbf{B} = \frac{1}{\sqrt{2}} \begin{pmatrix} \mathbf{I}_{\frac{\varphi(m)}{2}} & \sqrt{-1}\mathbf{J}_{\frac{\varphi(m)}{2}} \\ \mathbf{J}_{\frac{\varphi(m)}{2}} & -\sqrt{-1}\mathbf{I}_{\frac{\varphi(m)}{2}} \end{pmatrix} \in \mathbb{Z}_m^* \times [\varphi(m)] \tag{5}$$

$\mathbf{I}$ represents unit matrix. $\mathbf{J}$ is the reverse permutation matrix of $\mathbf{I}$. Meanwhile, this unitary matrix $\mathbf{B}$ is the generator matrix of the hyperplane H.

Definition 9. The Gaussian function $\rho_s : \ H \to (0, 1]$ is defined as follows

$$\rho_s(\mathbf{x}) = \exp(-\pi\langle \mathbf{x}, \mathbf{x}\rangle/s^2) = \exp(-\pi\|\mathbf{x}\|^2/s^2) \tag{6}$$

where $H = \{\mathbf{x} \in \mathbb{C}^{\mathbb{Z}_m^*} | x_i = \overline{x_{m-i}}, \forall i \in \mathbb{Z}_m^*\}$. Accordingly, we give the definition of continuous Gaussian distribution $\Psi = \mathcal{D}_s$ and that of discrete Gaussian distribution $\chi = \lfloor \Psi \rceil$ as follows.

Definition 10. For real $s > 0$, the probability density function of continuous Gaussian distribution $\Psi = \mathcal{D}_s$ is defined as $s^{-n} \cdot \rho_s(\mathbf{x})$, where s is the standard variance of Gaussian distribution.

Definition 11. For a coset $\Lambda + \mathbf{c}$ of a lattice Λ, let $s > 0$ be the standard variance, the discrete Gaussian distribution $\chi = \lfloor \Psi \rceil$ of lattice $\Lambda + \mathbf{c}$ is defined as

$$\mathcal{D}_{\Lambda+\mathbf{c},s}(\mathbf{x}) = \frac{\rho_s(\mathbf{x})}{\rho_s(\Lambda + c)}, \ \forall \mathbf{x} \in \Lambda + \mathbf{c}. \tag{7}$$

From the definition of $A_{s,\Psi}$ and that of $A_{s,\chi}$, it is known that major operations are executed on the codifferent $R^\vee = (\widehat{m}/g)^{-1} \cdot R$. Since the codifferent $R^\vee$ is an fractional ideal, although the decoding basis $\overrightarrow{\mathbf{d}} = \tau(\overrightarrow{\mathbf{p}})^\vee$ is integral basis, but the representation under the decoding basis will involve rational numbers, so use of integral ideal is more convenient in applications. For this purpose, an effective method is given as follows: Map $R^\vee$ to R: $\mathbf{e}^\vee \in R^\vee \xrightarrow{(\widehat{m}/g)\cdot\mathbf{e}^\vee} \mathbf{e} = (\widehat{m}/g) \cdot \mathbf{e}^\vee \in R$. Meanwhile, in order to maintain the advantage of $\mathbf{e}^\vee \in R^\vee$ represented under the decoding basis $\overrightarrow{\mathbf{d}}$ of the codifferent $R^\vee$ that has small coefficients (i.e., maintaining small coefficients invariant), we transform the decoding basis $\overrightarrow{\mathbf{d}}$ to $(\widehat{m}/g) \cdot \overrightarrow{\mathbf{d}}$. According to linearity, the integral coefficients of $\mathbf{e}$ represented under $(\widehat{m}/g) \cdot \overrightarrow{\mathbf{d}}$ are identical with the coefficients of $\mathbf{e}^\vee$ represented under $\overrightarrow{\mathbf{d}}$.

From the above analysis, by acting the expanded factor $\widehat{m}/g$ on the codifferent $\mathbf{e}^{\vee} \in R^{\vee}$, we have mapped $\mathbf{e} \in R^{\vee}$ to R. Thus, we have the following Hermite Normal Form of Learning with Errors (NHF-LWE) hard problem, which is more convenient in applications [22].

Definition 12. For cyclotomic integral ring R, we denote the discrete Gaussian distribution over R by $\chi = \lfloor \Psi \rceil = \lfloor (\widehat{m}/g) \cdot \mathcal{D}_s \rceil$, For $\mathbf{a} \in_{\mathcal{R}} R_q$, the secret vector $\mathbf{s} \leftarrow_{\mathcal{R}} \chi$, and the error vector $\mathbf{e} \leftarrow_{\mathcal{R}} \chi$, output $(\mathbf{a}, \mathbf{b} = \mathbf{a} \cdot \mathbf{s} + \mathbf{e} \mod R_q)$. We denote the NHF-LWE distribution over $R_q \times R_q$ by $A_{s,\chi}$. Similarly, for any probabilistic polynomial time (PPT) adversary, it cannot differentiate the distribution $A_{\mathbf{s},\chi}$ from the uniform distribution over $R_q \times R_q$ with non-negligible probability. We call it $\mathrm{NHF-LWE}_{q,\chi}$ hard problem, or $\mathrm{NHF-LWE}_{q,\chi}$ hard assumption.

After $1/g$ imbeds canonically, since the size of $\sigma_i(1/g)$ changes sharply, then the size ratio of $\|\mathbf{e}^{\vee}\|_2/\|\mathbf{e}\|_2$ depends on $\mathbf{e}^{\vee}$, and this size ration varys along with $\mathbf{e}^{\vee}$. Besides, there exists a positive correlation between this size ratio and the standard derivation s. We should multiply $\mathbf{e}$ by g to eliminate this influence mentioned above. $g \cdot \mathbf{e}$ is a subgaussian random variable. Now we review the definition and properties of subgaussian random variables [11] as follows.

Definition 13. For any $\delta > 0$, if for each $t \in \mathbb{R}$, the moment generating function of random variable $\mathbf{X}$ satisfies

$$E[\exp(2\pi t\mathbf{X})] \leq \exp(\delta) \cdot \exp(\pi r^2 t^2) \tag{8}$$

, then we say the random variable $\mathbf{X}$ is a δ-subgaussian random variable over $\mathbb{R}$ with parameter r.

Property 1. *Let $\mathbf{X}$ be a δ-subgaussian random variable over $\mathbb{R}$ with parameter r. By Markov's inequality, for any $t \geq 0$, we have*

$$Pr[|\mathbf{X}| \geq t] \leq 2\exp(\delta - \pi t^2/r^2) \tag{9}$$

Property 2. *Let $\mathbf{X}_1$ be a δ_1-subgaussian random variable over $\mathbb{R}$ with parameter r_1, and let $\mathbf{X}_2$ be a δ_2-subgaussian random variable over $\mathbb{R}$ with parameter r_2. $\mathbf{X}_1$ and $\mathbf{X}_2$ are mutually independent, then $\mathbf{X}_1 + \mathbf{X}_2$ is a $(\delta_1 + \delta_2)$-subgaussian random variable over $\mathbb{R}$ with parameter $\sqrt{r_1^2 + r_2^2}$.*

2) Discrete gaussian sampling: In the applications of $\mathrm{NHF}-\mathrm{LWE}_{q,\chi}$, the secrete vector $\mathbf{s}\in R_q$ and the error vector $\mathbf{e}\in R_q$ are sampled from the discrete Gaussian distribution $\lfloor\Psi\rceil$ over the cyclotomic number field K, which need to be sampled from the continuous Gaussian distribution Ψ over the cyclotomic number field K, and then obtain the discrete Gaussian distribution $\lfloor\Psi\rceil$.

The canonical embedding maps each element over the cyclotomic field K to the hyperplane H. Our goal is to obtain a discrete gaussian distribution with parameter $s>\omega(\sqrt{\log n})$. The basic idea of achieving the discrete Gaussian distribution $\lfloor\Psi\rceil$ over the cyclotomic field K is as follows: First, sample $\sigma(e)\in H$ from the continuous gaussian distribution $\Psi=(\widehat{m}/g)\cdot\mathcal{D}_{\sqrt{2}\cdot s}$ with parameter $\sqrt{2}\cdot s$ over H: For $1\leq i\leq\frac{n}{2}$, generate $\frac{n}{2}$ pairs of Gaussian random variables (a_i,b_i) with standard variance $\sqrt{2}\cdot s$ independently; For $1\leq i\leq\frac{n}{2}$, let $x_i=a_i+b_i$. For $\frac{n}{2}\leq i\leq n$, let $x_{\frac{n}{2}+i}=a_i-b_i$. Then, $\sigma(e)=(x_1,\ldots,x_n)$ is an element of H, which follows the continuous Gaussian distribution $\Psi=\mathcal{D}_{\sqrt{2}\cdot s}$ with standard variance $\sqrt{2}\cdot s$. Second, make inverse transformation from hyperplane H to $R=\mathbb{Z}[\zeta_m]$. Let $\mathbf{CRT}_m$ be the corresponding matrix of canonical embedding σ, and compute $\mathbf{e}=(\frac{\widehat{m}}{g})\cdot\mathbf{CRT}_m^{-1}\cdot\sigma(e)\in\mathbb{Q}^n$. Finally, discretize $\mathbf{e}$. Round each rational component of $\mathbf{e}$ to the nearest integer, so that we obtain vector $\lfloor\mathbf{e}\rceil$ with integral coefficients. Let $\overrightarrow{\mathbf{p}}$ be the powerful basis of $R=\mathbb{Z}[\zeta_m]$, and output $e=\langle\overrightarrow{\mathbf{p}},\mathbf{e}\rangle$, which is chosen from the discrete gaussian distribution $(\widehat{m}/g)\cdot\mathcal{D}_s$ over $R=\mathbb{Z}[\zeta_m]$.

So far, we have realized the discrete gaussian distribution over the cyclotomic field. However, in the computations, we also need to know the coefficient representation $\overline{\mathbf{e}}$ of $e\in K$ represented under the decoding basis $\overrightarrow{\mathbf{d}}$. So we give a computing method of $\overline{\mathbf{e}}$ from $e\in K$ as follows: Let $\overrightarrow{\mathbf{d}}$ represent the decoding basis of $R^\vee$, then the representation of $e\in K$ under the decoding basis $(\widehat{m}/g)\cdot\overrightarrow{\mathbf{d}}$ of $R=\mathbb{Z}[\zeta_m]$ is given: $e=(\widehat{m}/g)\cdot\langle\overrightarrow{\mathbf{d}},\overline{\mathbf{e}}\rangle$, $\overline{\mathbf{e}}=\mathbf{CRT}_m^*\cdot\sigma(e)=(\overline{\mathbf{CRT}_m})^T\cdot\sigma(e)$.

For $e=\langle\overrightarrow{\mathbf{p}},\mathbf{e}\rangle$ that follows the discrete gaussian distribution $(\widehat{m}/g)\cdot\mathcal{D}_s$ over $R=\mathbb{Z}[\zeta_m]$, the following two lemmas further consider the distribution regularities of subgaussian random variable $g\cdot e$ represented under the decoding basis of $R^\vee$.

Lemma II.2. *For $g=\prod_p(1-\zeta_p)$, where p runs all odd primes dividing m. Let $e\in\mathbb{Q}(\zeta_m)$, such that*

$g \cdot e$ is a δ-subgaussian random variable with parameter $\widehat{m} \cdot r$. Then for each $e' \in \mathbb{Q}(\zeta_m)$, each coefficient of $e' \cdot e \in \mathbb{Q}(\zeta_m)$, which is represented by the decoding basis of $R^\vee$, is a δ-subgaussian random variable with parameter $r \cdot \|e'\|_2$.

Lemma II.3. *Let $e \leftarrow_{\mathcal{R}} \lfloor \Psi \rceil$ be a error vector, where $\Psi = (\widehat{m}/g) \cdot \mathcal{D}_s = (\widehat{m}/g) \cdot s^{-n} \cdot \rho_s(\mathbf{x})$, then $g \cdot e$ is a δ-subgaussian random variable with parameter $\widehat{m} \cdot \sqrt{s^2 + 2\pi \cdot \mathbf{rad}(m)/m}$.*

F. Rejecting sampling

We review the rejection sampling algorithm [12].

There exists a subset $V \subseteq \mathbb{Z}^m$, in which norm of each element is less than T. Let $\alpha = \omega(T\sqrt{\log m})$ be a real number. Let $D : V \to \mathbb{R}$ be a probability distribution. Therefore, there is a constant number $M = O(1)$, which makes the distribution of the following algorithm $\mathcal{A}_1$ is within statistical distance $\frac{2^{-\omega(\log m)}}{M}$ of the distribution of the following algorithm $\mathcal{A}_2$. The probability that $\mathcal{A}_1$ outputs something is at least $\frac{1-2^{-\omega(\log m)}}{M}$. If $\alpha = \beta T$ with $\beta > 0$, then $M = e^{12/\beta + 1/(2\beta^2)}$, the output of algorithm $\mathcal{A}_1$ is within statistical distance $\frac{2^{-100}}{M}$ of the output of $\mathcal{A}_2$, and the probability that $\mathcal{A}_1$ outputs something is at least $\frac{1-2^{-100}}{M}$. The algorithm $\mathcal{A}_1$ is expressed as follows: First, sample $\mathbf{v} \leftarrow_{\mathcal{R}} D$ randomly. Second, sample $\mathbf{z} \leftarrow_{\mathcal{R}} \mathcal{D}^m_{\mathbf{v},\alpha}$ randomly. Finally, output $(\mathbf{z}, \mathbf{v})$ with probability $\min\{1, \frac{\mathcal{D}^m_\alpha(\mathbf{z})}{M\mathcal{D}^m_{\mathbf{v},\alpha}(\mathbf{z})}\}$. The algorithm $\mathcal{A}_2$ is expressed as follows: First, sample $\mathbf{v} \leftarrow_{\mathcal{R}} D$. Second, sample $\mathbf{z} \leftarrow_{\mathcal{R}} \mathcal{D}^m_\alpha$. Finally, output $(\mathbf{z}, \mathbf{v})$ with probability $\frac{1}{M}$.

G. Reconciliation mechanism

Here we review the reconciliation mechanism [6].

Definition 14. Define modular 2 rounding function $\lfloor \cdot \rceil_2 : \mathbb{Z}_q \to \mathbb{Z}_2$ via

$$\lfloor x \rceil_2 = \lfloor \frac{2}{q} \cdot x \rceil \tag{10}$$

Definition 15. Define cross-rounding function $\langle \cdot \rangle_2 : \mathbb{Z}_q \to \mathbb{Z}_2$ via

$$x \mapsto \lfloor \frac{q}{4} \cdot x \rfloor \mod 2 \tag{11}$$

Lemma II.4. *For even module q, if $x \in \mathbb{Z}_q$ is chosen uniformly at random, then the distribution of $\lfloor x \rceil_2$ is uniform over $\mathbb{Z}_q$, given $\langle x \rangle_2$.*

Definition 16. For even module q, $e \in E = [-\frac{q}{8}, \frac{q}{8}) \bigcap \mathbb{Z}$, let $w \in \mathbb{Z}_q$ and $b \in \mathbb{Z}_2$, define the reconciliation function $\mathbf{rec}: \ \mathbb{Z}_q \times \mathbb{Z}_2 \to \mathbb{Z}_2$ via

$$\mathbf{rec}(w, b) = \begin{cases} 0 & \text{if} \quad w \in I_b + E; \\ 1 & \text{otherwise.} \end{cases} \tag{12}$$

Lemma II.5. *For even module q, $e \in E = [-\frac{q}{8}, \frac{q}{8}) \bigcap \mathbb{Z}$, if $w = x + e \mod q$, given $w \in \mathbb{Z}_q$ and $\langle x \rangle_2$, then*

$$\mathbf{rec}(w, \langle x \rangle_2) = \lfloor x \rceil_2 = \mathbf{rec}(x, \langle x \rangle_2) \tag{13}$$

For even module q, if $x \in \mathbb{Z}_q$ is uniform at random, modular 2 rounding function $\lfloor x \rceil_2$ is uniform over $\mathbb{Z}_2$, and the distance between $x \in \mathbb{Z}_q$ and $w \in \mathbb{Z}_q$ is within certain realms under module q, then we can recover $\lfloor x \rceil_2$ based on the reconciliation function with the cross-rounding function $\langle x \rangle_2$ and $w \in \mathbb{Z}_q$. However, in the applications of ring learning with errors problems, we demand module q is odd. This bring a problem: If q is odd, then the output distribution of modular 2 rounding function $\lfloor x \rceil_2$ is not only biased, but also incurs a deviation. We have known that for odd module q, although $x \in \mathbb{Z}_q$ is uniform, $\lfloor x \rceil_2 = 0$ and $\lfloor x \rceil_2 = 1$ are biased. For constructing cryptographic schemes, we demand that each bit of the secret key is uniform. So we expand module q via $q \mapsto 2q$ to guarantee that $x \in \mathbb{Z}_{2q}$ is uniform, such that we can resolve this contradiction.

Definition 17. Define randomized function $\mathbf{dbl}: \ \mathbb{Z}_q \to \mathbb{Z}_{2q}$ via

$$x \mapsto \overline{x} = 2x - \overline{e}(\mod 2q) \tag{14}$$

Note $\mathbf{Pr}[\overline{e} = 0] = \frac{1}{2}$, $\mathbf{Pr}[\overline{e} = -1] = \mathbf{Pr}[\overline{e} = 1] = \frac{1}{4}$, $\overline{e} \leftarrow_{\mathcal{R}} \mathbb{Z}_2$.

Lemma II.6. *For odd module q, If $x \in \mathbb{Z}_q$ is uniform, then $\lfloor \overline{x} \rceil_2$ is uniform with $\overline{x} \leftarrow \mathbf{dbl}(x)$, given $\langle \overline{x} \rangle_2$.*

III. THE PROPOSED PROTOCOL

All the specific parameters are described as follows:

- A positive integer m: It depicts the algebraic specification of m order cyclotomic algebraic number field $R = \mathbb{Z}[\zeta_m] = \mathbb{Z}[x]/(\Phi_m(x))$, where $\Phi_m(x)$ is of degree $n = \varphi(m)$ cyclotomic polynomial.
- An odd prime module q: $\mathbf{gcd}(q, m) = 1$.
- $\mathbf{a} \leftarrow_{\mathcal{R}} U(R_q)$: global public parameter.
- $g = \prod_p (1 - \zeta_p)$, where p runs all odd primes dividing m. Specially, we have $g = 2$, if m is a power of 2.
- Discrete gaussian distribution $\chi_s = \lfloor \Psi \rceil$ over $R = \mathbb{Z}[\zeta_m]$: $\Psi = (\frac{\widehat{m}}{g}) \cdot \mathcal{D}_s = (\frac{\widehat{m}}{g}) \cdot s^{-n} \cdot \rho_s(\mathbf{x})$.
- $\mathbf{H}_1 : \{0,1\}^* \rightarrow R$: Apply this string as randomness to sample from $\mathcal{D}_{s_1}$ to obtain an element that is $\lfloor \Psi \rceil$ distributed over $R = \mathbb{Z}[\zeta_m]$.
- $\mathbf{H}_2 : \{0,1\}^* \rightarrow \{0,1\}^\kappa$ is the key derivation function, which is a random oracle actually.

A. Protocol description

Party i samples $\mathbf{s}_i, \mathbf{e}_i \leftarrow_{\mathcal{R}} \chi_{s_1}$ randomly, where $\mathbf{e}_i$ is an error vector. Party i uses $\mathbf{s}_i$ as its static secret key, and computes $\mathbf{P}_i = \mathbf{a} \cdot \mathbf{s}_i + \mathbf{e}_i \in R_q$, and uses $\mathbf{P}_i$ as its static public key. Similarly, party j samples $\mathbf{s}_j, \mathbf{e}_j \leftarrow_{\mathcal{R}} \chi_{s_1}$ randomly, where $\mathbf{e}_j$ is an error vector. Party j uses $\mathbf{s}_j$ as its static secret key, and computes $\mathbf{P}_j = \mathbf{a} \cdot \mathbf{s}_j + \mathbf{e}_j \in R_q$, and uses $\mathbf{P}_j$ as its static public key.

Initiation. Party i executes the following steps:

1) Sample $\mathbf{r}_i, \mathbf{f}_i \leftarrow_{\mathcal{R}} \chi_{s_1}$, compute $\mathbf{X}_i = \mathbf{a} \cdot \mathbf{r}_i + \mathbf{f}_i$, and send $\mathbf{X}_i$ to party j;
2) Compute $d = \mathbf{H}_1(\mathbf{X}_i, j, i)$, $\overline{\mathbf{r}}_i = \mathbf{r}_i + d \cdot \mathbf{s}_i$, and $\overline{\mathbf{f}}_i = \mathbf{f}_i + d \cdot \mathbf{e}_i$;
3) Let $\mathbf{c} \in \mathbb{Z}^{2n}$ represent the concatenation between the coefficient vector of $\overline{\mathbf{r}}_i$ and the coefficient vector of $\overline{\mathbf{f}}_i$. Let $\mathbf{c}_1 \in \mathbb{Z}^{2n}$ represent the concatenation between the coefficient vector of $d \cdot \mathbf{s}_i$ and the coefficient vector of $d \cdot \mathbf{e}_i$. Repeat step 1-3 with a probability of $1 - \min(1, \mathcal{D}_{\mathbb{Z}^{2n}, s_1}(\mathbf{c})/M \cdot \mathcal{D}_{\mathbb{Z}^{2n}, s_1, \mathbf{c}_1}(\mathbf{c}))$.

Response. After receiving $\mathbf{X}_i$, party j executes the following steps:

1) Sample $\mathbf{r}_j, \mathbf{f}_j \leftarrow_{\mathcal{R}} \chi_{s_1}$, compute $\mathbf{Y}_j = \mathbf{a} \cdot \mathbf{r}_j + \mathbf{f}_j$;
2) Compute $e = \mathbf{H}_1(\mathbf{X}_i, \mathbf{Y}_j, j, i)$, $\overline{\mathbf{r}}_j = \mathbf{r}_j + e \cdot \mathbf{s}_j$, and $\overline{\mathbf{f}}_j = \mathbf{f}_j + e \cdot \mathbf{e}_j$;
3) Let $\mathbf{c} \in \mathbb{Z}^{2n}$ represent the concatenation between the coefficient vector of $\overline{\mathbf{r}}_j$ and the coefficient vector of $\overline{\mathbf{f}}_j$. Let $\mathbf{c}_1 \in \mathbb{Z}^{2n}$ represent the concatenation between the coefficient vector of $e \cdot \mathbf{s}_j$ and the coefficient vector of $e \cdot \mathbf{e}_j$. Repeat steps 1-3 with a probability of $1 - \min(1, \mathcal{D}_{\mathbb{Z}^{2n}, s_1}(\mathbf{c})/M \cdot \mathcal{D}_{\mathbb{Z}^{2n}, s_1, \mathbf{c}_1}(\mathbf{c}))$;
4) Compute $\sigma_j = g \cdot (\mathbf{X}_i + d \cdot \mathbf{P}_i) \cdot (\mathbf{r}_j + e \cdot \mathbf{s}_j)$;
5) Compute $\overline{\mathbf{v}}_j \leftarrow \mathbf{dbl}(\sigma_j)$ and $\mathbf{v}_j = \langle \overline{\mathbf{v}}_j \rangle_2$, and send $(\mathbf{Y}_j, \mathbf{v}_j)$ to party i;
6) Compute $\tau_j = \lfloor \overline{\mathbf{v}}_j \rceil_2$ and $SK_j = \mathbf{H}_2(sid, \tau_j)$.

Completion. After receiving $(\mathbf{Y}_j, \mathbf{v}_j)$, party j executes the following steps:

1) Compute $e = \mathbf{H}_1(\mathbf{X}_i, \mathbf{Y}_j, j, i)$ and $\sigma_i = g \cdot (\mathbf{Y}_j + e \cdot \mathbf{P}_j) \cdot (\mathbf{r}_i + d \cdot \mathbf{s}_i)$;
2) Compute $\tau_i = \mathbf{rec}(\sigma_i, \mathbf{v}_j)$ and $SK_i = \mathbf{H}_2(sid, \tau_i)$.

B. Correctness

The following two lemmas analyze the requirement that party i and party j can negotiate a shared key.

Lemma III.1. *Suppose $\|g \cdot \mathbf{s}_i\|_2 \leq \ell$, $\|g \cdot \mathbf{r}_i\|_2 \leq \ell$, $\|g \cdot \mathbf{s}_j\|_2 \leq \ell$, $\|g \cdot \mathbf{r}_j\|_2 \leq \ell$, where $(\mathbf{s}_i, \mathbf{e}_i)$ are secret vectors chosen by party i, and $(\mathbf{s}_i, \mathbf{e}_i)$ are secret vectors chosen by party j. Let $e_1 = \sigma_i - \sigma_j$, $\overline{e}_1 \in R$ is a random element that is chosen in $\overline{\mathbf{v}}_j \leftarrow \mathbf{dbl}(\sigma_j)$, then $\overline{\mathbf{v}}_j = 2\sigma_j - \overline{e}_1 \in R_{2q}$. Let $w = t/s$. in order to realize*

$$\mathbf{rec}(\sigma_i, \mathbf{v}_j) = \tau_i = \tau_j = \lfloor \overline{\mathbf{v}}_j \rceil_2 \tag{15}$$

, module q is required to satisfy

$$(\frac{q}{8})^2 \geq [\ell^2 \cdot s'^2 \cdot (3s^2 + n) + 1 + \frac{\pi}{4}] \cdot w^2 \tag{16}$$

, where $t = \frac{q}{8}$, $s' = \sqrt{s^2 + 2\pi \cdot \mathbf{rad}(m)/m}$, s is the variance of distribution $\mathcal{D}_s$.

Proof For $(\sigma_i - \sigma_j)$, we obtain $\overline{\sigma}_j = 2\sigma_j - \overline{e}_1 \in R_{2q}$. Since $\|g \cdot \mathbf{s}_i\|_2 \leq \ell$, then each encoding basis coefficient of $g \cdot \mathbf{s}_i \cdot \mathbf{f}_j$ is δ-subgaussian with parameter $s' \cdot \ell$ by property 1. By property 2, each encoding basis coefficient of $g \cdot d$ is δ-subgaussian with parameter $\widehat{m} \cdot r'$. Since $\|g \cdot \mathbf{s}_i \cdot \mathbf{f}_j\|_2 \leq \|g \cdot \mathbf{s}_i\|_2 \cdot \|\mathbf{f}_j\|_\infty \leq \ell \cdot s\sqrt{n}$. By property 1, each encoding basis coefficient of $g \cdot d \cdot \mathbf{s}_i \cdot \mathbf{f}_j$ is δ-subgaussian with parameter $\ell \cdot s' \cdot s\sqrt{n}$. Similarly, we obtain that each encoding basis coefficient of $g \cdot d \cdot \mathbf{e}_j \cdot \mathbf{r}_i$, $g \cdot d \cdot \mathbf{e}_i \cdot \mathbf{r}_j$ and $g \cdot d \cdot \mathbf{f}_i \cdot \mathbf{s}_j$ is δ-subgaussian with parameter $\ell \cdot s' \cdot s\sqrt{n}$, respectively.

We have known that each encoding basis coefficient of $g \cdot d$ is δ-subgaussian with parameter $\widehat{m} \cdot s'$ and $\|g \cdot e \cdot \mathbf{s}_i \cdot \mathbf{e}_j\|_2 \leq \|g \cdot \mathbf{s}_i \cdot \mathbf{e}_j\|_2 \cdot \|e\|_\infty \leq \ell \cdot s\sqrt{n} \cdot s\sqrt{n} = \ell \cdot s^2 \cdot n$. Each encoding basis coefficient of $g \cdot d \cdot e \cdot \mathbf{s}_i \cdot \mathbf{e}_j$ is δ-subgaussian with parameter $s' \cdot \ell \cdot s^2 \cdot n$. By property 2, each coefficient of $g \cdot \mathbf{f}_j$ is δ-subgaussian with parameter $\widehat{m} \cdot s'$. Since $\|g \cdot \mathbf{r}_i\|_2 \leq \ell$, each encoding basis coefficient of $g \cdot \mathbf{f}_j \cdot \mathbf{r}_i$ is δ-subgaussian with parameter $s' \cdot \ell$. Similarly, each coefficient of $g \cdot \mathbf{f}_j \cdot \mathbf{r}_i$ is δ-subgaussian with parameter $s' \cdot \ell$.

By assumption, we obtain that each coefficient of $\overline{e}_1$ is 0-subgaussian with parameter $\sqrt{2\pi}$. Finally, we obtain that $2e_1 + \overline{e}_1$ is 8δ-subgaussian with parameter $2\sqrt{2} \cdot \sqrt{[\ell^2 \cdot s'^2 \cdot (3s^2 + n) + 1 + \frac{\pi}{4}]}$. By Markov's inequality and the union bound over all n coefficients, it naturally proves this lemma.

Lemma III.2. *When* $(\frac{q}{8})^2 \geq [\ell^2 \cdot s'^2 \cdot (3s^2 + n) + 1 + \frac{\pi}{4}] \cdot w^2$*, party* i *computes*

$$\mathbf{rec}(\sigma_i, \mathbf{v}_j) = \tau_i = \tau_j = \lfloor \overline{\mathbf{v}}_j \rceil_2 \tag{17}$$

, and succeeds in recovering τ_i *except with probability at most* $2n \cdot \exp(8\delta - \pi w^2)$*, where* $\delta \leq 2^{-n}$*.*

Proof According to lemma 3.1, combining with $Pr[|\mathbf{X}| \geq t] \leq 2\exp(\delta - \frac{\pi t^2}{s^2})$, we know when $(\frac{q}{8})^2 \geq [\ell^2 \cdot s'^2 \cdot (3s^2 + n) + 1 + \frac{\pi}{4}] \cdot w^2$, each coefficient of $2e_1 + \overline{e}_1$ represented by decoding basis does not fall into $[-\frac{q}{4}, \frac{q}{4})$ with probability of $2\exp(8\delta - \pi w^2)$. By lemma 2.5, party i recovers correctly $\tau_i = \tau_j$ except with probability at most $2n \cdot \exp(8\delta - \pi w^2)$.

Note If an adversary Eve got $\mathbf{Y}_j$, let us suppose that Eve can fake Party i's ephemeral secret key $(\mathbf{r}'_i, \mathbf{f}'_i)$ and ephemeral public key $\mathbf{X}'_i = \mathbf{a} \cdot \mathbf{r}'_i + \mathbf{r}'_i$. More seriously, we assume that Eve can fake Party i's static

secret key $(\mathbf{s}'_i, \mathbf{e}'_i)$ and static public key $\mathbf{P}'_i = \mathbf{a} \cdot \mathbf{s}'_i + \mathbf{f}'_i$ such that $\mathbf{P}'_i = \mathbf{P}_i$. Assume Eve can break the one-wayness of hash function $\mathbf{H}_1$ such that $d' = \mathbf{H}_1(\mathbf{X}_i, j, i') = d$ and $e' = \mathbf{H}_1(\mathbf{X}_i, \mathbf{Y}_i, j, i') = e$. In this case, Eve computes $\sigma = g \cdot (\mathbf{Y}_j + e' \cdot \mathbf{P}_j) \cdot (\mathbf{r}'_i + d' \cdot \mathbf{s}'_i) = g \cdot (\mathbf{Y}_j \cdot \mathbf{r}'_i + \mathbf{Y}_j \cdot d \cdot \mathbf{s}'_i + e \cdot \mathbf{P}_j \cdot \mathbf{r}'_i + e \cdot d \cdot \mathbf{P}_j \cdot \mathbf{s}'_i)$. At the same time, Party j computes $\sigma_j = g \cdot (\mathbf{X}_i + d \cdot \mathbf{P}_i) \cdot (\mathbf{r}_j + e \cdot \mathbf{s}_j) = g \cdot (\mathbf{X}_i \cdot \mathbf{r}_j + \mathbf{P}_i \cdot d \cdot \mathbf{r}_j + e \cdot \mathbf{s}_j \cdot \mathbf{X}_i + e \cdot \mathbf{s}_j \cdot d \cdot \mathbf{P}_i)$. After calculation, we can obtain an important inequation of two absolute distances: $\|\sigma - \sigma_j\| \gg \|\sigma_i - \sigma_j\|$. It is impossible that the forge σ is close to σ_j, because of $(\sigma - \sigma_j) > g \cdot e \cdot d \cdot \mathbf{a} \cdot (\mathbf{s}'_i - \mathbf{s}_i) \cdot \mathbf{s}_j$, which is a large vector. Therefore, the adversary Eve cannot compute the session key with the forge σ.

C. Performance

A general methodology for LWE security evaluation is to adopt distinguishing attack proposed by Lindner and Peikert [24], which is just applied to the general LWE problems. Because there dose not exist an effective attack method for RLWE problems, we are still using distinguishing attack for RLWE. The distinguishing attack is built on the BKZ algorithm for shortest vector problem (SVP) in lattices. Subsequently, Chen and Nguyen proposed BKZ 2.0 algorithm [25]. Let n be the dimension of the underlying lattice, for the module q and the variance s of errors of decisional LWE problem (i.e., the error distribution is $\mathcal{D}_{\mathbb{Z}^n, s}$), we require

$$n \geq \frac{(k + 110) \cdot \log_2(\frac{q}{s})}{7.2} \tag{18}$$

Note that k is secure bits that is trying to achieve (i.e., the time/advantage ration is of at least 2^k) [25].

From the generation procedure of distribution χ, we can compute the number of bits needed to represent secret key. Since a_i is a random variable with derivation $\frac{s}{\sqrt{2}}$ over Gaussian distribution, and $Pr[|a_i| \geq 4 \cdot \frac{s}{\sqrt{2}}] \leq 2 \cdot \exp(-16\pi) \leq 2^{-70}$ (i.e., lemma 8.2, [11]), then we can use $\log_2(8 \cdot \frac{s}{\sqrt{2}})$ bits to represent a_i with a great probability (i.e., $1 - 2^{-70}$). Thus, we require $\log_2(8 \cdot \frac{s}{\sqrt{2}})$ bits to represent $\Psi = (\frac{\widehat{m}}{g}) \cdot \mathcal{D}_s$. In other words, we require $n \cdot \log_2(8 \cdot \frac{s}{\sqrt{2}})$ bits to represent χ, where s is the deviation of error distribution.

Let ε represent successful advantage of distinguishing attack initiated by adversary. We set $w = \sqrt{\frac{\ln(\frac{2n}{\varepsilon})}{\pi}}$. Let $m = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_k^{e_k}$ be the complete prime factor factorization of m, then $\mathbf{rad}(m) = p_1 \cdot p_2 \cdot \cdots \cdot p_k$.

Therefore, $\mathbf{rad}(m)/m \leq 1$. We can obtain $\|g \cdot \mathbf{s}_i\|_2 \leq (r+1) \cdot \widehat{m} \cdot \sqrt{n}$ and $\|g \cdot \mathbf{r}_i\|_2 \leq (r+1) \cdot \widehat{m} \cdot \sqrt{n}$ hold with a probability of $(1 - 2^{-n})$ at least, respectively. Similarly, we have $r'^2 \leq r^2 + 2\pi$. Thus, according to lemma 3.1, we can set

$$q \geq 8 \cdot \sqrt{(s+1)^2 \cdot \widehat{m} \cdot n \cdot (s^2 + 2\pi) \cdot (3s^2 + 1) + \frac{\pi}{4}} \cdot w = O(\widehat{m} \cdot s^2 \cdot \sqrt{n}) \cdot w.$$

By Euler's phi function, we can get $n = \varphi(m) = \prod_{j=1}^{k} p_j^{e_j - 1} \cdot (p_j - 1) = m \cdot \prod_{j=1}^{k} (1 - \frac{1}{p_j})$. Since each $p_j \geq 2$, then $m = n \cdot \prod_{j=1}^{k} (1 - \frac{1}{p_j})^{-1} = O(n)$. When $\widehat{m}$ is odd, then $\widehat{m} = m$; when $\widehat{m}$ is even, then $\widehat{m} = m/2$. In short, we obtain $\widehat{m} = O(n)$. So we only need to set $q = O(\widehat{m} \cdot s^2 \cdot \sqrt{n}) \cdot w = \widetilde{O}(n^2)$. Combing with theorem 2.1, when $\lambda = 2$, the number of samples is $\lambda - 1 = 1$. We let the standard deviation r of Gaussian distribution $\mathcal{D}_s$ be $s = \xi \cdot q$, and let $\xi = \gamma \cdot (2n/\log_2(2n))^{1/4}$. To guarantee $\gamma \cdot q \geq \omega(\sqrt{\log_2 n})$, we set $s = (2n/\log_2(2n))^{1/4} \cdot \omega(\sqrt{\log_2 n})$. There exists a polynomial time (PT) quantum reduction from solving $\widetilde{O}(n^{2.5})$-approximating shortest vector problem on ideal lattice over R to solving Ring-$\mathrm{DLWE}_{q,\chi}$, given one sample from χ, where $\chi = \lfloor \Psi \rceil$, $\Psi = (\frac{\widehat{m}}{g}) \cdot D_{\xi \cdot q}$, and $\xi = \gamma \cdot (2n/\log_2(2n))^{1/4}$.

D. Security

Theorem III.3. *Let n be a power of 2, and let q be a prime satisfying $q \equiv 1 \mod 2n$. Then under the hard assumption $\mathbf{RLWE}_{q,\chi_s}$, our AKE protocol is secure in the Bellare-Rogaway model.*

IV. CONCLUSIONS

In this paper, we combine the reconciliation mechanism and representation method under the decoding basis to design a secure AKE protocol from lattices. Compared with the AKE protocol of Zhang *et al.* [5], each bit of the shared key negotiated in our improved AKE protocol is uniformly distributed. In addition, our modulus q is only taken a value of polynomial magnitude, rather than a sub-exponential modulus. Specially, we provide a new method that maps any bit string to certain element, which follows the discrete gaussian distribution over the cyclotomic number ring.

REFERENCES

[1] Bellare M, Rogaway P. Entity authentication and key distribution. In *13th Annual International Cryptology Conference*. Santa Barbara, CA, USA, Aug. 22-26, 1994, pp. 232-249.

[2] Fujioka A. Strongly secure authenticated key exchange from factoring, codes, and lattices. In *Proceedings of 15th International Conference and Theory in Public Key Cryptography.* Darmstadt, Gemany, May. 21-23, 2012, pp. 467-484.

[3] Ding J. A simple provably secure key exchange scheme based on the learning with errors problems. Cryptology ePrint Archive, Report 2012/688, 2012.(Available from: http://eprint.iacr.org/,) accessed on May. 1th 2014.

[4] Fujioka A. Practical and post-quantum authenticated key exchange from one-way secure key encapsulation mechanism. In *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security.* Hangzhou, China, May. 8-10, 2013, pp. 83-94.

[5] Zhang J, Zhang Z, Ding J, *et al.*. Authenticated key exchange from ideal lattices. In *Proceedings of 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Sofia, Bulgaria, April 26-30, 2015, Part II, Volume 9057, 2015, pp. 719-751.

[6] Peikert C. Lattice cryptography for the internet. In *Proceedings of the 6th International Workshop, Post-Quantum Cryptography*. Waterloo, ON, Canada, Oct. 1-3, 2014. pp. 197-219.

[7] Bos W. Post-quantum key exchange from ring learning with errors problem. Cryptology ePrint Archive, Report 2014/599, 2012.(Available from: http://eprint.iacr.org/,) accessed on Aug. 5th, 2014.

[8] Krawczyk H. HMQV: A high-performance secure diffie-hellman protocol. In *Proceedings of the 25th Annual International Cryptology Conference*. Santa Barbara, California USA, Aug. 14-18, 2005, pp. 546-566.

[9] Regev O. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM*. 2009, Volume 56(6): pp. 1-40.

[10] Lyubashevsky V, Peikert C, and Regev O. On ideal lattices and learning with errors over rings. In *Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Riviera, French, 2010. pp. 1-23.

[11] Lyubashevsky V, Peikert C, and Regev O. A toolkit for ring-LWE cryptography. In *Proceedings of the 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques.* Athens, Greece, 2013: 35-54.

[12] Lyubashevsky V. Lattice signatures without trapdoors. In *David Pointcheval and Thomas Johansson, editors, EUROCRYPT.* 2012. pp. 738-755.

[13] Barker E and Roginsky A. Recommendation for the entropy sources used for random bit generation. *Draft NIST Special Publication* 800-908, August 2012.

[14] Damgard I. Towards practical public key systems secure against chosen ciphertext attacks. In *Proceedings of Advances in Cryptology-CRYPTO '91*. Volume 576 of the series Lecture Notes in Computer Science. pp. 445-456.

[15] Bellare M, Palacio A. The knowledge-of-exponent assumptions and 3-round zero-knowledge protocols. In *Proceedings of 24th Annual International Cryptology Conference*. Santa Barbara, California, USA, August 15-19, 2004. Volume 3152 of the series Lecture Notes in Computer Science. pp. 273-289.

[16] Goldwasser S, Kalai Y.T., Peikert C, and Vaikuntanathan V. Robustness of the learning with errors assumption. In *Innovations in Computer Science.* 2010. pp. 230-240.

[17] Leo Ducas, Nguyen P.Q., Faster gaussian lattice sampling using lasy floating-point arithmetic. In *Proceedings of 18th International Conference on the Theory and Application of Cryptology and Information Security,* Beijing, China, December 2-6, 2012. Volume 7658 of the series Lecture Notes in Computer Science, 2012. pp. 415-432.

[18] Applebaum B, Cash D, *et al.* Fast cryptographic primitives and circular-secure encryption based on hard learning problems. *Advances in Cryptology-CRYPTO,* 2009. pp. 595-618.

[19] Gentry C, Vaikuntanathan V, *et al.* How to use a short basis: trapdoors for hard lattices and new cryptographic constructions. In *proceeding of the 40th Annual ACM Symposium on Theory of Computing,* Victoria BC, Canada, 2008. pp. 197-206.

[20] Peikert C. An efficient and parallel gaussian sampler for lattices. In *Proceedings of 30th Annual Cryptology Conference,* Santa Barbara, CA, USA, August 15-19, 2010. Volume 6223: 80-97.

[21] Micciancio D, Peikert C. Trapdoors for lattices: simpler, tighter, faster, smaller. In *proceeding of 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques,* Cambridge, UK, April 15-19, 2012. Volume 7237: 700-718.

[22] Applebaum B, Cash D, *et al.* Fast cryptographic primitives and circular-secure encryption based on hard learning problems. *Advances in Cryptology-CRYPTO,* 2009. pp. 595-618.

[23] Stehle D, Steinfeld R, *et al.* Efficient public key encryption based on ideal lattices. In *Proceedings of 15th International Conference on the Theory and Application of Cryptology and Information Security.* Tokyo, Japan, December 6-10, 2009. Volume 5912: 617-635.

[24] Lindner R, Peikert C. Better key sizes for LWE based encryption In *Proceedings of The Cryptographers' Track at the RSA Conference 2011.* San Francisco, CA, USA, February 14-18, 2011.

[25] Chen Y, Nguyen P.Q.. Better lattice security estimates. In *Proceedings of 17th International Conference on the Theory and Application of Cryptology and Information Security.* Seoul, South Korea, December 4-8, 2011.

[26] Ducas L, Durmus A, Lepoint T, and Lyubashevsky V. Lattice signatures and bimodal gaussians. In *Proceedings of 33rd Annual Cryptology Conference on Advances in Cryptology-CRYPTO,* Santa Barbara, CA, USA, August 18-22, 2013 LNCS 2013, Springer-Verlag: Berlin, Volume 8042: 40-56.

[27] Bellare M, Neven G. Multi-signatures in the plain public-key model and a general forking lemma. In *Proceedings of 13th ACM Symposium on Computer and Communications Security(CCS'2006).* Hilton Alexandria Mark Center, Alexandria, VA, U.S.A. Oct 30-Nov 3, 2006. pp. 390-399.