Robustly Secure Two-Party Authenticated Key Exchange from Ring-LWE

Xiaopeng Yang, Wenping Ma, and Chengli Zhang

Abstract

Using the hard assumption of Ring-Decision Learning With Errors (DLWE) in the lattice, we propose a new authenticated key exchange (AKE) scheme which is based on Peikert's reconciliation technique. Under the CK^{+} model, the proposed scheme is provably secure. Compared with the traditional Diffie-Hellman (DH) authenticated key exchange (AKE) schemes, the proposed scheme not only has better efficiency and stronger security but also resists quantum attacks because of the hard assumption on lattice problem. The comparisons between Ring-LWE based ones shows that the proposed scheme protects the shared session key with balanced key derivation function (KDF) compared with those current AKE schemes from LWE.

Index Terms

Cryptography, Authenticated key exchange, Lattices, Learning with errors, Robust extractor

I. Introduction

Authenticated Key Exchange (AKE) is an elementary cryptographical original, which not only permits participants to negotiate a common session key but also provides identity authentication between two parties. Generally speaking, every participant owns certain public information, namely a static public key (SPK), which is issued by a trusted third party, e.g., public key infrastructure (PKI), or certification authority (CA), and the homologous secret information, namely, a static secret key (SSK). During the

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, and zcl0719@163.com)

execution of the agreement, each participant first generates his own ephemeral secret key (ESK) and concomitant ephemeral public key, and exchanges the ephemeral public key (EPK). Then, each participant uses their static public keys, the static secret keys, the ephemeral public keys, and the ephemeral secret keys to compute certain session state. Finally, each participant derives a common session key by using a function named the key derivation function (KDF), namely, robust extractor. Bellare and Rogaway first presented a security model of AKE called BR model (Bellare *et al.*, 1994), which was based on the indistinguishability between the real common session key and any random key uniformly chosen from the same distribution. Menezes, Qu, and Vanstone put forward the MQV protocol (Menezes *et al.*, 1995). Due to its prominent security properties, the MQV protocol has been selected by National Security Agency (NSA) as the key exchange mechanism preferred to safeguard US government information. In 2001, Canetti and Krawcyk projected Canetti-Krawcyk (CK) security model (Canetti *et al.*, 2001). Moreover, it pointed that a combination of symmetrical encryption, message authentication code (MAC), and common session key contributes to build a secure channel for Internet. But Krawczyk (2005) pointed that the MQV protocol is not resistant to some attacks such as unknown key share (UKS) attacks, key compromise impersonation (KCI) attacks, and disclosure of DH exponents. Besides, the MQV protocol lacks perfect forward secrecy (PFS). Thus, he proposed HMQV protocol that is resistant to the above attacks. This protocol utilized the Exponential Challenge-Response Signatures to realize authentication. Krawczyk (2005) and Fujioka *et al.* (2012) independently programmed the satisfying CK^+ security model of AKE. In CK^+ model, the protocol not only achieves basic SK security and weak perfect forward security (wPFS), but also has resistance to KCI, and resistance to MEX.

Recently, cryptographic schemes based on lattices have appeared as a prospective replacement to more traditional ones based on the factoring and discrete logarithm problems. 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 n. Additionally, robust 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. Especially, public key encryptions from LWE (Lyubashevsky*et al.*, 2010; Benny*et al.*, 2009) and identity-based encryptions from LWE (Peikert *et al.*, 2008) are widely used.

Jin-tai Ding *et al.*(2012) proposed a simple provably secure key exchange from LWE. In order to eliminate the noises from the LWE problem, they use a signal function. Meanwhile, they give a multiparty key exchange protocol, which lacks its security analysis. We find out that using of the signal function would expose some information of the session key. Jiang Zhang *et al.*(2014) recently proposed an AKE from ideal lattices. In order to eliminate the noises from the LWE problem, they construct a characteristic function and a modular function. Given the characteristic function, the distribution of the modular function was not uniform, namely, it is not a balanced function. To make the output distribution of the modular function undistinguishable from uniform distribution, the modulus q is required to be large, namely, $q = 2^{\omega(\log n)}$.

This paper builds a new robustly secure AKE scheme via Ring-LWE. Our security analysis is based on the hard average-case problems Ring-$\mathrm{DLWE}_{q,\chi}$, which is at least as hard as $\widetilde{O}(\sqrt{n}/\gamma)$-approximate SIVP on ideal lattices in R.

By virtue of the design idea of HMQV protocol, we tactfully embed the identity authentication into the message transmission. Since only one party needs to extract the common session key with the robust extractor during the session computation, so our scheme can significantly improve the robustness and reduce the computational complexity, compared with other existing schemes from LWE.

How to evaluate the security of a cryptographic protocol is one of the important research matters. From the viewpoint of provably security, there are two methods to evaluate the security of a cryptographic protocol: One is the CK security model which is proposed by Canetti and Krawezyk (2001). The other one is the UC (Universally Composable) security model which is also presented by Canetti and Krawezyk (2002). The latter is always stronger than the former. The major difference between CK model and UC model originates from the cognition and characterization of the insider attacks to group key exchange protocols. The adoption of Non Information Oracle can reduce the UC security to the CK security. The adoption of some internal authentication technology can increase the CK security to the UC security. Thus, it is enough for this paper to consider the CK model.

II. Preliminaries

A. 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 algorithm A runs in polynomial time (PT) of λ, then it is efficient. If a function $f(\lambda) = o(n^{-c})$, 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.

B. Gaussian distribution on lattice

For arbitrary $\delta > 0$, the random variable X over $\mathbb{R}$ is called δ-subgaussian variable with parameter $r > 0$, if the moment-generating function satisfies $\mathrm{E}[\exp(2\pi t X)] \leq \exp(\delta) \cdot \exp(\pi r^2 t^2)$, for each $t \in \mathbb{R}$. By Markov's inequality, we obtain $\Pr[|X| \geq t] \leq 2\exp(\delta - x t^2/r^2)$, for each $t \geq 0$. For $r > 0$, the probability distribution function of the gaussian distribution $\mathcal{D}_r$ is $\exp(-\pi x^2/r^2)/r$.

Fact1 B-bounded center random variable is 0-subgaussian variable with parameter $B\sqrt{2\pi}$. If X_1 is a δ_1-subgaussian variable with parameter r_1, X_2 is a δ_2-subgaussian variable with parameter r_2, and X_1 and X_2 are independent of each other, then $X_1 + X_2$ is a $\delta_1 + \delta_2$-subgaussian variable with parameter $\sqrt{r_1^2 + r_2^2}$.

C. Cyclotomic field and cyclotomic ring

For positive integer m, let $K = \mathbb{Q}(\zeta_m)$ represent the m-th cyclotomic field, let $R = \mathbb{Z}[\zeta_m]$ represent the m-th cyclotomic ring, where ζ_m is an m order element. The unique monic polynomial $f(X) \in \mathbb{Q}[X]$

of minimal degree having ζ_m as root is called the m-th cyclotomic polynomial. Its complex roots are in the form of ω_m^i, where $i \in \mathbb{Z}_m^*, \omega_m = \exp(2\pi i/m) \in \mathbb{C}$. So, $[R:\mathbb{Z}] = \varphi(m), R \cong \mathbb{Z}[X]/(\Phi_m(X))$, where $\Phi_m(X) \in \mathbb{Z}[X]$. Specially, $\{\zeta_m^j\}_{j=0}^{\varphi(m)-1}$ is a $\mathbb{Z}$-basis of $R = \mathbb{Z}[\zeta_m]$. Let $g = \prod_{p|m}(1-\zeta_m^{m/p})$.

Definition1 (Regular embedding) Define $\sigma_i|_{\mathbb{Q}} : K \to \mathbb{C}$ via $\zeta_m \mapsto \omega_m^i$, the regular embedding is defined as $\sigma(e) = (\sigma_i(e))_{i \in \mathbb{Z}_m^*}$.

Definition2 (Norm) The norm is defined as $\|e\|_2 = (\sum_{i \in \mathbb{Z}_m^*} |\sigma_i(e)|^2)^{1/2}$, $\|e\|_\infty = \max_{i \in \mathbb{Z}_m^*} |\sigma_i(e)|$.

Consider the fractional codifferent ideal $R^\vee = (\widehat{m}/g)^{-1}R$, its specific $\mathbb{Z}$-basis is called the decoding basis. The encoding basis not only has the optimal error resilience but also allows the fast sample algorithm to be used to generate the error terms. Our scheme adopts the encoding basis of $R = (\widehat{m}/g) \cdot R^\vee$.

Lemma1 Assume $e \in \mathbb{Q}(\zeta_m)$ such that $g \cdot e$ is a δ-subgaussian variable with parameter $\widehat{m} \cdot r$. Let $e' \in \mathbb{Q}(\zeta_m)$, then each encoding basis coefficient of $e \cdot e'$ is a δ-subgaussian variable with parameter $r \cdot \|e\|_2$.

Lemma2 Let $e \leftarrow \chi_r$, where $\chi_r = \lfloor \varphi_r \rceil$, $\varphi_r = (\widehat{m}/g) \cdot \mathcal{D}_r$, then $g \cdot e$ is a δ-subgaussian variable with parameter $\widehat{m} \cdot \sqrt{r^2 + 2\pi \cdot \mathrm{rad}(m)/m}$, and $\|g \cdot e\|_2 \leq \widehat{m} \cdot (r + \sqrt{\mathrm{rad}(m)/m}) \cdot \sqrt{n}$ holds with at least $1 - 2^{-n}$ probability.

D. Hard problems in the lattice

Definition3 (Ring-LWE distribution) For $s \in R$, the distribution χ over R, a sample from the Ring-LWE distribution $A_{s,\chi}$ over $R_q \times R_q$ is to sample $a \leftarrow R_q$, $e \leftarrow \chi$ uniformly at random, outputting $(a, b = a \cdot s + e)$.

Definition4 (Average-case problem)The Ring-DLWE problem is with non-negligible probability to differentiate independent samples from $A_{s,\chi}$, where $s \in \chi$, and the same number of random samples from the uniform distribution over $R_q \times R_q$.

Definition5 (Worst-case problem) The shortest independent vector problem (SIVP) is to input a basis $\mathbf{B}$ of lattice, outputting n linearly independent vectors $\mathbf{S} \subset \mathcal{L}(\mathbf{B})$ satisfying $\|\mathbf{S}\| \leq poly(n) \cdot \lambda_1(\mathcal{L}(\mathbf{B}))$.

Theorem1 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 $q \equiv 1 \mod m$, $\gamma q \geq \omega(\sqrt{\log n})$. 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-DLWE$_{q,\chi}$, given $\lambda - 1$ samples from χ, where $\chi = \lfloor \varphi \rceil$, $\varphi = (\widehat{m}/g) \cdot \mathcal{D}_{\xi q}$, and $\xi = \gamma \cdot (n\lambda / \log(n\lambda))^{1/4}$.

III. CK$^+$ SECURITY MODEL

In this subsection, we review the CK$^+$ model. All the participants are regarded as probabilistic polynomial time (PPT) Turing machines.

Session. Let k be the security parameter. A positive integer $m = m(k)$ represents the max number of all the participants in our AKE scheme. Each participant has a static secret key and a homologous static public key, which are guaranteed via a certificate authority (CA), binding up with its identity. We say an implementation of protocol is a session. An influent message of the form (Π, I, i, j) or (Π, I, i, j, X_i) activates session. Π is the protocol identifier. I and R are role identifiers. i and j are participant identifiers. (Π, I, i, j) activates participant i, which is the session initiator. Participant i sends a message X_i to participant j. Participant j sends a message Y_j to participant i. After exchanging two-channel messages, participant i and participant j derive a session key, respectively.

Provided i is the initiator, then the session is denoted via $sid = (\Pi, I, i, j)$ or (Π, I, i, j, X_i, Y_j). Provided j is the responsor, then the session is denoted via $sid = (\Pi, R, j, i, X_i, Y_j)$. For $sid = (\Pi, *, i, j, *, *)$, the third coordinate represents the owner of sid, while the fourth one represents the peer of sid. Provided the owner of protocol computes the session key, then a session is completed. $sid = (\Pi, I, i, j, X_i, Y_i)$ matches $\overline{sid} = (\Pi, R, j, i, X_i, Y_i)$ and vice versa.

Freshness. Set $sid = (\Pi, I, i^*, j^*, X_i, Y_j)$ or $sid = (\Pi, R, j^*, i^*, X_i, Y_j)$ as a completed session. Suppose that the matching session exists, then set $\overline{sid}^*$ as the matching session of sid^*. sid^* is fresh provided the following situations satisfy:

-sid^* has not been sent a **SessionKeyReveal** query.

-Provided $\overline{sid}^*$ exists, it has not been queried from a **SessionKeyReveal** query.

-Provided $\overline{sid}^*$ does not exist, i^* and j^* have not been queried from a **Corrupt** query.

Adversary abilities. We regard an adversary $\mathcal{A}$ as a probabilistic polynomial time (PPT) Turing machine. $\mathcal{A}$ dominates the whole networks. Specifically, it can wiretap, change, cancel any data transfer, or add data. We permit the adversary to ask some oracles to acquire the relevant messages that are concerned with the session key and all participants' static secret keys. We define above mentioned oracles queries as follows:

$-\mathbf{Send}_0(\Pi, I, i, j)$: $\mathcal{A}$ activates participant i as an initiator, and acquires a message X_i, which is sent to participant j.

$-\mathbf{Send}_1(\Pi, R, j, i, X_i)$: $\mathcal{A}$ activates participant j as an responsor with X_i on behalf of participant i, and acquires a message Y_i, which is sent to participant i.

$-\mathbf{Send}_2(\Pi, I, i, j, X_i, Y_i)$: $\mathcal{A}$ sends Y_i to finish a session of i on behalf of j.

$-\mathbf{SessionKeyReveal}(sid)$: Once the session is finished, $\mathcal{A}$ acquires the session key sk of the session sid. Otherwise, this query terminates.

$\mathbf{SessionStateReveal}(sid)$: $\mathcal{A}$ obtains the session state (namely all ephemeral keys and intermediate computation results) of the owner of the session sid.

$-\mathbf{Corrupt}(i)$: Once $\mathcal{A}$ corrupts participant i, then $\mathcal{A}$ obtains the static secret key of participant i. In this case, participant i is dishonest. Otherwise, i is honest.

$-\mathbf{Test}(sid^*)$: We limit this query only on fresh session. $\mathcal{A}$ can send out query only once. After receiving this query, test oracle selects a bit $b \in_{\mathcal{R}} \{0, 1\}$, randomly. When $b = 1$, $\mathcal{A}$ obtains the session key of sid^*. Otherwise, it gets a random key, which is selected from the same distribution of the real key sk.

Experiment. We permit the adversary $\mathcal{A}$ to send any series of the above mentioned queries, however sends out only one **Test** query by a fresh session sid^*. Finally, $\mathcal{A}$ outputs a guess b' for b. When $b' = b$, $\mathcal{A}$ wins the game. We define the advantage of $\mathcal{A}$ as $\mathbf{Adv}_{\Pi,\mathcal{A}}^{AKE} = |\Pr[b' = b] - \frac{1}{2}|$.

Security. An AKE protocol is CK$^+$ secure provided the following situations satisfy:

-Provided two honest participants finish matching sessions, then they compute an identical session key with an overwhelming probability.

-For any PPT adversary $\mathcal{A}$, $\mathbf{Adv}_{\Pi,\mathcal{A}}^{AKE}$ is negligible in security parameter for the test session sid^*,

1. If $\overline{sid}^*$ exists, and the SSK of the owner of sid^* and the ESK of $\overline{sid}^*$ are given to $\mathcal{A}$.
2. If $\overline{sid}^*$ exists, and the ESK of the owner of sid^* and the ESK of $\overline{sid}^*$ are given to $\mathcal{A}$.
3. If $\overline{sid}^*$ exists, and the SSK of the owner of sid^* and the SSK of the peer of sid^* are given to $\mathcal{A}$.
4. If $\overline{sid}^*$ exists, and the ESK of sid^* and the SSK of the peer of sid^* are given to $\mathcal{A}$.
5. If $\overline{sid}^*$ does not exist, and the SSK of the owner of sid^* is given to $\mathcal{A}$.
6. If $\overline{sid}^*$ does not exist, and the ESK of the owner of sid^* is given to $\mathcal{A}$.

IV. Robustly secure authenticated key exchange based on ring-LWE

Before describing our AKE scheme, we first introduce some notations.

Definition 6 The modular rounding function $\lfloor\cdot\rceil_p : \mathbb{Z}_q \to \mathbb{Z}_p$ is defined by $x \mapsto \frac{p}{q}\cdot x$, where $p|q$.

Definition 7 The cross-rounding function $\langle\cdot\rangle_2 : \mathbb{Z}_q \to \mathbb{Z}_2$ is defined by $x \mapsto \lfloor \frac{4}{q}\cdot x \rfloor \mod 2$.

Lemma 3 For even modular q, if $v \in \mathbb{Z}_q$ is uniformly random, then $\lfloor v \rceil_2$ is randomly random given $\langle v \rangle_2$.

Definition 8 If v is close to w, $\lfloor v \rceil_2$ can be recovered given w and $\langle v \rangle_2$. Set $E = [-\frac{q}{8}, \frac{q}{8}) \bigcap \mathbb{Z}$, define the reconciliation function $\mathrm{rec} : \mathbb{Z}_q \times \mathbb{Z}_q \to \mathbb{Z}_2$ as follows: $\mathrm{rec}(w, b) = 0$, if $w \in \mathbf{I}_b + E \mod q$; $\mathrm{rec}(w, b) = 1$, otherwise.

Lemma 4 For even modular q, if $w = v + e \mod q$, $v \in \mathbb{Z}_q$,$e \in E$, then $\mathrm{rec}(w, \langle v \rangle_2) = \lfloor v \rceil_2$.

Definition 9 The randomization function $\mathrm{dbl} : \mathbb{Z}_q \to \mathbb{Z}_{2q}$ is defined via $v \mapsto \overline{v} = 2v - \overline{e}(\mod q)$, where $\overline{e} \in_{\mathcal{R}} \mathbb{Z}_2$, $\Pr[\overline{e} = 0] = \frac{1}{2}$, $\Pr[\overline{e} = -1] = \Pr[\overline{e} = 1] = \frac{1}{4}$. $\overline{e}$ in our scheme is 0-subgaussian with parameter $\sqrt{2\pi}$.

Lemma 5 For an odd modular q, if $v \in \mathbb{Z}_q$ is uniformly random, $\overline{v} \leftarrow \mathrm{dbl}(v) \in \mathbb{Z}_{2q}$, then $\lfloor v \rceil_2$ is uniformly random given $\langle \overline{v} \rangle_2$.

A. The scheme

Our AKE scheme is built over the cyclotomic field $R_q = \mathbb{Z}_q[X]/(\Phi_m(X))$. When q is odd, directly using of the modular rounding function will cause the calculated bits biased, namely, using of unbalanced robust extractor will expose some information of the shared session key. Thus, our scheme scales up the modular to extend the data. Concretely, let q be an odd prime modular satisfying $q \equiv 1 \mod m$ and $\gamma q \geq \omega(\sqrt{\log n})$. Let $\mathbf{P}_{\mathrm{A}} = a \cdot s_{\mathrm{A}} + e_{\mathrm{A}} \in R_q$ and $s_{\mathrm{A}} \in R_q$ be the static public key (SPK) and the static secret key (SSK) of A respectively, where $s_{\mathrm{A}}, e_{\mathrm{A}} \leftarrow \chi_r$. Let $\mathbf{P}_{\mathrm{B}} = a \cdot s_{\mathrm{B}} + e_{\mathrm{B}} \in R_q$ and $s_{\mathrm{B}} \in R_q$ be the SPK and the SSK of B respectively, where $s_{\mathrm{B}}, e_{\mathrm{B}} \leftarrow \chi_r$. Let $H(\cdot) : \{0,1\}^* \rightarrow \chi_r$, which maps a string into a sample in χ_r. More specifically, one can first hash the inputs to certain random string via using SHA-2, and then use it as the randomness to sample a vector (or a ring element) from χ_r.

Our scheme uses the reconciliation technique to generate the session state for two parties and extract the shared session key for one of the parties, which not only is different from existing bilateral extracting mode but also obviously reduces computational complexity. Suppose that $D = d_j$ is the decoding basis. Let $v = \sum_j v_j d_j$, where $v_j \in \mathbb{Z}_q$, then $\lfloor v \rceil_2 = \sum_j \lfloor v_j \rceil_2 \cdot d_j \in R_2$, $\langle v \rangle_2 = \sum_j \langle v_j \rangle_2 \cdot d_j$. Let $w = \sum_j w_j \cdot d_j$, $b = \sum_j b_j \cdot d_j$. Our scheme applies the randomization function to act on each coefficient of the encoding basis. Choose $\psi = (\widehat{m}/g) \cdot D_r$, where $\widehat{m}/g$ corresponds to the transform $R^\vee \rightarrow R$. Then, our scheme processes the distribution ψ with the discrete way $\chi_r = \lfloor \psi \rceil$. Specifically, we round each vector of the encoding basis to the nearest rational integer via selecting $a \in K$ from the distribution ψ. We first reconcile $2w \in R_q$ so as to reconcile $w \in R_q$. The specific scheme is given as follows:

Initiation : Party A first computes $x_{\mathrm{A}} = a \cdot r_{\mathrm{A}} + f_{\mathrm{A}} \in R_q$, where $r_{\mathrm{A}}, f_{\mathrm{A}} \leftarrow \chi_r$, and then sends x_{A} to party B.

Response : After receiving x_{A}, party B computes $y_{\mathrm{B}} = a \cdot r_{\mathrm{B}} + f_{\mathrm{B}} \in R_q$, where $r_{\mathrm{B}}, f_{\mathrm{B}} \leftarrow \chi_r$, $d = H(x_{\mathrm{A}}, \mathrm{B})$, $e = H(y_{\mathrm{B}}, \mathrm{A})$. Then, it computes $\sigma_{\mathrm{B}} = g \cdot (x_{\mathrm{A}} + d \cdot \mathbf{P}_{\mathrm{A}}) \cdot (r_{\mathrm{B}} + e \cdot s_{\mathrm{B}})$, $\overline{v}_{\mathrm{B}} = \mathrm{dbl}(\sigma_{\mathrm{B}})$, $v_{\mathrm{B}} = \langle \overline{\sigma}_{\mathrm{B}} \rangle_2$, and $SK_{\mathrm{B}} = \lfloor \overline{v}_{\mathrm{B}} \rceil_2$. Finally, it sends y_{B} and v_{B} to party A, and takes SK_{B} as its session key.

Completion : After receiving y_{B} and v_{B}, party A computes $\sigma_{\mathrm{A}} = g \cdot (y_{\mathrm{B}} + e \cdot \mathbf{P}_{\mathrm{B}}) \cdot (r_{\mathrm{A}} + d \cdot s_{\mathrm{A}})$ and

$\mathrm{rec}(\sigma_{\mathrm{A}}, v_{\mathrm{B}}) = SK_{\mathrm{A}}$, and then takes SK_{A} as its session key.

B. Correctness

Lemma 6 Suppose $\|g \cdot s_i\|_2 \leq \ell$, $\|g \cdot r_i\|_2 \leq \ell$, where $i = \mathrm{A}, \mathrm{B}$, and

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

where $w > 0$, $r' = \sqrt{r^2 + 2\pi \cdot \mathrm{rad}(m)/m}$, then $SK_{\mathrm{A}} = SK_{\mathrm{B}}$ holds with probability at least $1 - 2n \cdot \exp(8\delta - \pi w^2)$, where $\delta \geq 2^{-n}$.

Proof It is obtained by calculating that $\sigma_{\mathrm{A}} = \sigma_{\mathrm{B}} + g \cdot [d \cdot f_{\mathrm{B}} \cdot s_{\mathrm{A}} + e \cdot e_{\mathrm{B}} \cdot r_{\mathrm{A}} - d \cdot e_{\mathrm{A}} \cdot r_{\mathrm{B}} - e \cdot f_{\mathrm{A}} \cdot s_{\mathrm{B}} + d \cdot e \cdot (s_{\mathrm{A}} \cdot e_{\mathrm{B}} - s_{\mathrm{B}} \cdot e_{\mathrm{A}})] + g \cdot (f_{\mathrm{B}} \cdot r_{\mathrm{A}} - f_{\mathrm{A}} \cdot r_{\mathrm{B}})$. Set $e_1 = g \cdot [d \cdot f_{\mathrm{B}} \cdot s_{\mathrm{A}} + e \cdot e_{\mathrm{B}} \cdot r_{\mathrm{A}} - d \cdot e_{\mathrm{A}} \cdot r_{\mathrm{B}} - e \cdot f_{\mathrm{A}} \cdot s_{\mathrm{B}} + d \cdot e \cdot (s_{\mathrm{A}} \cdot e_{\mathrm{B}} - s_{\mathrm{B}} \cdot e_{\mathrm{A}})] + g \cdot (f_{\mathrm{B}} \cdot r_{\mathrm{A}} - f_{\mathrm{A}} \cdot r_{\mathrm{B}})$. Let $\overline{e}_1 \in R$ be the random element chosen in $\overline{\sigma}_{\mathrm{B}} \leftarrow \mathrm{dbl}(\sigma_{\mathrm{B}})$. Then, we obtain $\overline{\sigma}_{\mathrm{B}} = 2\sigma_{\mathrm{B}} - \overline{e}_1 \in R_{2q}$. By lemma 4, it suffices to prove that each encoding basis coefficient of $2e_1 + \overline{e}_1$ falls into $[-\frac{q}{4}, \frac{q}{4})$, then $g \cdot f_{\mathrm{B}}$ is δ-subgaussian variable with parameter $\widehat{m} \cdot r'$, where $r' = \sqrt{r^2 + 2\pi \cdot \mathrm{rad}(m)/m}$ by lemma 2.

Since $\|g \cdot s_{\mathrm{A}}\|_2 \leq \ell$, then each encoding basis coefficient of $g \cdot s_{\mathrm{A}} \cdot f_{\mathrm{B}}$ is δ-subgaussian with parameter $r' \cdot \ell$ by lemma 1. By lemma 2, each encoding basis coefficient of $g \cdot d$ is δ-subgaussian with parameter $\widehat{m} \cdot r'$. Since $\|g \cdot s_{\mathrm{A}} \cdot f_{\mathrm{B}}\|_2 \leq \|g \cdot s_{\mathrm{A}}\|_2 \cdot \|f_{\mathrm{B}}\|_\infty \leq \ell \cdot r\sqrt{n}$ holds with probability at least $1 - 2^{-n}$. By lemma 1, each encoding basis coefficient of $g \cdot d \cdot s_{\mathrm{A}} \cdot f_{\mathrm{B}}$ is δ-subgaussian with parameter $\ell \cdot r' \cdot r\sqrt{n}$. Similarly, we obtain that each encoding basis coefficient of $g \cdot d \cdot e_{\mathrm{B}} \cdot r_{\mathrm{A}}$, $g \cdot d \cdot e_{\mathrm{A}} \cdot r_{\mathrm{B}}$ and $g \cdot d \cdot f_{\mathrm{A}} \cdot s_{\mathrm{B}}$ is δ-subgaussian with parameter $\ell \cdot r' \cdot r\sqrt{n}$, respectively.

We have known that each encoding basis coefficient of $g \cdot d$ is δ-subgaussian with parameter $\widehat{m} \cdot r'$ and $\|g \cdot e \cdot s_{\mathrm{A}} \cdot e_{\mathrm{B}}\|_2 \leq \|g \cdot s_{\mathrm{A}} \cdot e_{\mathrm{B}}\|_2 \cdot \|e\|_\infty \leq \ell \cdot r\sqrt{n} \cdot r\sqrt{n} = \ell \cdot r^2 \cdot n$. By lemma 1, each encoding basis coefficient of $g \cdot d \cdot e \cdot s_{\mathrm{A}} \cdot e_{\mathrm{B}}$ is δ-subgaussian with parameter $r' \cdot \ell \cdot r^2 \cdot n$. By lemma 2, each coefficient of $g \cdot f_{\mathrm{B}}$ is δ-subgaussian with parameter $\widehat{m} \cdot r'$. Since $\|g \cdot r_{\mathrm{A}}\|_2 \leq \ell$, each encoding basis coefficient of $g \cdot f_{\mathrm{B}} \cdot r_{\mathrm{A}}$ is δ-subgaussian with parameter $r' \cdot \ell$ by lemma 1. Similarly, each coefficient of $g \cdot f_{\mathrm{B}} \cdot r_{\mathrm{A}}$ is δ-subgaussian with parameter $r' \cdot \ell$.

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 $2\sqrt{2} \cdot \sqrt{[\ell^2 \cdot r'^2 \cdot (3r^2 + n) + 1 + \frac{\pi}{4}]}$. By Markov's inequality and the union bound over all n coefficients, it naturally proves this lemma.

C. Choices of parameters

Since $\mathrm{rad}(m)/m \leq 1$, then $\|g \cdot s_A\|_2 \leq (r+1) \cdot \widehat{m} \cdot \sqrt{n}$, $\|g \cdot s_B\|_2 \leq (r+1) \cdot \widehat{m} \cdot \sqrt{n}$, $\|g \cdot r_A\|_2 \leq (r+1) \cdot \widehat{m} \cdot \sqrt{n}$, $\|g \cdot r_B\|_2 \leq (r+1) \cdot \widehat{m} \cdot \sqrt{n}$. Moreover, because of $r'^2 \leq r^2 + 2\pi$, we take $w = \sqrt{\log(2n/\varepsilon)/\pi}$, $\widehat{m} = O(n)$, $\varepsilon = 2^{-256}$, $q = O(r^2 \cdot n^{3/2} \cdot \ln n)$. Consider the simplest case, namely, $\lambda = 2$, let $r = \xi q$, where $\xi = \gamma \cdot [2n/\log(2n)]^{1/4}$ satisfying $\gamma \cdot q \geq \omega(\sqrt{\log n})$. Now we have that Ring-DLWE$_{q,\chi}$ is difficult, supposing that SIVP on ideal lattice in R is difficult to approximate to within $\widetilde{O}(\sqrt{n}/\gamma) = \widetilde{O}(q \cdot \sqrt{n}) = \widetilde{O}(n^{2.5})$.

V. Security analysis

In CK$^+$ model, let sid^* be the session identifier of the test session. Let n be the security parameter. Let $\mathcal{A}$ be the adversary. Suc represents the event that the adversary wins.

A. Event $\mathbf{E}_1 \bigwedge Suc$

Let $\mathbf{E}_1$ represent the event that the test session sid^* has matching session $\overline{sid}^*$, the owner of sid^* is the initiator, and the SSK of the initiator is given to $\mathcal{A}$.

$Simulation.$ We alter the computation of the session key over four hybrid games. $\mathbf{G}_{1,x}$ represents these games and $Adv(\mathcal{A}, \mathbf{G}_{1,x})$ represents the advantage of $\mathcal{A}$ wins in the game $\mathbf{G}_{1,x}$, where $x = 1, 2, 3, 4$.

$\mathbf{G}_{1,0}$: The adversary $\mathcal{A}$ chooses $sid^* = (\Pi, I, \mathrm{A}^*, \mathrm{B}^*, x_{\mathrm{A}^*}, (y_{\mathrm{B}^*}, v_{\mathrm{B}^*}))$ to be the test session, where x_{A^*} is the session output of A^*, and y_{B^*} is the session output of B^* activated by $\mathbf{Send}_1(\Pi, R, \mathrm{B}^*, \mathrm{A}^*, x_{\mathrm{A}^*})$. Then, the simulator $\mathcal{S}$ randomly selects $a \in R_q$, honestly generates both the static public keys for two parties, and simulates the attack environment for $\mathcal{A}$. $\mathcal{S}$ maintains two tables L and L_{sk} for the random oracle $H(\cdot)$ and $\mathbf{SessionKeyReveal}$ respectively, and answers the following queries from $\mathcal{A}$.

$H(\cdot)$: If there is no (in, out) in L, then $\mathcal{S}$ randomly selects $out \in \chi_r$, and adds (in, out) into L. Then, it returns out to $\mathcal{A}$.

$\mathbf{Send}_0(\Pi, I, \mathrm{A}, \mathrm{B})$: $\mathcal{A}$ initiates a new session from A to B. $\mathcal{S}$ randomly selects $r_{\mathrm{A}}, f_{\mathrm{A}} \leftarrow \chi_r$, and returns $x_{\mathrm{A}} = a \cdot r_{\mathrm{A}} + f_{\mathrm{A}} \in R_q$ to $\mathcal{A}$.

$\mathbf{Send}_1(\Pi, R, \mathrm{B}, \mathrm{A}, x_{\mathrm{A}})$: $\mathcal{S}$ randomly selects $r_{\mathrm{B}}, f_{\mathrm{B}} \leftarrow \chi_r$, and computes $y_{\mathrm{B}} = a \cdot r_{\mathrm{B}} + f_{\mathrm{B}} \in R_q, \sigma_{\mathrm{B}}, \overline{v}_{\mathrm{B}}, v_{\mathrm{B}}$ and SK_{B}. Finally, it returns $(y_{\mathrm{B}}, v_{\mathrm{B}})$ to $\mathcal{A}$.

$\mathbf{Send}_2(\Pi, I, \mathrm{A}, \mathrm{B}, x_{\mathrm{A}}, (y_{\mathrm{B}}, v_{\mathrm{B}}))$: $\mathcal{S}$ computes $\sigma_{\mathrm{A}}, SK_{\mathrm{A}}$ according to the scheme.

$\mathbf{SessionKeyReveal}(sid)$: Let $sid = (\Pi, *, \mathrm{A}, *, *, *, *)$, $\mathcal{S}$ returns SK_{A} to $\mathcal{A}$, if the session key of sid is generated. If there is no (in, out) in L_{sk}, then $\mathcal{S}$ randomly selects $out \in \{0,1\}^n$, and it adds (in, out) into L_{sk}. Then, returns out to $\mathcal{A}$.

$\mathbf{Corrupt}(\mathrm{A})$: $\mathcal{S}$ returns s_{A} to $\mathcal{A}$.

$\mathbf{Test}(sid)$: If $(\mathrm{A}, \mathrm{B}) \neq (\mathrm{A}^*, \mathrm{B}^*)$, or x_{A} is not the session output of A^*, and y_{B} is not the session output of B^*, then $\mathcal{S}$ aborts. Otherwise, $\mathcal{S}$ randomly selects $b \in \{0,1\}, SK'_{\mathrm{A}} \in \{0,1\}^n$. If $b = 0$, then $\mathcal{S}$ returns SK'_{A}. Otherwise, $\mathcal{S}$ returns the real session key of sid.

$\mathbf{G}_{1,1}$: $\mathcal{S}$ computes $y'_{\mathrm{B}} = a \cdot r'_{\mathrm{B}} + f'_{\mathrm{B}}$, where $r'_{\mathrm{B}}, f'_{\mathrm{B}} \leftarrow \chi_r$. Then, $\mathcal{S}$ behaves almost identically as in $\mathbf{G}_{1,0}$, except during $\mathbf{Send}_1$, if $(\mathrm{A}, \mathrm{B}) \neq (\mathrm{A}^*, \mathrm{B}^*)$, or y'_{B} is not the session output of $\mathbf{B}^*$, then $\mathcal{S}$ behaves identically as in $\mathbf{G}_{1,0}$. Otherwise, $\mathcal{S}$ randomly selects $e \leftarrow \chi_r$, computes $y_{\mathrm{B}} = y'_{\mathrm{B}} - e \cdot \mathbf{P}_{\mathrm{B}}$. If there is $(\mathrm{A}, y_{\mathrm{B}})$ in L, then $\mathcal{S}$ aborts. Otherwise, it adds $(\mathbf{A}, y_{\mathrm{B}})$ into L, computes $\sigma_{\mathrm{B}} = g \cdot (x_{\mathrm{A}} + d \cdot \mathbf{P}_{\mathrm{A}}) \cdot r'_{\mathrm{B}}$. Finally, it honestly computes $\overline{v}_{\mathrm{B}}, v_{\mathrm{B}}, SK_{\mathrm{B}}$ according to the scheme, and sends $(y_{\mathrm{B}}, v_{\mathrm{B}})$ to $\mathcal{A}$.

$\mathbf{G}_{1,2}$: $\mathcal{S}$ computes $x'_{\mathrm{A}} = a \cdot r'_{\mathrm{A}} + f'_{\mathrm{A}}$, where $r'_{\mathrm{A}}, f'_{\mathrm{A}} \leftarrow \chi_r$. Then, it behaves almost identically as in $\mathbf{G}_{1,1}$, except during $\mathbf{Send}_0$, if $(\mathrm{A}, \mathrm{B}) \neq (\mathrm{A}^*, \mathrm{B}^*)$, or x'_{A} is not the session output of A^*, then $\mathcal{S}$ behaves identically as in $\mathbf{G}_{1,1}$. Otherwise, it randomly selects $d \leftarrow \chi_r$, and computes $x_{\mathrm{A}} = x'_{\mathrm{A}} - d \cdot \mathbf{P}_{\mathrm{A}}$. If there is $(\mathrm{B}, x_{\mathrm{A}})$ in L, then $\mathcal{S}$ aborts. Otherwise, it adds $(\mathrm{B}, x_{\mathrm{A}})$ into L. Finally, it returns x_{A} to A. During $\mathbf{Send}_2$, $\mathcal{S}$ behaves identically with in $\mathbf{G}_{1,1}$. Otherwise, if $(y_{\mathrm{B}}, v_{\mathrm{B}})$ is not the session output of B^*, then let SK_{B} be the session key of sid. $\mathcal{S}$ sets $SK_{\mathrm{A}} = SK_{\mathrm{B}}$. Otherwise, $\mathcal{S}$ computes $\sigma_{\mathrm{A}} = g \cdot (y_{\mathrm{B}} + e \cdot \mathbf{P}_{\mathrm{B}}) \cdot r'_{\mathrm{A}}$. Finally, it honestly computes $SK_{\rm A}$ according to the scheme.

$\mathbf{G}_{1,3}$: $\mathcal{S}$ randomly selects $x'_{\rm A} \in R_q$, behaves almost identically as in $\mathbf{G}_{1,2}$, except during $\mathbf{Send}_2$, if $({\rm A},{\rm B}) \neq ({\rm A}^*,{\rm B}^*)$, or $x_{\rm A}$ is not the session output of ${\rm A}^*$ and $(y_{\rm B},\sigma_{\rm B})$ is not the session output of ${\rm B}^*$, then $\mathcal{S}$ behaves identically as in $\mathbf{G}_{1,2}$. Otherwise, it randomly selects $SK_{\rm A} \leftarrow \{0,1\}^n$ as the session key.

$\mathbf{G}_{1,4}$: $\mathcal{S}$ randomly selects $y'_{\rm B} \leftarrow R_q$, and behaves identically as in $\mathbf{G}_{1,3}$, except during $\mathbf{Send}_1$, if $({\rm A},{\rm B}) \neq ({\rm A}^*,{\rm B}^*)$, or $y'_{\rm B}$ is not the session output of ${\rm B}^*$, then it answers queries identically as in $\mathbf{G}_{1,3}$. Otherwise, it randomly selects $e \leftarrow \chi_R$, and computes $y_{\rm B} = y'_{\rm B} - e \cdot \mathbf{P}_{\rm B}$. If there is $({\rm A}, y_{\rm B})$ in L, then $\mathcal{S}$ aborts. Otherwise, it adds $({\rm A}, y_{\rm B})$ into L. Then, it randomly selects $\sigma_{\rm B} \leftarrow R_q$, and computes $\overline{v}_{\rm B}, v_{\rm B}$. If A has queried $\mathbf{SessionKeyReveal}$, then $\mathcal{S}$ aborts. Otherwise, $\mathcal{S}$ randomly selects $SK_{\rm B} \in \{0,1\}^n$, and sets $\lfloor \overline{v}_{\rm B} \rceil_2 = SK_{\rm B}$. Finally, $\mathcal{S}$ sends $(y_{\rm B},\sigma_{\rm B})$ to $\mathcal{A}$.

$Analysis.$ $(a, y'_{\rm B} = a \cdot r'_{\rm B} + f'_{\rm B})$ is a Ring-LWE group, where $r'_{\rm B}, f'_{\rm B} \leftarrow \chi_r$. Since the distribution of $y'_{\rm B}$ is indistinguishable from the uniform distribution over R_q, then the probability of the event that $\mathcal{A}$ correctly guesses $y_{\rm B} = y'_{\rm B} - e \cdot \mathbf{P}_{\rm B}$ is negligible. Since $\mathbf{P}_{\rm B} = a \cdot s_{\rm B} + e_{\rm B} \in R_q$, then $y_{\rm B} = a \cdot (r'_{\rm B} - e \cdot s_{\rm B}) + (f'_{\rm B} - e \cdot e_{\rm B})$.The distribution of $r'_{\rm B} - e \cdot s_{\rm B}$ and that one of $f'_{\rm B} - e \cdot e_{\rm B}$ is close to χ_r respectively. The distribution of $y_{\rm B}$ in $\mathbf{G}_{1,1}$ is close to that one of $y_{\rm B}$ in $\mathbf{G}_{1,0}$. Assume $\gamma \cdot q \geq \omega(\sqrt{\log n})$, and Ring-DLWE$_{q,\chi}$ is hard, then we obtain $|Adv(\mathcal{A}, \mathbf{G}_{1,1}) - Adv(\mathcal{A}, \mathbf{G}_{1,0})| \leq negl$.

The distribution of $x_{\rm A}$ in $\mathbf{G}_{1,2}$ is close to that in $\mathbf{G}_{1,1}$. The probability of the event that $\mathcal{A}$ quires $H(\cdot)$ with $x_{\rm A}$ is negligible. The probability of the event that $\mathcal{S}$ aborts in $\mathbf{G}_{1,2}$ is close to that one in $\mathbf{G}_{1,1}$. So we obtain $|Adv(\mathcal{A}, \mathbf{G}_{1,2}) - Adv(\mathcal{A}, \mathbf{G}_{1,1})| \leq negl$.

The real session key $SK_{\rm A}$ in $\mathbf{G}_{1,2}$ is replaced by a randomly chosen key in $\mathbf{G}_{1,3}$. By lemma 5, if $\sigma_{\rm B}$ is uniformly random, then $\lfloor \overline{\sigma}_{\rm B} \rceil_2$ is uniformly random given $\langle \overline{\sigma}_{\rm B} \rangle_2$. $\mathcal{A}$ cannot differentiate the view of $\mathbf{G}_{1,3}$ and that one of $\mathbf{G}_{1,2}$, namely, $|Adv(\mathcal{A}, \mathbf{G}_{1,3}) - Adv(\mathcal{A}, \mathbf{G}_{1,2})| \leq negl$.

Under the Ring-DLWE$_{q,\chi}$ assumption, $\mathbf{G}_{1,4}$ and $\mathbf{G}_{1,3}$ are computationally indistinguishable. Let (α_1, β_1) and (α_2, β_2) be two Ring-DLWE challenge groups. Assume that there exists a adversary that can differentiate $\mathbf{G}_{1,4}$ and $\mathbf{G}_{1,3}$, then we can construct a distinguisher $\mathcal{D}$ that can solve the Ring-DLWE problem. Concretely, $\mathcal{D}$ first sets the public parameters $\alpha_1 = a, \alpha_2 = s_{\mathrm{B}}, \beta_1 = y'_{\mathrm{B}}$. Then, $\mathcal{D}$ behaves identically with in $\mathbf{G}_{1,3}$, except during $\mathbf{Send}_1$, if $(\mathrm{A}, \mathrm{B}) \neq (\mathrm{A}^*, \mathrm{B}^*)$, or y'_{B} is not the session output of B^*, then $\mathcal{D}$ answers queries identically as in $\mathbf{G}_{1,3}$. Otherwise, $\mathcal{D}$ randomly selects $e \leftarrow \chi_r$, and computes $y_{\mathrm{B}} = y'_{\mathrm{B}} - e \cdot \mathbf{P}_{\mathrm{B}}$. if there is $(y_{\mathrm{B}}, \mathrm{A})$ in L, then $\mathcal{D}$ aborts. Otherwise, $\mathcal{D}$ adds $(y_{\mathrm{B}}, \mathrm{A})$ into L. Then, $\mathcal{D}$ computes $\sigma_{\mathrm{B}} = g \cdot x'_{\mathrm{A}}(r_{\mathrm{B}} + e \cdot s_{\mathrm{B}})$, and it sets $\beta_2 = r_{\mathrm{B}} + e \cdot s_{\mathrm{B}}$. Since $x'_{\mathrm{A}} \leftarrow_{\mathcal{R}} R_q$, then the distribution of β_2 is computationally indistinguishable with the uniform distribution over R_q. Thus, the distribution of σ_{B} is computationally indistinguishable with the uniform distribution over R_q. Let $(y_{\mathrm{B}}, v_{\mathrm{B}})$ be the session output of $\mathrm{B} = \mathrm{B}^*$. Let $(y_{\mathrm{B}}, v'_{\mathrm{B}})$ be the session information of $\mathrm{A} = \mathrm{A}^*$, which is used to accomplish the test session. In $\mathbf{G}_{1,4}$, $\sigma_{\mathrm{B}} \leftarrow R_q$ which is chosen randomly is independent of both public keys, except $\overline{v}_{\mathrm{B}}$. We use $q_{1,x}$ to represent that $\mathcal{A}$ makes a $\mathbf{SessionKeyReveal}$ query in $\mathbf{G}_{1,x}$.

If $v_{\mathrm{B}} = v'_{\mathrm{B}}$, then $SK_{\mathrm{A}} = \mathrm{rec}(\sigma_{\mathrm{A}}, v_{\mathrm{B}}) = \lfloor \overline{v}_{\mathrm{B}} \rceil_2 = SK_{\mathrm{B}}$. In $\mathbf{G}_{1,4}$, σ_{B} is randomly selected from the uniform distribution over R_q. By lemma 5, $\mathcal{A}$ cannot differentiate the view of $\mathbf{G}_{1,4}$ and that of $\mathbf{G}_{1,3}$. If $v_{\mathrm{B}} \neq v'_{\mathrm{B}}$, then $q_{1,4}$ does not happen. In all, we obtain $|Adv(\mathcal{A}, \mathbf{G}_{1,4}|\neg q_{1,4}) - Adv(\mathcal{A}, \mathbf{G}_{1,3}|\neg q_{1,3})| \leq negl$. Since all the information are completely randomized in $\mathbf{G}_{1,4}$, then we obtain $Adv(\mathcal{A}, \mathbf{G}_{1,4}) = 0$. Thus, we obtain $\Pr[\mathbf{E}_1 \bigwedge Suc] = 0$.

B. Event $\mathrm{E}_2 \bigwedge Suc$

Let $\mathbf{E}_2$ represent the event that the test session sid^* has no matching session $\overline{sid}^*$, the owner of sid^* is the initiator, and the ephemeral key of the initiator is given to $\mathcal{A}$.

Simulation. We alter the computation of the session key over seven hybrid games. $\mathbf{G}_{2,x}$ represents these games and $Adv(\mathcal{A}, \mathbf{G}_{2,x})$ represents the advantage of $\mathcal{A}$ wins in the game $\mathbf{G}_{2,x}$, where $x = 1, 2, 3, 4, 5, 6, 7$.

$\mathbf{G}_{2,0}$: It is identical with $G_{1,0}$.

$\mathbf{G}_{2,1}$: $\mathcal{S}$ behaves identically as in $\mathbf{G}_{2,0}$, except during $\mathbf{Send}_0(\Pi, I, \mathrm{A}, \mathrm{B})$, if $\mathrm{A} \neq \mathrm{B}^*$, then $\mathcal{S}$ answers queries identically as in $G_{2,1}$. Additionally, it computes $x'_{\mathrm{A}} = a \cdot r'_{\mathrm{A}} + f'_{\mathrm{A}}$, where $r'_{\mathrm{A}}, f'_{\mathrm{A}} \leftarrow \chi_r$. Then, $\mathcal{S}$ randomly selects $d \leftarrow \chi_r$, and computes $x_{\mathrm{A}} = x'_{\mathrm{A}} - d \cdot \mathbf{P}_{\mathrm{A}}$. If there is $(\mathrm{B}, x_{\mathrm{A}})$ in L, then $\mathcal{S}$ aborts. Otherwise, it adds $(\mathrm{B}, x_{\mathrm{A}})$ into L, and returns x_{A} to $\mathcal{A}$. During $\mathbf{Send}_1$, if $\mathrm{B} \neq \mathrm{B}^*$, then $\mathcal{S}$ answers queries identically as in $\mathbf{G}_{2,0}$. In addition, it computes $y'_{\mathrm{B}} = a \cdot r'_{\mathrm{B}} + f'_{\mathrm{B}}$, where $r'_{\mathrm{B}}, f'_{\mathrm{B}} \leftarrow \chi_r$. Then, $\mathcal{S}$ randomly selects $e \leftarrow \chi_r$, and computes $y_{\mathrm{B}} = y'_{\mathrm{B}} - e \cdot \mathbf{P}_{\mathrm{B}}$. If there is $(\mathrm{A}, y_{\mathrm{B}})$ in L, then $\mathcal{S}$ aborts. Otherwise, it adds $(\mathrm{A}, y_{\mathrm{B}})$ into L, and computes $\sigma_{\mathrm{B}} = g \cdot (x_{\mathrm{A}} + d \cdot \mathbf{P}_{\mathrm{A}}) \cdot r'_{\mathrm{B}}$. Finally, $\mathcal{S}$ computes $\overline{v}_{\mathrm{B}}, v_{\mathrm{B}}, SK_{\mathrm{B}}$ according to the protocol, and sends $(y_{\mathrm{B}}, v_{\mathrm{B}})$ to $\mathcal{A}$. During $\mathbf{Send}_2$, if $\mathrm{A} \neq \mathrm{B}^*$, then $\mathcal{S}$ answers quires identically as in $\mathbf{G}_{2,1}$. Otherwise, let $x_{\mathrm{A}} = x'_{\mathrm{A}} - d \cdot \mathbf{P}_{\mathrm{A}}$, where $x'_{\mathrm{A}} = a \cdot r'_{\mathrm{A}} + f'_{\mathrm{A}}$, $\mathcal{S}$ computes $\sigma_{\mathrm{A}} = g \cdot (y_{\mathrm{B}} + e \cdot \mathbf{P}_{\mathrm{B}}) \cdot r'_{\mathrm{A}}$. Finally, it computes SK_{A} according to the scheme.

$\mathbf{G}_{2,2}$: $\mathcal{S}$ behaves identically as in $\mathbf{G}_{2,1}$, except that it replaces the public key in $\mathbf{G}_{2,1}$ with $\mathbf{P}_{\mathrm{B}^*}$ which is uniformly chosen in $\mathbf{G}_{2,2}$.

$\mathbf{G}_{2,3}$: $\mathcal{S}$ computes $x'_{\mathrm{A}} = a \cdot r'_{\mathrm{A}} + f'_{\mathrm{A}}$, where $r'_{\mathrm{A}}, f'_{\mathrm{A}} \leftarrow \chi_r$. Then, $\mathcal{S}$ behaves almost identically as in $\mathbf{G}_{2,2}$, except during $\mathbf{Send}_0$, if $(\mathrm{A}, \mathrm{B}) \neq (\mathrm{A}^*, \mathrm{B}^*)$, or x^*_{A} is not the session output of A^*, then $\mathcal{S}$ answers quires identically as in $\mathbf{G}_{2,2}$. Otherwise, $\mathcal{S}$ randomly selects $d \leftarrow \chi_r$, and computes $x_{\mathrm{A}} = x'_{\mathrm{A}} - d \cdot \mathbf{P}_{\mathrm{A}}$. If there is $(\mathrm{B}, x_{\mathrm{A}})$ in L, then $\mathcal{S}$ aborts. Otherwise, it adds $(\mathrm{B}, x_{\mathrm{A}})$ into L, and returns x_{A} to $\mathcal{A}$. During $\mathbf{Send}_2$, if $(\mathrm{A}, \mathrm{B}) \neq (\mathrm{A}^*, \mathrm{B}^*)$, or x_{A^*} is not the session output of A^*, then $\mathcal{S}$ behaves identically as in $\mathbf{G}_{2,2}$. Otherwise, it computes $\sigma_{\mathrm{A}} = g \cdot (y_{\mathrm{B}} + e \cdot \mathbf{P}_{\mathrm{B}}) \cdot r'_{\mathrm{A}}$. Finally, it computes SK_{A} according to the scheme.

$\mathbf{G}_{2,4}$: $\mathcal{S}$ first computes $t_1 = a \cdot r'_{\mathrm{A}} + f'_{\mathrm{A}}$, $t_2 = \mathbf{P}_{\mathrm{B}} \cdot r'_{\mathrm{A}} + \widetilde{e}'_{\mathrm{A}}$, where $r'_{\mathrm{A}}, \widetilde{e}'_{\mathrm{A}} \leftarrow \chi_r$. Then, $\mathcal{S}$ computes $x'_{\mathrm{A}} = t_1 + f'_{\mathrm{A}} = a \cdot r'_{\mathrm{A}} + (f'_{\mathrm{A}} + \widetilde{f}'_{\mathrm{A}})$, where $f'_A \leftarrow \chi_\gamma$. Finally, $\mathcal{S}$ behaves almost identically as in $\mathbf{G}_{2,3}$, except during $\mathbf{Send}_2$, if $(\mathrm{A}, \mathrm{B}) \neq (\mathrm{A}^*, \mathrm{B}^*)$, or x^*_{A} is not the session output of A^*, then $\mathcal{S}$ answers quires identically as in $\mathbf{G}_{2,3}$. Otherwise, it computes $\sigma_{\mathrm{A}} = g \cdot (e \cdot t_2 + y_{\mathrm{B}} \cdot r'_{\mathrm{A}}) = g \cdot [(y_{\mathrm{B}} + e \cdot \mathbf{P}_{\mathrm{B}}) \cdot r'_{\mathrm{A}} + e \cdot \widetilde{e}'_{\mathrm{A}}]$. Finally, it computes SK_{A} according to the scheme.

$\mathbf{G}_{2,5}$: $\mathcal{S}$ behaves almost identically as in $\mathbf{G}_{2,4}$, except during $\mathbf{Send}_2$, if $(\mathrm{A}, \mathrm{B}) \neq (\mathrm{A}^*, \mathrm{B}^*)$, or x^*_{A} is not the session output of A^*, then $\mathcal{S}$ answers quires identically as in $\mathbf{G}_{2,4}$. Otherwise, it randomly selects $\sigma_{\mathrm{A}} \leftarrow \chi_r$.

$\mathbf{G}_{2,6}$: $\mathcal{S}$ randomly selects $t_1, t_2 \leftarrow R_q$, and behaves almost identically as in $\mathbf{G}_{2,5}$.

$\mathbf{G}_{2,7}$: $\mathcal{S}$ randomly selects $SK_{\mathrm{A}} \leftarrow \{0, 1\}^n$, and behaves almost identically as in $\mathbf{G}_{2,6}$.

Analysis. As similar analysis of the indistinguishability between $\mathbf{G}_{1,1}$ and $\mathbf{G}_{1,0}$, we can obtain $|Adv(\mathcal{A}, \mathbf{G}_{2,1}) -$

$Adv(\mathcal{A}, \mathbf{G}_{2,0})| \leq negl.$

Since $\mathcal{S}$ replaces $\mathbf{P}_{\mathrm{B}^*} = a \cdot s_{\mathrm{B}^*} + e_{\mathrm{B}^*} \in R_q$ in $\mathbf{G}_{2,2}$ with $\mathbf{P}_{\mathrm{B}^*} \leftarrow_{\mathcal{R}} R_q$ in $\mathbf{G}_{2,3}$, if the adversary can differentiate $\mathbf{G}_{2,1}$ and $\mathbf{G}_{2,2}$, then Ring-DLWE$_{q,\chi}$ is solvable. Thus, we can obtain $|Adv(\mathcal{A}, \mathbf{G}_{2,1}) - Adv(\mathcal{A}, \mathbf{G}_{2,0})| \leq negl.$

As similar analysis of the indistinguishability between $\mathbf{G}_{1,1}$ and $\mathbf{G}_{1,0}$, we can obtain $|Adv(\mathcal{A}, \mathbf{G}_{2,3}) - Adv(\mathcal{A}, \mathbf{G}_{2,2})| \leq ngel.$

In $\mathbf{G}_{2,4}$, $x'_A = a \cdot r'_{\mathrm{A}} + (\widetilde{f}'_{\mathrm{A}} + f'_{\mathrm{A}})$, $\sigma_{\mathrm{A}} = g \cdot [(y_{\mathrm{B}} + e \cdot \mathbf{P}_{\mathrm{B}}) \cdot r'_{\mathrm{A}} + e \cdot \widetilde{e}'_{\mathrm{A}}]$, where $\widetilde{e}'_{\mathrm{A}}, \widetilde{f}'_{\mathrm{A}}, f'_{\mathrm{A}} \leftarrow \chi_r$. Since the distribution of $\widetilde{f}'_{\mathrm{A}} + f'_{\mathrm{A}}$ is close to χ_r. So, we can obtain $|Adv(\mathcal{A}, \mathbf{G}_{2,4}) - Adv(\mathcal{A}, \mathbf{G}_{2,3})| \leq negl.$

$\mathcal{S}$ replaces $\sigma_{\mathrm{A}} = g \cdot (e \cdot t_2 + y_{\mathrm{B}} \cdot r'_{\mathrm{A}})$ in $\mathbf{G}_{2,4}$ with $\sigma_{\mathrm{A}} \leftarrow_{\mathcal{R}} R_q$ in $\mathbf{G}_{2,5}$. By lemma 5, we can obtain $|Adv(\mathcal{A}, \mathbf{G}_{2,5}) - Adv(\mathcal{A}, \mathbf{G}_{2,4})| \leq negl.$

$\mathcal{S}$ replaces $t_1 = a \cdot r'_{\mathrm{A}} + \widetilde{f}'_{\mathrm{A}}$ and $t_2 = \mathbf{P}_{\mathrm{B}} \cdot r'_{\mathrm{A}} + \widetilde{e}'_{\mathrm{A}}$ in $\mathbf{G}_{2,5}$ with two random elements from R_q. If the adversary can differentiate $\mathbf{G}_{2,5}$ and $\mathbf{G}_{2,6}$, then Ring-DLWE$_{q,\chi}$ is solvable.

$\mathbf{G}_{2,6}$ is completely randomized, then $\mathcal{A}$ cannot obtain any advantage via asking $\mathbf{Test}$ oracle, namely $Adv(\mathcal{A}, \mathbf{G}_{2,6}) = 0$. Thus, we obtain $\Pr[\mathbf{E}_2 \bigwedge Suc] = 0$.

C. Event $\mathbf{E}_3 \bigwedge Suc$

Let $\mathbf{E}_3$ represent the event that the test session sid^* has no matching session $\overline{sid}^*$, the owner of sid^* is the responsor, and the SSK of the responsor is given to $\mathcal{A}$.

The proof is essentially identical with $\mathbf{E}_2 \bigwedge Suc$. In $\mathbf{G}_{3,2}$, $\mathcal{S}$ randomly selects $\mathbf{P}_{\mathrm{A}^*} \leftarrow R_q$. In $\mathbf{G}_{3,3}$, $\mathcal{S}$ first computes $y'_{\mathrm{B}} = a \cdot r'_{\mathrm{B}} + f'_{\mathrm{B}}$, where $r'_{\mathrm{B}}, f'_{\mathrm{B}} \leftarrow \chi_r$. Then, $\mathcal{S}$ behaves almost identically as in $\mathbf{G}_{3,2}$, except during $\mathbf{Send}_1$, if $(\mathrm{A}, \mathrm{B}) \neq (\mathrm{A}^*, \mathrm{B}^*)$, or y'_{B} is not the session output of B^*, then $\mathcal{S}$ answers quires identically as in $\mathbf{G}_{3,2}$. Otherwise, it randomly selects $e \leftarrow \chi_r$, and computes $y_{\mathrm{B}} = y'_{\mathrm{B}} - e \cdot \mathbf{P}_{\mathrm{B}}$. If there is $(\mathrm{A}, \mathbf{P}_{\mathrm{B}})$ in L, then $\mathcal{S}$ aborts. Otherwise, it adds $(\mathbf{A}, \mathbf{P}_B)$ into L, and computes $\sigma_{\mathrm{B}} = g \cdot (x_{\mathrm{A}} + d \cdot \mathbf{P}_{\mathrm{A}}) \cdot r'_{\mathrm{B}}$. Finally, $\mathcal{S}$ computes SK_{B} according to the scheme, and sends $(y_{\mathrm{B}}, v_{\mathrm{B}})$ to $\mathcal{A}$. In $\mathbf{G}_{3,4}$, $\mathcal{S}$ computes $t_1 = a \cdot r'_{\mathrm{B}} + f'_{\mathrm{B}}$, $t_2 = \mathbf{P}_{\mathrm{A}} \cdot r'_{\mathrm{B}} + \widetilde{e}'_{\mathrm{B}}$. Then $\mathcal{S}$ computes $y'_{\mathrm{B}} = t_1 + f'_{\mathrm{B}} = a \cdot r'_{\mathrm{B}} + (\widetilde{f}'_{\mathrm{B}} + f'_{\mathrm{B}})$, where $f'_{\mathrm{B}}, \widetilde{f}'_{\mathrm{B}}, \widetilde{e}'_{\mathrm{B}} \leftarrow \chi_r$. Finally, $\mathcal{S}$ behaves almost identically as in $\mathbf{G}_{3,3}$, except during $\mathbf{Send}_1$, if $(\mathrm{A}, \mathrm{B}) \neq (\mathrm{A}^*, \mathrm{B}^*)$, or y'_{B} is not the session output of B^*, then $\mathcal{S}$ answers quires identically as in $\mathbf{G}_{3,3}$. Otherwise, $\mathcal{S}$ randomly selects $e \leftarrow \chi_r$, and computes $y_{\mathrm{B}} = y'_{\mathrm{B}} - e \cdot \mathbf{P}_{\mathrm{B}}$. If there is $(\mathrm{A}, \mathbf{P}_{\mathrm{B}})$ in L, then $\mathcal{S}$ aborts. Otherwise, it adds $(\mathrm{A}, \mathbf{P}_{\mathrm{B}})$ into L, and computes $\sigma_{\mathrm{B}} = g \cdot (e \cdot t_2 + x_{\mathrm{A}} \cdot r'_{\mathrm{B}}) = g \cdot [(x_{\mathrm{A}} + e \cdot \mathbf{P}_{\mathrm{A}}) \cdot r'_{\mathrm{B}} + e \cdot \widetilde{e}'_{\mathrm{B}}]$. Finally, $\mathcal{S}$ computes $v_{\mathrm{B}}, \overline{v}_{\mathrm{B}}, SK_{\mathrm{B}}$ according to the scheme, and send $(y_{\mathrm{B}}, v_{\mathrm{B}})$ to $\mathcal{A}$. In $\mathbf{G}_{3,5}$, if $(\mathrm{A}, \mathrm{B}) \neq (\mathrm{A}^*, \mathrm{B}^*)$, or y'_{B} is not the session output of B^*, then $\mathcal{S}$ answers quires identically as in $\mathbf{G}_{3,4}$. Otherwise, $\mathcal{S}$ selects randomly $\sigma_{\mathrm{B}} \leftarrow R_q$. In $\mathbf{G}_{3,7}$, $\mathcal{S}$ randomly selects $SK_{\mathrm{B}} \leftarrow \{0,1\}^n$, and behaves almost identically as in $\mathbf{G}_{3,6}$.

D. Event $\mathbf{E}_4 \bigwedge Suc$

Let $\mathbf{E}_4$ represent the event that the test session sid^* has no matching session $\overline{sid}^*$, the owner of sid^* is the responsor, and the ephemeral key of the responsor is given to $\mathcal{A}$. The proof is essentially identical with $\mathbf{E}_1 \bigwedge Suc$.

E. Event $\mathbf{E}_5 \bigwedge Suc$

Let $\mathbf{E}_5$ represent the event that the test session sid^* has matching session $\overline{sid}^*$, both the static secret keys are given to $\mathcal{A}$. The proof is essentially identical with $\mathbf{E}_1 \bigwedge Suc$.

F. Event $\mathbf{E}_6 \bigwedge Suc$

Let $\mathbf{E}_6$ represent the event that the test session sid^* has matching session $\overline{sid}^*$, both the ephemeral keys are given to $\mathcal{A}$. The event that the ephemeral key of $\overline{sid}^*$ is given $\mathcal{A}$ is same as the event that sid has no matching session. Since $\mathcal{A}$ cannot determine arbitrary ephemeral key, then the proof is essentially identical with $\mathbf{E}_2 \bigwedge Suc$.

G. Event $\mathbf{E}_7 \bigwedge Suc$

Let $\mathbf{E}_7$ represent the event that the test session sid^* has matching session $\overline{sid}^*$, the static secret keys of sid^* and the ephemeral keys of $\overline{sid}^*$ are given to $\mathcal{A}$. The event that the ephemeral key of $\overline{sid}^*$ is given to $\mathcal{A}$ is same as the event that sid has no matching session. Since $\mathcal{A}$ cannot determine arbitrary ephemeral key, then the proof is essentially identical with $\mathbf{E}_1 \bigwedge Suc$.

H. Event $\mathbf{E}_8 \bigwedge Suc$

Let $\mathbf{E}_8$ represent the event that the test session sid^* has matching session $\overline{sid}^*$, the ephemeral keys of sid^* and the static secret keys of $\overline{sid}^*$ are given to $\mathcal{A}$. The event that the ephemeral key of $\overline{sid}^*$ is given to $\mathcal{A}$ is same as the event that $\overline{sid}^*$ has no matching session. Since $\mathcal{A}$ cannot determine arbitrary ephemeral key, then the proof is essentially identical with $\mathbf{E}_4 \bigwedge Suc$.

VI. Conclusions

In this paper, we build a new efficient authenticated key exchange based on Ring-LWE, which is provably secure under CK^+ secure model. This new scheme has many other advantages over those existing ones. First, compared with the AKE schemes based on trapdoor one-way functions and ones based on multilinear maps respectively, the operations from LWE not only are positive but also does not need to store lots of public parameters. Second, compared with current Key Exchange (KE) schemes based on LWE, the proposed scheme not only protects the shared session key with balanced key derivation function (KDF) but also resists quantum attacks because of the hard assumption in lattice. Finally, only one party needs to retrieve its session key with the robust extractor. Thus, the communication overhead of the network is decreased and the computation is greatly reduced. In addition, since the proposed scheme is built in the cyclotomic ring, then we can adopt Fast Fourier Transform (FFT) over the cyclotomic field to accelerate the calculations, which can obviously improve the efficiency of our scheme.

References

[1] W. Diffie and M. Hellman. New directions in cryptography. Information Theory, IEEE Transactions on 22(6):644-654, 1976.

[2] M. Bellare and P. Rogaway. Entity authentication and key distribution. volume 773 of Lecture Notes in Computer Science, pages 232-249. Springer Berlin Heidelberg, 1994.

[3] A. Menezes, M. Qu, and S. Vanstone, Some new key agreement protocols providing mutual implicit authentication, SecondWorkshop on Selected Areas in Cryptography, 1995.

[4] L. Law, A. Menezes, M. Qu, J. Solinas, and S. Vanstone, An efficient Protocol for Authenticated Key Agreement, Designs, Codes and Cryptography, 119-134, 2003.

[5] R. Canetti and H. Krawczyk. Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels. In B. Pfitzmann, editor, Advances in Cryptology-EUROCRYPT 2001.

[6] H. Krawczyk. HMQV: A High-Performance Secure Diffie-Hellman Protocol. In V. Shoup, editor, Advances in Cryptology-CRYPTO 2005, volume 3621 of Lecture Notes in Computer Science, pages 546-566. Springer Berlin Heidelberg, 2005.

[7] Fujioka. A, Suzuki. K, Xagawa. K, Yoneyama. K. Stronger Secure Authenticated Key Exchange from Factoring, Codes, and Lattices. In Fischlin [22], pages 467-484.

[8] M. Ajtai. Generating Hard Instances of The Short Basis Problem. In ICALP, pages 1-9, 1999.

[9] J. Alwen and C. Peikert. Generating Shorter Bases for Hard Random Lattices. Theory of Computing Systems, pages 535-553, 2011.

[10] C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for Hard Lattices and New Cryptographic Constructions. In STOC, pages 197C206, 2008.

[11] V. Lyubashevsky, C. Peikert, and O. Regev. On Ideal Lattices and Learning With Errors over Rings. In EUROCRYPT, pages 1-23, 2010.

[12] Fujioka. A, Suzuki. K, Xagawa. K, Yoneyama. K. Practical and Post-Quantum Authenticated Key Exchange from One-Way Secure Key Encapsulation Mechanism, ASIA CCS'13, May 8-10, 2013, Hangzhou, China. Copyright 2013 ACM 978-1-4503-1767-2/13/05.

[13] Daniele Micciancio, Chris Peikert, Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller, Cryptology ePrint Archive, Report 2011/501 (2011).

[14] Damien Stehl$\acute{e}$, Ron Steinfeld, Keisuke Tanaka, Keita Xagawa. Efficient Public Key Encryption Based on Ideal Lattices (Extended Abstract). Advances in Cryptology-ASIACRYPT 2009; 617-635.

[15] D. Micciancio and O. Regev. Worst-case to Average-case Reductions Based on Gaussian Measures. SIAMJ. Comput., 37:267-302, April 2007.

[16] L$\acute{e}$o Ducas, Phong Q. Nguyen, Faster Gaussian Lattice Sampling using Lazzy Floating-Point Arithmetic, Advances in Cryptology-ASIACRYPT 2012: 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6 2012.

[17] D. Micciancio and O. Regev. Worst-case to Average-case Reductions Based on Gaussian Measures. SIAM J. Comput., 37:267-302, April 2007.

[18] D. Micciancio and O. Regev. Lattice-based Cryptography. In D. Bernstein, J. Buchmann, and E. Dahmen, editors, Post-Quantum Cryptography, pages 147-191. Springer Berlin Heidelberg, 2009.

[19] C. Peikert. Lattice Cryptography for the Internet. Cryptology ePrint Archive, Report 2014/070, 2014.

[20] Z. Brakerski, A. Langlois, C. Peikert, O. Regev, and D.Stehle. Classical Hardness of Learning with Errors. In Proc. of 45th STOC, pages 575-584. ACM, 2013.

[21] D. Micciancio and C. Peikert. Hardness of SIS and LWE with Small Parameters. In Proc. CRYPTO '13, volume 8042 of Lecture Notes in Computer Science, pages 21-39. Springer, 2013.

[22] C. Peikert. An Efficient and Parallel Gaussian Sampler for Lattices. In Proc. of Crypto '10, LNCS 6223, pages 80-97. Spinger-Verlag,

2010.

[23] Bresson E, Chevassut O, Pointcheval D. Provably Authenticated Group Diffie-Hallman Key Exchange. CCS'01: Proceedings of the 8th ACM conference on Computer and Communications Security. Philadelpia:ACM, 2001.

[24] Katz J,Yung M.Scalable Protocols for Authenticated Group Key Exchange. Advance in Cryptology-Crypto 2003. Springer.

[25] Bohli J, Vasco M, Steinwandt R. Secure Group Key Establishment Revisited. International Journal of Informational Security. 2007. 6(4):243-254.

[26] Katz J, Shin J. Modeling Insider Attacks on Group Key Exchange Protocols. Proceedings of the 12th ACM Conference on Computer and Communication Security-CCS'05. ACM, 2005:180-189.

[27] Manulis M. Survey on Security Requirements and Models for Group Key Exchange. http://eprint.iacr.org /2006/388.

[28] Bresson E, Manulis M. Malicious Participants in Group Key Exchange: Key Control and Contributiveness in the Shadow of Trust. Proceedings of the ATC'07 of LNCS, Springer, 2007.

[29] Bresson E, Manulis M. Securing Group Key Exchange against Strong Corruptions and Key Registration Attacks. UACT, 2008.

[30] Ran Canetti. Universally Composable Security: A New Paradigm for Cryptographic Protocols. Cryptology ePrint Archive, Report 2000/067, 2000. http://eprint.iacr.org/, Version updated on 13 Dec 2005.

[31] X. L. Jintai Ding. A Simple Provably Secure Key Exchange Scheme Based on The Learning With Errors Problem. Cryptology ePrint Archive, Report 2012/688, 2012.

[32] V. Lyubashevsky, C. Peikert, and O. Regev. A Toolkit for Ring-LWE Cryptography. In T. Johansson and P. Nguyen, editors, Advances in Cryptology, 2013.