Generic and Practical Key Establishment from Lattice

Zhengzhong Jin[1,2] and Yunlei Zhao[3](✉)

[1] School of Mathematics, Fudan University, Shanghai, China
[2] Department of Computer Science, Johns Hopkins University, Baltimore, USA
[3] School of Computer Science, Fudan University, Shanghai, China
ylzhao@fudan.edu.cn

Abstract. In this work, we abstract some key ingredients in previous key establishment and public-key encryption schemes from LWE and its variants. Specifically, we explicitly formalize the building tool, referred to as key consensus (KC) and its asymmetric variant AKC. KC and AKC allow two communicating parties to reach consensus from close values, which plays the fundamental role in lattice-based cryptography. We then prove the upper bounds on parameters for any KC and AKC, which reveal the inherent constraints on the parameters among security, bandwidth, error probability, and consensus range. As a conceptual contribution, this simplifies the design and analysis of these cryptosystems in the future. Guided by the proved upper bounds, we design and analyze both generic and highly practical KC and AKC schemes, which are referred to as OKCN and AKCN respectively for presentation simplicity. We present a generic protocol structure for key establishment from learning with rounding (LWR), which can be instantiated with either KC or AKC. We then provide an analysis breaking the correlation between the rounded deterministic noise and the secret, and design an algorithm to calculate the error probability numerically. When applied to LWE-based key establishment, OKCN and AKCN can result in more practical or well-balanced schemes, compared to existing LWE-based protocols in the literature.

1 Introduction

Most public-key cryptosystems currently in use, based on the hardness of solving (elliptic curve) discrete logarithm or factoring large integers, will be broken, if large-scale quantum computers are ever built. The arrival of such quantum computers is now believed by many scientists to be merely a significant engineering

This work is supported in part by National Key Research and Development Program of China under Grant No. 2017YFB0802000, National Natural Science Foundation of China under Grant Nos. 61472084 and U1536205, Shanghai Innovation Action Project under Grant No. 16DZ1100200, Shanghai Science and Technology Development Funds under Grant No. 6JC1400801, and Shandong Provincial Key Research and Development Program of China under Grant Nos. 2017CXG0701 and 2018CXGC0701.

R. H. Deng et al. (Eds.): ACNS 2019, LNCS 11464, pp. 302–322, 2019.
https://doi.org/10.1007/978-3-030-21568-2_15

challenge, and is estimated to be within the next two decades or so. Historically, it has taken almost two decades to deploy the modern public key cryptography infrastructure. Therefore, regardless of whether we can estimate the exact time of the arrival of the quantum computing era, we should begin now to prepare our information security systems to be able to resist quantum computing. In addition, for the content we want to protect over a period of 15 years or longer, it becomes necessary to switch to post-quantum cryptography today. In the majority of contexts, *ephemeral* key establishment (KE), which plays a central role in modern cryptography, is among the most critical asymmetric primitives to upgrade to post-quantum security.

Lattice-based cryptography is one of the promising mathematical approaches to achieving security resistant to quantum attacks. For cryptographic usage, compared with the classic hard lattice problems such as SVP and CVP, the learning with errors (LWE) problem is proven to be much more versatile [Reg09]. One of the main technical contributions in recent years on achieving practical key establishment based on LWE and its variants is the improvement and generalization of the key reconciliation mechanisms [Reg09,DXL12,LPR10,LP10]. But the key reconciliation mechanisms were only previously used and analyzed, for both KE and PKE, in a *non-black-box* way. This means, for new key reconciliation mechanisms developed in the future to be used for constructing lattice-based cryptosystems, we need to analyze their security from scratch. Moreover, for the various parameters involved in key reconciliation, the bounds on what could or couldn't be achieved are unclear. As a consequence, we lack basic criteria to evaluate various reconciliation mechanisms and to indicate whether they can be further improved.

Abstraction/generalization is fundamental to natural science (mathematics, physics), and is particularly important to cryptography. For example, in the area of signature, Schnorr signature is generalized via Fiat-Shamir transformation [FS86], with abstraction of Σ-protocol [CDS94]. The similar abstraction and generalization also plays a fundamental role in CCA-secure PKE, and in many more areas of modern cryptography. Abstraction and generalization is particularly helpful and expected for lattice-based cryptography, as they are usually less easy to understand and evaluate, and are related to the ongoing NIST post-quantum cryptography standardization [NIST].

1.1 Our Contributions

In this work, we abstract the key ingredients in previous key establishment and PKE schemes based on LWE and its variants, by introducing and formalizing the building tool, referred to as key consensus (KC) and its asymmetric variant AKC. KC and AKC allow two communicating parties to reach consensus from close values obtained by some secure information exchange, such as exchanging their LWE samples. We then discover upper bounds on parameters for any KC and AKC. As a conceptual contribution, this simplifies the design and analysis of these cryptosystems in the future. We then design and analyze both generic and highly practical KC and AKC schemes, which are referred to as *symmetric* *key consensus with noise* (OKCN) and *asymmetric key consensus with noise* (AKCN) respectively for presentation simplicity.

We propose the first construction of key establishment *merely* based on the LWR problem with concrete analysis and evaluation, to the best of our knowledge. We use the randomness lifting technique to present a unified protocol structure that can be instantiated with either KC or AKC. We provide an analysis breaking the correlation between the rounded deterministic noise and the secret, and design an algorithm to calculate the error probability numerically. When applied to LWE-based key establishment, OKCN and AKCN can result in more practical or well-balanced schemes, compared to the related LWE-based protocols in the literature. The protocols developed in this work are implemented. The code and scripts, together with those for evaluating concrete security and failure rates, are (anonymously) available from Github http://github.com/OKCN.

1.2 Related Work

AKC (resp., KC) was pioneered by the works on lattice-based PKE [LP10, LPR10] (resp., the work on key establishment [DXL12]). LWR-based key establishment was pioneered by the Lizard protocol [CKLS16]. The Lizard protocol is AKC-based, and is based on (special variants of) both LWE and LWR. To the best our knowledge, key establishment protocol *merely* from the LWR problem was first achieved in an early version of our work [JZ16].[1] The works [BBG+17, DKRV17, BGL+18] considered AKC-based key transport protocols from some variants of LWR (some of which use sparse-ternary secret keys), and show that randomness lifting is not necessary for AKC-based protocol from LWR. But these protocols do not support KC-based instantiations. We remark that, for the recommended parameters in all the works, randomness lifting corresponds to uniform sampling from $[-2^k, 2^k-1]$ for some positive integer k, which is fast and easy.

2 Preliminaries

A string or value α means a binary one, and $|\alpha|$ is its binary length. For any real number x, $\lfloor x \rfloor$ denotes the largest integer that less than or equal to x, and $\lfloor x \rceil = \lfloor x + 1/2 \rfloor$. For any positive integers a and b, denote by $\mathsf{lcm}(a, b)$ the least common multiple of them. For any $i, j \in \mathbb{Z}$ such that $i < j$, denote by $[i, j]$ the set of integers $\{i, i+1, \cdots, j-1, j\}$. For any positive integer t, we let $\mathbb{Z}_t$ denote $\mathbb{Z}/t\mathbb{Z}$. The elements of $\mathbb{Z}_t$ are represented, by default, as $[0, t-1]$. Nevertheless, sometimes, $\mathbb{Z}_t$ is explicitly specified to be represented as $[-\lfloor (t-1)/2 \rfloor, \lfloor t/2 \rfloor]$.

If S is a finite set then $|S|$ is its cardinality, and $x \leftarrow S$ is the operation of picking an element uniformly at random from $\mathcal{S}$. For two sets $A, B \subseteq \mathbb{Z}_q$, define

[1] Our work appeared in the literature since November 2016 [JZ16], and the construction and analysis of LWR-based protocol are presented in the update of February 2017.

$A+B \triangleq \{a+b|a \in A, b \in B\}$. For an addictive group $(G,+)$, an element $x \in G$ and a subset $S \subseteq G$, denote by $x+S$ the set containing $x+s$ for all $s \in S$. For a set S, denote by $\mathcal{U}(S)$ the uniform distribution over S. For any discrete random variable X over $\mathbb{R}$, denote $\mathsf{Supp}(X) = \{x \in \mathbb{R} \mid \Pr[X=x] > 0\}$.

We use standard notations and conventions below for writing probabilistic algorithms, experiments and interactive protocols. If $\mathcal{D}$ denotes a probability distribution, $x \leftarrow \mathcal{D}$ is the operation of picking an element according to $\mathcal{D}$. If α is neither an algorithm nor a set then $x \leftarrow \alpha$ is a simple assignment statement. If A is a probabilistic algorithm, then $A(x_1, x_2, \cdots; r)$ is the result of running A on inputs $x_1, x_2, \cdots$ and coins r. We let $y \leftarrow A(x_1, x_2, \cdots)$ denote the experiment of picking r at random and letting y be $A(x_1, x_2, \cdots; r)$. By $\Pr[R_1; \cdots; R_n : E]$ we denote the probability of event E, after the ordered execution of random processes $R_1, \cdots, R_n$.

2.1 The LWE and LWR Problems

Given positive *continuous* $\alpha > 0$, define the real Gaussian function $\rho_\alpha(x) \triangleq \exp(-x^2/2\alpha^2)/\sqrt{2\pi\alpha^2}$ for $x \in \mathbb{R}$. Let $D_{\mathbb{Z},\alpha}$ denote the one-dimensional *discrete* Gaussian distribution over $\mathbb{Z}$, which is determined by its probability density function $D_{\mathbb{Z},\alpha}(x) \triangleq \rho_\alpha(x)/\rho_\alpha(\mathbb{Z}), x \in \mathbb{Z}$. Finally, let $D_{\mathbb{Z}^n,\alpha}$ denote the n-dimensional *spherical* discrete Gaussian distribution over $\mathbb{Z}^n$, where each coordinate is drawn *independently* from $D_{\mathbb{Z},\alpha}$.

Given positive integers n and q that are both polynomials in the security parameter λ, an integer vector $\mathbf{s} \in \mathbb{Z}_q^n$, and a probability distribution χ on $\mathbb{Z}_q$, let $A_{q,\mathbf{s},\chi}$ be the distribution over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ obtained by choosing $\mathbf{a} \in \mathbb{Z}_q^n$ uniformly at random, and an error term $e \leftarrow \chi$, and outputting the pair $(\mathbf{a}, b = \mathbf{a}^T\mathbf{s} + e) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$. The error distribution χ is typically taken to be the discrete Gaussian probability distribution $D_{\mathbb{Z},\alpha}$ defined previously; However, as suggested in [BCD+16], other alternative distributions of χ can be taken. Briefly speaking, the (decisional) *learning with errors* (LWE) assumption [Reg09] says that, for sufficiently large security parameter λ, no probabilistic polynomial-time (PT) algorithm can distinguish, with non-negligible probability, $A_{q,\mathbf{s},\chi}$ from the uniform distribution over $\mathbb{Z}_q^n \times \mathbb{Z}_q$. This holds even if $\mathcal{A}$ sees polynomially many samples, and even if the secret vector $\mathbf{s}$ is drawn randomly from χ^n [ACPS09].

The LWR problem [BPR12] is a "decarbonized" variant of the LWE problem. Let $\mathcal{D}$ be some distribution over $\mathbb{Z}_q^n$, and $\mathbf{s} \leftarrow \mathcal{D}$. For integers $q \geq p \geq 2$ and any $x \in \mathbb{Z}_q$, denote

$$\lfloor x \rceil_p = \lfloor \frac{p}{q} x \rceil. \tag{1}$$

Then, for positive integers n and $q \geq p \geq 2$, the LWR distribution $A_{n,q,p}(\mathbf{s})$ over $\mathbb{Z}_q^n \times \mathbb{Z}_p$ is obtained by sampling $\mathbf{a}$ from $\mathbb{Z}_q^n$ uniformly at random, and outputting $\left(\mathbf{a}, \left\lfloor \mathbf{a}^T\mathbf{s} \right\rceil_p\right) \in \mathbb{Z}_q^n \times \mathbb{Z}_p$. Briefly speaking, the (decisional) LWR assumption says that, for sufficiently large security parameter, no PT algorithm $\mathcal{A}$ can distinguish, with non-negligible probability, the distribution $A_{n,q,p}(\mathbf{s})$ from the distribution $(\mathbf{a} \leftarrow \mathbb{Z}_q^n, \lfloor u \rceil_p)$ where $u \leftarrow \mathbb{Z}_q$. This holds even if $\mathcal{A}$ sees polynomially many samples. An efficient reduction from the LWE problem to the LWR problem, for super-polynomial large q, is provided in [BPR12]. Let B denote the bound for any component in the secret $\mathbf{s}$. It is recently shown that, when $q \geq 2mBp$ (equivalently, $m \leq q/2Bp$), the LWE problem can be reduced to the (decisional) LWR assumption with m independently random samples [BGM+16]. Moreover, the reduction from LWE to LWR is actually independent of the distribution of the secret $\mathbf{s}$.

3 Key Consensus with Noise

Before presenting the definition of key consensus (KC) scheme, we first introduce a new function $|\cdot|_t$ relative to arbitrary positive integer $t \geq 1$: $|x|_t = \min\{x \bmod t, t - x \bmod t\}, \quad \forall x \in \mathbb{Z}$, where the result of modular operation is represented in $\{0, ..., (t-1)\}$. For instance, $|-1|_t = \min\{-1 \mod t, (t+1) \mod t\} = \min\{t-1, 1\} = 1$. In the following description, we use $|\sigma_1 - \sigma_2|_q$ to measure the distance between two elements $\sigma_1, \sigma_2 \in \mathbb{Z}_q$.

Definition 1. *A KC scheme $KC = (\mathsf{params}, \mathsf{Con}, \mathsf{Rec})$ is specified as follows.*

- $\mathsf{params} = (q, m, g, d, aux)$ *denotes the system parameters, where q, m, g, d are positive integers satisfying $2 \leq m, g \leq q, 0 \leq d \leq \lfloor \frac{q}{2} \rfloor$, and aux denotes some auxiliary values that are usually determined by (q, m, g, d) and could be set to be a special symbol $\emptyset$ indicating "empty".*
- $(k_1, v) \leftarrow \mathsf{Con}(\sigma_1, \mathsf{params})$*: On input of $(\sigma_1 \in \mathbb{Z}_q, \mathsf{params})$, the* probabilistic *polynomial-time conciliation algorithm Con outputs (k_1, v), where $k_1 \in \mathbb{Z}_m$ is the shared-key, and $v \in \mathbb{Z}_g$ is a hint signal that will be publicly delivered to the communicating peer to help the two parties reach consensus.*
- $k_2 \leftarrow \mathsf{Rec}(\sigma_2, v, \mathsf{params})$*: On input of $(\sigma_2 \in \mathbb{Z}_q, v, \mathsf{params})$, the* deterministic *polynomial-time reconciliation algorithm Rec outputs $k_2 \in \mathbb{Z}_m$.*

Correctness: *A KC scheme is* correct*, if for any $\sigma_1, \sigma_2 \in \mathbb{Z}_q$ such that $|\sigma_1 - \sigma_2|_q \leq d$, $(k_1, v) \leftarrow \mathsf{Con}(\sigma_1, \mathsf{params})$ and $k_2 \leftarrow \mathsf{Rec}(\sigma_2, v, \mathsf{params})$, it holds $k_1 = k_2$.*

Security: *A KC scheme is* secure*, if k_1 and v are independent, and k_1 is uniformly distributed over $\mathbb{Z}_m$, whenever $\sigma_1 \leftarrow \mathbb{Z}_q$ and k_1 is the output of $\mathsf{Con}(\sigma_1, \mathsf{params})$. The probability is taken over the sampling of σ_1 and the random coins used by Con.*

3.1 Efficiency Upper Bound of KC

The following theorem reveals an upper bound on the parameters q (dominating security and efficiency), m (parameterizing range of consensus key), g (parameterizing bandwidth), and d (parameterizing error rate), which allows us to take balance on these parameters according to different priorities. Due to space limitation, the proof is given in the full version [JZ16].

Algorithm 1. OKCN: Symmetric KC with Noise

```
1:  $\mathsf{params} = (q, m, g, d, aux)$, $aux = \{q' = \mathsf{lcm}(q, m), \alpha = q'/q, \beta = q'/m\}$
2:  procedure Con($(\sigma_1, \mathsf{params})$)                    ▷ $\sigma_1 \in [0, q-1]$
3:      $e \leftarrow [-\lfloor(\alpha - 1)/2\rfloor, \lfloor\alpha/2\rfloor]$
4:      $\sigma_A = (\alpha\sigma_1 + e) \bmod q'$
5:      $k_1 = \lfloor\sigma_A/\beta\rfloor \in \mathbb{Z}_m$
6:      $v' = \sigma_A \mod \beta$
7:      $v = \lfloor v'g/\beta\rfloor$                                ▷ $v \in \mathbb{Z}_g$
8:      return $(k_1, v)$
9:  end procedure
10: procedure Rec($\sigma_2, v, \mathsf{params}$)                    ▷ $\sigma_2 \in [0, q-1]$
11:     $k_2 = \lfloor\alpha\sigma_2/\beta - (v + 1/2)/g\rceil \bmod m$
12:     return $k_2$
13: end procedure
```

Theorem 1. *If* $KC = (\mathsf{params}, \mathsf{Con}, \mathsf{Rec})$ *is a* correct *and* secure *key consensus scheme, and* $\mathsf{params} = (q, m, g, d, aux)$*, then* $2md \leq q\left(1 - \frac{1}{g}\right)$.

3.2 Construction and Analysis of OKCN

The key consensus scheme, named *symmetric key consensus with noise* (OKCN)", is presented in Algorithm 1. The following fact is direct from the definition of $|\cdot|_t$.

Fact 1. *For any* $x, y, t, l \in \mathbb{Z}$ *where* $t \geq 1$ *and* $l \geq 0$*, if* $|x - y|_q \leq l$*, then there exists* $\theta \in \mathbb{Z}$ *and* $\delta \in [-l, l]$ *such that* $x = y + \theta t + \delta$.

Theorem 2. *Suppose that the system parameters satisfy* $(2d+1)m < q\left(1 - \frac{1}{g}\right)$ *where* $m \geq 2$ *and* $g \geq 2$*. Then, the* OKCN *scheme is* correct.

Proof. Suppose $|\sigma_1 - \sigma_2|_q \leq d$. By Fact 1, there exist $\theta \in \mathbb{Z}$ and $\delta \in [-d, d]$ such that $\sigma_2 = \sigma_1 + \theta q + \delta$. From line 4 and 6 in Algorithm 1, we know that there is a $\theta' \in \mathbb{Z}$, such that $\alpha\sigma_1 + e + \theta' q' = \sigma_A = k_1\beta + v'$. And from the definition of α, β, we have $\alpha/\beta = m/q$. Taking these into the formula of k_2 in Rec (line 11 in Algorithm 1), we have

$$
\begin{aligned}
k_2 &= \lfloor\alpha\sigma_2/\beta - (v + 1/2)/g\rceil \bmod m && (2)\\
&= \lfloor\alpha(\theta q + \sigma_1 + \delta)/\beta - (v + 1/2)/g\rceil \bmod m && (3)\\
&= \left\lfloor m(\theta - \theta') + \frac{1}{\beta}(k_1\beta + v' - e) + \frac{\alpha\delta}{\beta} - \frac{1}{g}(v + 1/2)\right\rceil \bmod m && (4)\\
&= \left\lfloor k_1 + \left(\frac{v'}{\beta} - \frac{v + 1/2}{g}\right) - \frac{e}{\beta} + \frac{\alpha\delta}{\beta}\right\rceil \bmod m && (5)
\end{aligned}
$$

Algorithm 2. OKCN simple

```
params : $q = 2^{\bar{q}}, g = 2^{\bar{g}}, m = 2^{\bar{m}}, d$, where $\bar{g} + \bar{m} = \bar{q}$
procedure Con($\sigma_1$, params)
    $k_1 = \left\lfloor \frac{\sigma_1}{g} \right\rfloor$
    $v = \sigma_1 \bmod g$
    return $(k_1, v)$
end procedure
procedure Rec($\sigma_2, v$, params)
    $k_2 = \left\lfloor \frac{\sigma_2 - v}{g} \right\rceil \bmod m$
    return $k_2$
end procedure
```

Notice that $|v'/\beta - (v + 1/2)/g| = |v'g - \beta(v + 1/2)|/\beta g \leq 1/2g$. So

$$\left| \left(\frac{v'}{\beta} - \frac{v + 1/2}{g} \right) - \frac{e}{\beta} + \frac{\alpha\delta}{\beta} \right| \leq \frac{1}{2g} + \frac{\alpha}{\beta}(d + 1/2).$$

From the assumed condition $(2d + 1)m < q(1 - \frac{1}{g})$, we get that the right-hand side is strictly smaller than 1/2; Consequently, after the rounding, $k_2 = k_1$. □

Theorem 3. *OKCN is secure. Specifically, when $\sigma_1 \leftarrow \mathbb{Z}_q$, k_1 and v are independent, and k_1 is uniform over $\mathbb{Z}_m$, where the probability is taken over the sampling of σ_1 and the random coins used by* Con.

Proof. Recall that $q' = \mathsf{lcm}(q, m), \alpha = q'/q, \beta = q'/m$. We first demonstrate that σ_A is subject to uniform distribution over $\mathbb{Z}_{q'}$. Consider the map $f : \mathbb{Z}_q \times \mathbb{Z}_\alpha \rightarrow \mathbb{Z}_{q'}$; $f(\sigma, e) = (\alpha\sigma + e) \bmod q'$, where the elements in $\mathbb{Z}_q$ and $\mathbb{Z}_\alpha$ are represented in the same way as specified in Algorithm 1. It is easy to check that f is an one-to-one map. Since $\sigma_1 \leftarrow \mathbb{Z}_q$ and $e \leftarrow \mathbb{Z}_\alpha$ are subject to uniform distributions, and they are independent, $\sigma_A = (\alpha\sigma_1 + e) \bmod q' = f(\sigma_1, e)$ is also subject to uniform distribution over $\mathbb{Z}_{q'}$.

In the similar way, defining $f' : \mathbb{Z}_m \times \mathbb{Z}_\beta \rightarrow \mathbb{Z}_{q'}$ such that $f'(k_1, v') = \beta k_1 + v'$, then f' is obviously a one-to-one map. From line 6 of Algorithm 1, $f'(k_1, v') = \sigma_A$. As σ_A is distributed uniformly over $\mathbb{Z}_{q'}$, (k_1, v') is uniformly distributed over $\mathbb{Z}_m \times \mathbb{Z}_\beta$, and so k_1 and v' are independent. As v only depends on v', k_1 and v are independent. □

Special Parameters, and Performance Speeding-Up. The first and the second line of Con (line 3 and 4 in Algorithm 1) play the role in transforming a uniform distribution over $\mathbb{Z}_q$ to a uniform distribution over $\mathbb{Z}_{q'}$. If one chooses q, g, m to be power of 2, i.e., $q = 2^{\bar{q}}, g = 2^{\bar{g}}, m = 2^{\bar{m}}$ where $\bar{q}, \bar{g}, \bar{m} \in \mathbb{Z}$, then such transformation is not necessary, and the random noise e used in calculating σ_A in Algorithm 1 is avoided. If we take $\bar{g} + \bar{m} = \bar{q}$, it can be further simplified into the variant depicted in Algorithm 2, with the constraint on parameters is further relaxed.

Corollary 1. *If m, g are power of 2, $q = m \cdot g$, and $2md < q$, then the KC scheme described in Algorithm 2 is* correct *and* secure. *Notice that the constraint on parameters is further simplified to $2md < q$ in this case.*

To the best of our knowledge, OKCN is the first multi-bit reconciliation mechanism, and the first that can be instantiated to tightly match the upper-bound proved in Theorem 1.

4 Asymmetric Key Consensus with Noise

Definition 2. *An asymmetric key consensus scheme $AKC = (\mathsf{params}, \mathsf{Con}, \mathsf{Rec})$ is specified as follows:*

- $\mathsf{params} = (q, m, g, d, aux)$ *denotes the system parameters, where q, $2 \leq m, g \leq q, 1 \leq d \leq \lfloor \frac{q}{2} \rfloor$ are positive integers, and aux denotes some auxiliary values that are usually determined by (q, m, g, d) and could be set to be empty.*
- $v \leftarrow \mathsf{Con}(\sigma_1, k_1, \mathsf{params})$: *On input of $(\sigma_1 \in \mathbb{Z}_q, k_1 \in \mathbb{Z}_m, \mathsf{params})$, the* probabilistic *polynomial-time conciliation algorithm* Con *outputs the public hint signal $v \in \mathbb{Z}_g$.*
- $k_2 \leftarrow \mathsf{Rec}(\sigma_2, v, \mathsf{params})$: *On input of $(\sigma_2, v, \mathsf{params})$, the* deterministic *polynomial-time algorithm* Rec *outputs $k_2 \in \mathbb{Z}_m$.*

Correctness: *An AKC scheme is* correct, *if for any $\sigma_1, \sigma_2 \in \mathbb{Z}_q$ such that $|\sigma_1 - \sigma_2|_q \leq d$, and $v \leftarrow \mathsf{Con}(\sigma_1, k_1, \mathsf{params}), k_2 \leftarrow \mathsf{Rec}(\sigma_2, v, \mathsf{params})$, it holds $k_1 = k_2$.*

Security: *An AKC scheme is* secure, *if v is independent of k_1 whenever σ_1 is uniformly distributed over $\mathbb{Z}_q$, and v is the output of $\mathsf{Con}(\sigma_1, k_1, \mathsf{params})$. Specifically, for arbitrary $\tilde{v} \in \mathbb{Z}_g$ and arbitrary $\tilde{k}_1, \tilde{k}_1' \in \mathbb{Z}_m$, it holds that $\Pr[v = \tilde{v} | k_1 = \tilde{k}_1] = \Pr[v = \tilde{v} | k_1 = \tilde{k}_1']$, where the probability is taken over $\sigma_1 \leftarrow \mathbb{Z}_q$ and the random coins used by Con.*

Theorem 4. *Let AKC be an asymmetric key consensus scheme with* $\mathsf{params} = (q, m, d, g, aux)$. *If AKC is* correct *and* secure, *then $2md \leq q\left(1 - \frac{m}{g}\right)$.*

The proof of Theorem 4 is given in the full version [JZ16]. Comparing the formula $2md \leq q(1 - m/g)$ in Theorem 4 with the formula $2md \leq q(1 - 1/g)$ in Theorem 1, we see that the only difference is a factor m in g. This indicates that, on the same values of (q, m, d), an AKC scheme has to use a bigger bandwidth parameter g compared to KC.

4.1 Construction and Analysis of AKCN

The AKCN scheme, referred to as *asymmetric key consensus with noise*, is depicted in Algorithm 3. For AKCN, we can offline compute and store k_1 and $g\lfloor k_1 q/m \rceil$ in order to accelerate online performance.

Algorithm 3. AKCN: Asymmetric KC with Noise

```
params = $(q, m, g, d, aux)$, where $aux = \emptyset$.
procedure Con($\sigma_1, k_1$, params)                    ▷ $\sigma_1 \in [0, q-1]$
    $v = \lfloor g(\sigma_1 + \lfloor k_1 q/m \rceil)/q \rceil \bmod g$
    return $v$
end procedure
procedure Rec($\sigma_2, v$, params)                      ▷ $\sigma_2 \in [0, q-1]$
    $k_2 = \lfloor m(v/g - \sigma_2/q) \rceil \bmod m$
    return $k_2$
end procedure
```

The design of AKCN was guided by, and motivated for, the upper-bound for AKC proved in this work. In designing AKCN, we combine all the existing optimizations in the literature in order to almost meet the upperbound proved in Theorem 4. AKCN is a generalization of the basic reconciliation mechanisms proposed in [LPR10,LP10], and its design was also inspired by the design of our OKCN and the works [BPR12,PG13]. But AKCN and the underlying reconciliation mechanism of [PG13] could be viewed as incomparable in general. In particular, the reconciliation mechanisms proposed in [LPR10,LP10] correspond to the special case of AKCN when $g = q$ and $m = 2$. Note that, with AKCN, we use Eq. 1 described in the definition of LWR [BPR12], which may also be derived implicitly from [Pei09].

Theorem 5. *Suppose the parameters of AKCN satisfy* $(2d+1)m < q\left(1 - \frac{m}{g}\right)$. *Then, the AKCN scheme described in Algorithm 3 is* correct.

Proof. From the formula generating v, we know that there exist $\varepsilon_1, \varepsilon_2 \in \mathbb{R}$ and $\theta \in \mathbb{Z}$, where $|\varepsilon_1| \leq 1/2$ and $|\varepsilon_2| \leq 1/2$, such that

$$v = \frac{g}{q}\left(\sigma_1 + \left(\frac{k_1 q}{m} + \varepsilon_1\right)\right) + \varepsilon_2 + \theta g$$

Taking this into the formula computing k_2 in Rec, we have

$$\begin{aligned} k_2 &= \lfloor m(v/g - \sigma_2/q) \rceil \bmod m \\ &= \left\lfloor m\left(\frac{1}{q}(\sigma_1 + k_1 q/m + \varepsilon_1) + \frac{\varepsilon_2}{g} + \theta - \frac{\sigma_2}{q}\right)\right\rceil \bmod m \\ &= \left\lfloor k_1 + \frac{m}{q}(\sigma_1 - \sigma_2) + \frac{m}{q}\varepsilon_1 + \frac{m}{g}\varepsilon_2 \right\rceil \bmod m \end{aligned}$$

By Fact 1 (page 6), there exist $\theta' \in \mathbb{Z}$ and $\delta \in [-d, d]$ such that $\sigma_1 = \sigma_2 + \theta' q + \delta$. Hence,

$$k_2 = \left\lfloor k_1 + \frac{m}{q}\delta + \frac{m}{q}\varepsilon_1 + \frac{m}{g}\varepsilon_2 \right\rceil \bmod m$$

Since $|m\delta/q + m\varepsilon_1/q + m\varepsilon_2/g| \leq md/q + m/2q + m/2g < 1/2$, $k_1 = k_2$. □

Theorem 6. *The AKCN scheme is* secure*. Specifically, v is independent of k_1 when $\sigma_1 \leftarrow \mathbb{Z}_q$.*

Proof. For arbitrary $\tilde{v} \in \mathbb{Z}_g$ and arbitrary $\tilde{k}_1, \tilde{k}_1' \in \mathbb{Z}_m$, we prove that $\Pr[v = \tilde{v}|k_1 = \tilde{k}_1] = \Pr[v = \tilde{v}|k_1 = \tilde{k}_1']$ when $\sigma_1 \leftarrow \mathbb{Z}_q$.

For any $(\tilde{k}, \tilde{v})$ in $\mathbb{Z}_m \times \mathbb{Z}_g$, the event $(v = \tilde{v} \mid k_1 = \tilde{k})$ is equivalent to the event that there exists $\sigma_1 \in \mathbb{Z}_q$ such that $\tilde{v} = \lfloor g(\sigma_1 + \lfloor \tilde{k}q/m \rceil)/q \rceil \bmod g$. Note that $\sigma_1 \in \mathbb{Z}_q$ satisfies $\tilde{v} = \lfloor g(\sigma_1 + \lfloor \tilde{k}q/m \rceil)/q \rceil \bmod g$, if and only if there exist $\varepsilon \in (-1/2, 1/2]$ and $\theta \in \mathbb{Z}$ such that $\tilde{v} = g(\sigma_1 + \lfloor \tilde{k}q/m \rceil)/q + \varepsilon - \theta g$. That is, $\sigma_1 = (q(\tilde{v} - \varepsilon)/g - \lfloor \tilde{k}q/m \rceil) \bmod q$, for some $\varepsilon \in (-1/2, 1/2]$. Let $\Sigma(\tilde{v}, \tilde{k}) = \{\sigma_1 \in \mathbb{Z}_q \mid \exists \varepsilon \in (-1/2, 1/2]\ s.t.\ \sigma_1 = (q(\tilde{v} - \varepsilon)/g - \lfloor \tilde{k}q/m \rceil) \bmod q\}$. Defining the map $\phi : \Sigma(\tilde{v}, 0) \to \Sigma(\tilde{v}, \tilde{k})$, by setting $\phi(x) = \left(x - \lfloor \tilde{k}q/m \rceil\right) \bmod q$. Then ϕ is obviously a one-to-one map. Hence, the cardinality of $\Sigma(\tilde{v}, \tilde{k})$ is irrelevant to $\tilde{k}$. Specifically, for arbitrary $\tilde{v} \in \mathbb{Z}_g$ and arbitrary $\tilde{k}_1, \tilde{k}_1' \in \mathbb{Z}_m$, it holds that $\left|\Sigma(\tilde{v}, \tilde{k}_1)\right| = \left|\Sigma(\tilde{v}, \tilde{k}_1')\right| = |\Sigma(\tilde{v}, 0)|$.

Now, for arbitrary $\tilde{v} \in \mathbb{Z}_g$ and arbitrary $\tilde{k} \in \mathbb{Z}_m$, when $\sigma_1 \leftarrow \mathbb{Z}_q$ we have that $\Pr[v = \tilde{v} \mid k_1 = \tilde{k}] = \Pr\left[\sigma_1 \in \Sigma(\tilde{v}, \tilde{k}) \mid k_1 = \tilde{k}\right] = |\Sigma(\tilde{v}, \tilde{k})|/q = |\Sigma(\tilde{v}, 0)|/q$. The right-hand side only depends on $\tilde{v}$, and so v is independent of k_1. □

4.2 Discussions on KC vs. AKC

Key establishment (KE) schemes based upon KC and AKC have different performances and features.

- KC-based KE corresponds to Diffie-Hellman key establishment in the lattice world, while AKC-based to El Gamal key transport.
- When deploying AKC-based KE in practice, if the randomness used by the responder (e.g., a low-power device like smart card) is poor, it will significantly ruin the session-key security. Or, if the responder is just lazy (or for economic reasons), who may re-use session-keys across multiple sessions, as demonstrated with some deployed TLS implementations in reality. In comparison, with KC-based KE, the two players play a symmetric role in generating the session-key, and thus the damage caused by poor randomness can be alleviated. In addition, symmetry is usually a desirable feature for cryptographic schemes in practice.
- On the same parameters (q, m, g) (which imply the same bandwidth), OKCN-based KE has lower error probability than AKCN-based. Or, on the same parameters (q, m, d) (which imply the same error probability), OKCN-based KE has smaller bandwidth than AKCN-based. This comparison is enabled by the upper-bounds on these parameters proved in Theorems 1 and 4.
- KC-based KE is more versatile, in the sense that it can also be straightforwardly adapted into a key transport protocol or a CPA-secure PKE scheme. Moreover, in another work [CGZ18], we show that the deterministic version of OKCN is also a fundamental building tool for lattice-based signature.

Initiator

$\mathsf{seed} \leftarrow \{0,1\}^{\kappa}$
$\mathbf{A} = \mathsf{Gen}(\mathsf{seed}) \in \mathbb{Z}_q^{n \times n}$
$\mathbf{X}_1 \leftarrow \chi^{n \times l_A}$
$\mathbf{Y}_1 = \lfloor \mathbf{A}\mathbf{X}_1 \rceil_p$

Responder

$$\xrightarrow{\mathsf{seed}, \mathbf{Y}_1 \in \mathbb{Z}_p^{n \times l_A}}$$

$\mathbf{A} = \mathsf{Gen}(\mathsf{seed})$
$\mathbf{X}_2 \leftarrow \chi^{n \times l_B}$
$\mathbf{Y}_2 = \lfloor \mathbf{A}^T \mathbf{X}_2 \rceil_p$
$\boldsymbol{\epsilon} \leftarrow [-q/2p, q/2p - 1]^{n \times l_A}$
$\mathbf{\Sigma}_2 = \mathbf{Y}_1^T \mathbf{X}_2 + \lfloor \boldsymbol{\epsilon}^T \mathbf{X}_2 \rceil_p$
$(\mathbf{K}_2, \mathbf{V}) \leftarrow \mathsf{Con}(\mathbf{\Sigma}_2, \mathsf{params})$

$$\xleftarrow{\mathbf{Y}_2 \in \mathbb{Z}_p^{n \times l_B}, \mathbf{V} \in \mathbb{Z}_g^{l_A \times l_B}}$$

$\mathbf{\Sigma}_1 = \mathbf{X}_1^T \mathbf{Y}_2$
$\mathbf{K}_1 \leftarrow \mathsf{Rec}(\mathbf{\Sigma}_1, \mathbf{V}, \mathsf{params})$

Fig. 1. LWR-based key establishment from KC, where $\mathbf{K}_1, \mathbf{K}_2 \in \mathbb{Z}_m^{l_A \times l_B}$ and $|\mathbf{K}_1| = |\mathbf{K}_2| = l_A \, l_B |m|$.

- KC-based KE is more appropriate for incorporating into the existing standards like IKE and TLS that are based on Diffie-Hellman via the SIGMA mechanism [Kra03]. We note that key transport is explicitly abandoned with TLS1.3.
- For the parameters proposed in this work, OKCN is actually (slightly) more efficient than AKCN.

For the above reasons, we focus more on KC-based key establishment (specifically, key exchange) than AKC-based in this work. Still, we aim for a unified protocol structure that can be instantiated with either KC or AKC, in order to simplify system complexity.

5 LWR-Based Key Establishment

The KC-based key establishment (KE) from the LWR problem is depicted in Fig. 1. Denote by $(n, l_A, l_B, q, p, KC, \chi)$ the system parameters, where $p|q$, and p and q are chosen to be power of 2. Let $KC = (\mathsf{params} = (p, m, g, d, aux), \mathsf{Con}, \mathsf{Rec})$ be a *correct* and *secure* key consensus scheme, χ be a small noise distribution over $\mathbb{Z}_q$, and Gen be a pseudo-random generator (PRG) generating the matrix $\mathbf{A}$ from a small seed. In the actual implementation, we use OKCN-simple as the underlying KC mechanism. For presentation simplicity, we assume $\mathbf{A} \in \mathbb{Z}_q^{n \times n}$ to be square matrix. The length of the random seed, i.e., κ, is typically set to be 256. The actual session-key is derived from $\mathbf{K}_1$ and $\mathbf{K}_2$ via some key derivation function KDF. For presentation simplicity, the functions Con and Rec are applied to matrices, meaning that they are applied to each of the coordinates respectively. For presentation simplicity, we describe the LWR-based key establishment protocol from any KC scheme. But it can be trivially adapted to work on any *correct* and *secure* AKC scheme. In this case, the responder user Bob simply chooses $\mathbf{K}_2 \leftarrow \mathbb{Z}_m^{l_A \times l_B}$, and the output of $\mathsf{Con}(\boldsymbol{\Sigma}_2, \mathbf{K}_2, \mathsf{params})$ is simply defined to be $\mathbf{V}$. The security proof of the LWR-based KE protocol is analogous to that in [Pei14,BCD+16], and is given in the full version.

5.1 Analysis of Correctness and Failure Rate

For any integer x, let $\{x\}_p$ denote $x - \frac{q}{p}\lfloor x \rceil_p$, where $\lfloor x \rceil_p = \lfloor \frac{p}{q} x \rceil$. Then, for any integer x, $\{x\}_p \in [-q/2p, q/2p - 1]$, hence $\{x\}_p$ can be naturally regarded as an element in $\mathbb{Z}_{q/p}$. In fact, $\{x\}_p$ is equal to $x \bmod q/p$, where the result is represented in $[-q/2p, q/2p-1]$. When the notation $\{\cdot\}_p$ is applied to a matrix, it means $\{\cdot\}_p$ applies to every element of the matrix respectively.

We have $\boldsymbol{\Sigma}_2 = \mathbf{Y}_1^T \mathbf{X}_2 + \lfloor \boldsymbol{\varepsilon}^T \mathbf{X}_2 \rceil_p = \lfloor \mathbf{A}\mathbf{X}_1 \rceil_p^T \mathbf{X}_2 + \lfloor \boldsymbol{\varepsilon}^T \mathbf{X}_2 \rceil_p = \frac{p}{q}(\mathbf{A}\mathbf{X}_1 - \{\mathbf{A}\mathbf{X}_1\}_p)^T \mathbf{X}_2 + \lfloor \boldsymbol{\varepsilon}^T \mathbf{X}_2 \rceil_p$. And $\boldsymbol{\Sigma}_1 = \mathbf{X}_1^T \mathbf{Y}_2 = \mathbf{X}_1^T \lfloor \mathbf{A}^T \mathbf{X}_2 \rceil_p = \frac{p}{q}(\mathbf{X}_1^T \mathbf{A}^T \mathbf{X}_2 - \mathbf{X}_1^T \{\mathbf{A}^T \mathbf{X}_2\}_p)$. Hence,

$$\begin{aligned} \boldsymbol{\Sigma}_2 - \boldsymbol{\Sigma}_1 &= \frac{p}{q}(\mathbf{X}_1^T \{\mathbf{A}^T \mathbf{X}_2\}_p - \{\mathbf{A}\mathbf{X}_1\}_p^T \mathbf{X}_2) + \lfloor \varepsilon^T \mathbf{X}_2 \rceil_p \mod p \\ &= \left\lfloor \frac{p}{q}(\mathbf{X}_1^T \{\mathbf{A}^T \mathbf{X}_2\}_p - \{\mathbf{A}\mathbf{X}_1\}_p^T \mathbf{X}_2 + \varepsilon^T \mathbf{X}_2) \right\rceil \mod p \end{aligned}$$

The general idea is that $\mathbf{X}_1, \mathbf{X}_2, \boldsymbol{\varepsilon}, \{\mathbf{A}^T \mathbf{X}_2\}_p$ and $\{\mathbf{A}\mathbf{X}_1\}_p$ are small enough, so that $\boldsymbol{\Sigma}_1$ and $\boldsymbol{\Sigma}_2$ are close. If $|\boldsymbol{\Sigma}_1 - \boldsymbol{\Sigma}_2|_p \le d$, the *correctness* of the underlying *KC* guarantees $\mathbf{K}_1 = \mathbf{K}_2$. For given concrete parameters, we numerically derive the probability of $|\boldsymbol{\Sigma}_2 - \boldsymbol{\Sigma}_1|_p > d$ by numerically calculating the distribution of $\mathbf{X}_1^T \{\mathbf{A}^T \mathbf{X}_2\}_p - (\{\mathbf{A}\mathbf{X}_1\}_p^T \mathbf{X}_2 - \varepsilon^T \mathbf{X}_2)$ for the case of $l_A = l_B = 1$, then applying the *union bound*. The independency between variables indicated by the following Theorem 7 can greatly simplify the calculation.

Let $\mathsf{Inv}(\mathbf{X}_1, \mathbf{X}_2)$ denote the event that there exist invertible elements of ring $\mathbb{Z}_{q/p}$ in both vectors $\mathbf{X}_1$ and $\mathbf{X}_2$. We claim that $\mathsf{Inv}(\mathbf{X}_1, \mathbf{X}_2)$ happens with *overwhelming* probability. This claim follows from $\Pr[\mathsf{Inv}(\mathbf{X}_1, \mathbf{X}_2)] = 1 - \Pr[\text{all entries of } \mathbf{X}_1, \mathbf{X}_2 \text{ are non-invertible in } \mathbb{Z}_{q/p}] = 1 - \Pr[x \leftarrow \chi : x \text{ is non-}\mathit{invertible}]^{n \cdot (l_A + l_B)}$. In our application, $\Pr[x \leftarrow \chi : x \text{ is non-invertible}]$ is far from one, hence, $\mathsf{Inv}(\mathbf{X}_1, \mathbf{X}_2)$ holds with overwhelming probability.

Lemma 1. *Consider the case of $l_A = l_B = 1$. For any $a \in \mathbb{Z}_{q/p}, \mathbf{x} \in \mathbb{Z}_{q/p}^n$, denote $S_{\mathbf{x},a} = \{\mathbf{y} \in \mathbb{Z}_{q/p}^n \mid \mathbf{x}^T \mathbf{y} \bmod (q/p) = a\}$. For any fixed $a \in \mathbb{Z}_{q/p}$, conditioned on $\mathsf{Inv}(\mathbf{X}_1, \mathbf{X}_2)$ and $\mathbf{X}_1^T \mathbf{A}^T \mathbf{X}_2 \bmod (q/p) = a$, the random vectors $\{\mathbf{A}^T \mathbf{X}_2\}_p$ and $\{\mathbf{A}\mathbf{X}_1\}_p$ are independent, and are subjected to uniform distribution over $S_{\mathbf{X}_1,a}, S_{\mathbf{X}_2,a}$ respectively.*

Proof. Under the condition of $\mathsf{Inv}(\mathbf{X}_1, \mathbf{X}_2)$, for any fixed $\mathbf{X}_1$ and $\mathbf{X}_2$, define the map $\phi_{\mathbf{X}_1,\mathbf{X}_2} \colon \mathbb{Z}_q^{n \times n} \to \mathbb{Z}_{q/p}^n \times \mathbb{Z}_{q/p}^n$, such that $\mathbf{A} \mapsto (\{\mathbf{A}\mathbf{X}_1\}_p, \{\mathbf{A}^T \mathbf{X}_2\}_p)$.

We shall prove that the image of $\phi_{\mathbf{X}_1,\mathbf{X}_2}$ is $S = \{(\mathbf{y}_1, \mathbf{y}_2) \in \mathbb{Z}_{q/p}^n \times \mathbb{Z}_{q/p}^n \mid \mathbf{X}_2^T \mathbf{y}_1 = \mathbf{X}_1^T \mathbf{y}_2 \mod (q/p)\}$. Denote $\mathbf{X}_1 = (x_1, \mathbf{X}_1'^T)^T$ and $\mathbf{y}_2 = (y_2, \mathbf{y}_2'^T)^T$.

Without loss of generality, we assume x_1 is invertible in the ring $\mathbb{Z}_{q/p}$. For any $(\mathbf{y}_1, \mathbf{y}_2) \in S$, we need to find an $\mathbf{A}$ such that $\phi_{\mathbf{X}_1,\mathbf{X}_2}(\mathbf{A}) = (\mathbf{y}_1, \mathbf{y}_2)$.

From the condition $\mathsf{Inv}(\mathbf{X}_1, \mathbf{X}_2)$, we know that there exists an $\mathbf{A}' \in \mathbb{Z}^{(n-1)\times n}$ such that $\{\mathbf{A}'\mathbf{X}_2\}_p = \mathbf{y}_2'$. Then, we let $\mathbf{a}_1 = x_1^{-1}(\mathbf{y}_1 - \mathbf{A}'^T\mathbf{X}_1') \bmod (q/p)$, and $\mathbf{A} = (\mathbf{a}_1, \mathbf{A}'^T)$. Now we check that $\phi_{\mathbf{X}_1,\mathbf{X}_2}(\mathbf{A}) = (\mathbf{y}_1, \mathbf{y}_2)$.

$$\{\mathbf{A}\mathbf{X}_1\}_p = \left\{ \begin{pmatrix} \mathbf{a}_1 & \mathbf{A}'^T \end{pmatrix} \begin{pmatrix} x_1 \\ \mathbf{x}_1' \end{pmatrix} \right\}_p = \{x_1\mathbf{a}_1 + \mathbf{A}'^T\mathbf{X}_1'\}_p = \mathbf{y}_1$$

$$\begin{aligned} \{\mathbf{A}^T\mathbf{X}_2\}_p &= \left\{ \begin{pmatrix} \mathbf{a}_1^T \\ \mathbf{A}' \end{pmatrix} \mathbf{X}_2 \right\}_p = \left\{ \begin{pmatrix} \mathbf{a}_1^T\mathbf{X}_2 \\ \mathbf{A}'\mathbf{X}_2 \end{pmatrix} \right\}_p = \left\{ \begin{pmatrix} x_1^{-1}(\mathbf{y}_1^T - \mathbf{X}_1'^T\mathbf{A})\mathbf{X}_2 \\ \mathbf{A}'\mathbf{X}_2 \end{pmatrix} \right\}_p \\ &= \left\{ \begin{pmatrix} x_1^{-1}(\mathbf{X}_1^T\mathbf{y}_2 - \mathbf{X}_1'^T\mathbf{y}_2') \\ \mathbf{y}_2' \end{pmatrix} \right\}_p = \left\{ \begin{pmatrix} y_2 \\ \mathbf{y}_2' \end{pmatrix} \right\}_p = \mathbf{y}_2 \end{aligned}$$

Hence, if we treat $\mathbb{Z}_q^{n\times n}$ and S as $\mathbb{Z}$-modules, then $\phi_{\mathbf{X}_1,\mathbf{X}_2} : \mathbb{Z}_q^{n\times n} \to S$ is a surjective homomorphism. Then, for any fixed $(\mathbf{X}_1, \mathbf{X}_2)$, $(\{\mathbf{A}\mathbf{X}_1\}_p, \{\mathbf{A}^T\mathbf{X}_2\}_p)$ is uniformly distributed over S. This completes the proof. □

Theorem 7. *Under the condition* $\mathsf{Inv}(\mathbf{X}_1, \mathbf{X}_2)$, *the following two distributions are identical:*

- $(a, \mathbf{X}_1, \mathbf{X}_2, \{\mathbf{A}\mathbf{X}_1\}_p, \{\mathbf{A}^T\mathbf{X}_2\}_p)$, *where* $\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times n}$, $\mathbf{X}_1 \leftarrow \chi^n$, $\mathbf{X}_2 \leftarrow \chi^n$, *and* $a = \mathbf{X}_1^T\mathbf{A}^T\mathbf{X}_2 \bmod (q/p)$.
- $(a, \mathbf{X}_1, \mathbf{X}_2, \mathbf{y}_1, \mathbf{y}_2)$, *where* $a \leftarrow \mathbb{Z}_{q/p}, \mathbf{X}_1 \leftarrow \chi^n$, $\mathbf{X}_2 \leftarrow \chi^n$, $\mathbf{y}_1 \leftarrow S_{\mathbf{X}_2,a}$, *and* $\mathbf{y}_2 \leftarrow S_{\mathbf{X}_1,a}$.

Proof. For any $\tilde{a} \in \mathbb{Z}_{q/p}$, $\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2 \in \mathsf{Supp}(\chi^n)$, $\tilde{\mathbf{y}}_1, \tilde{\mathbf{y}}_2 \in \mathbb{Z}_{q/p}^n$, we have

$$\begin{aligned} &\Pr[a = \tilde{a}, \mathbf{X}_1 = \tilde{\mathbf{X}}_1, \mathbf{X}_2 = \tilde{\mathbf{X}}_2, \{\mathbf{A}\mathbf{X}_1\}_p = \tilde{\mathbf{y}}_1, \{\mathbf{A}^T\mathbf{X}_2\}_p = \tilde{\mathbf{y}}_2 \mid \mathsf{Inv}(\mathbf{X}_1, \mathbf{X}_2)] \\ =&\Pr[\{\mathbf{A}\mathbf{X}_1\}_p = \tilde{\mathbf{y}}_1, \{\mathbf{A}^T\mathbf{X}_2\}_p = \tilde{\mathbf{y}}_2 \mid a = \tilde{a}, \mathbf{X}_1 = \tilde{\mathbf{X}}_1, \mathbf{X}_2 = \tilde{\mathbf{X}}_2, \mathsf{Inv}(\mathbf{X}_1, \mathbf{X}_2)] \\ &\Pr[a = \tilde{a}, \mathbf{X}_1 = \tilde{\mathbf{X}}_1, \mathbf{X}_2 = \tilde{\mathbf{X}}_2 \mid \mathsf{Inv}(\mathbf{X}_1, \mathbf{X}_2)] \end{aligned}$$

From Lemma 1, the first term equals to $\Pr[\mathbf{y}_1 \leftarrow S_{\tilde{\mathbf{X}}_2,\tilde{a}}; \mathbf{y}_2 \leftarrow S_{\tilde{\mathbf{X}}_1,\tilde{a}} : \mathbf{y}_1 = \tilde{\mathbf{y}}_1, \mathbf{y}_2 = \tilde{\mathbf{y}}_2 \mid a = \tilde{a}, \mathbf{X}_1 = \tilde{\mathbf{X}}_1, \mathbf{X}_2 = \tilde{\mathbf{X}}_2, \mathsf{Inv}(\mathbf{X}_1, \mathbf{X}_2)]$.

For the second term, we shall prove that a is independent of $(\mathbf{X}_1, \mathbf{X}_2)$, and is uniformly distributed over $\mathbb{Z}_{q/p}$. Under the condition of $\mathsf{Inv}(\mathbf{X}_1, \mathbf{X}_2)$, the map $\mathbb{Z}_q^{n\times n} \to \mathbb{Z}_{q/p}$, such that $\mathbf{A} \mapsto \mathbf{X}_1^T\mathbf{A}^T\mathbf{X}_2 \bmod (q/p)$, is a surjective homomorphism between the two $\mathbb{Z}$-modules. Then, $\Pr[a = \tilde{a} \mid \mathbf{X}_1 = \tilde{\mathbf{X}}_1, \mathbf{X}_2 = \tilde{\mathbf{X}}_2, \mathsf{Inv}(\mathbf{X}_1, \mathbf{X}_2)] = p/q$. Hence, under the condition of $\mathsf{Inv}(\mathbf{X}_1, \mathbf{X}_2)$, a is independent of $(\mathbf{X}_1, \mathbf{X}_2)$, and is distributed uniformly at random. So the two ways of sampling result in the same distribution. □

We design and implement the following algorithm to numerically calculate the distribution of $\boldsymbol{\Sigma}_2 - \boldsymbol{\Sigma}_1$ efficiently. For any $c_1, c_2 \in \mathbb{Z}_q, a \in \mathbb{Z}_{q/p}$, we numerically calculate $\Pr[\mathbf{X}_1^T\{\mathbf{A}^T\mathbf{X}_2\}_p = c_1]$ and $\Pr[\{\mathbf{A}\mathbf{X}_1\}_p^T\mathbf{X}_2 - \boldsymbol{\varepsilon}^T\mathbf{X}_2 = c_2, \mathbf{X}_1^T\mathbf{A}^T\mathbf{X}_2 \bmod (q/p) = a]$, then derive the distribution of $\boldsymbol{\Sigma}_2 - \boldsymbol{\Sigma}_1$.

As $\mathsf{Inv}(\mathbf{X}_1, \mathbf{X}_2)$ occurs with *overwhelming* probability, for any event E, we have $|\Pr[E] - \Pr[E|\mathsf{Inv}(\mathbf{X}_1, \mathbf{X}_2)]| < negl$. For simplicity, we ignore the effect of $\mathsf{Inv}(\mathbf{X}_1, \mathbf{X}_2)$ in the following calculations. By Theorem 7, $\Pr[\mathbf{X}_1^T\{\mathbf{A}^T\mathbf{X}_2\}_p = c_1] = \Pr[\mathbf{X}_1 \leftarrow \chi^n, \mathbf{y}_2 \leftarrow \mathbb{Z}_{q/p}^n; \mathbf{X}_1^T\mathbf{y}_2 = c_1]$. This probability can be numerically calculated by computer programs. The probability $\Pr[\{\mathbf{A}\mathbf{X}_1\}_p^T\mathbf{X}_2 - \boldsymbol{\varepsilon}^T\mathbf{X}_2 = c_2, \mathbf{X}_1^T\mathbf{A}^T\mathbf{X}_2 \bmod (q/p) = a]$ can also be calculated by the similar way. Then, for arbitrary $c \in \mathbb{Z}_q$,

$$\begin{aligned}
&\Pr[\boldsymbol{\Sigma}_1 - \boldsymbol{\Sigma}_2 = c] = \Pr[\mathbf{X}_1^T\{\mathbf{A}^T\mathbf{X}_2\}_p - \{\mathbf{A}\mathbf{X}_1\}_p^T\mathbf{X}_2 + \varepsilon^T\mathbf{X}_2 = c] \\
&= \sum_{\substack{c_1 - c_2 = c \\ a \in \mathbb{Z}_{q/p}}} \begin{matrix} \Pr[\mathbf{X}_1^T\{\mathbf{A}^T\mathbf{X}_2\}_p = c_1, \{\mathbf{A}\mathbf{X}_1\}_p^T\mathbf{X}_2 - \varepsilon^T\mathbf{X}_2 = c_2 | \mathbf{X}_1^T\mathbf{A}^T\mathbf{X}_2 \bmod (q/p) = a] \cdot \\ \Pr[\mathbf{X}_1^T\mathbf{A}^T\mathbf{X}_2 \bmod (q/p) = a] \end{matrix} \\
&= \sum_{\substack{c_1 - c_2 = c \\ a \in \mathbb{Z}_{q/p}}} \begin{matrix} \Pr[\mathbf{X}_1^T\{\mathbf{A}^T\mathbf{X}_2\}_p = c_1 | \mathbf{X}_1^T\mathbf{A}^T\mathbf{X}_2 \bmod (q/p) = a] \cdot \\ \Pr[\{\mathbf{A}\mathbf{X}_1\}_p^T\mathbf{X}_2 - \varepsilon^T\mathbf{X}_2 = c_2 | \mathbf{X}_1^T\mathbf{A}^T\mathbf{X}_2 \bmod (q/p) = a] \Pr[\mathbf{X}_1^T\mathbf{A}^T\mathbf{X}_2 \bmod (q/p) = a] \end{matrix} \\
&= \sum_{\substack{a \in \mathbb{Z}_{q/p} \\ c_1 - c_2 = c}} \frac{\Pr[\mathbf{X}_1^T\{\mathbf{A}^T\mathbf{X}_2\}_p = c_1, c_1 \bmod (q/p) = a] \Pr[\{\mathbf{A}\mathbf{X}_1\}_p^T\mathbf{X}_2 - \varepsilon^T\mathbf{X}_2 = c_2, \mathbf{X}_1^T\mathbf{A}^T\mathbf{X}_2 \bmod (q/p) = a]}{\Pr[\mathbf{X}_1^T\mathbf{A}^T\mathbf{X}_2 \bmod (q/p) = a]} \\
&= \sum_{\substack{a \in \mathbb{Z}_{q/p} \\ c_1 - c_2 = c \\ c_1 \bmod (q/p) = a}} \frac{\Pr[\mathbf{X}_1^T\{\mathbf{A}^T\mathbf{X}_2\}_p = c_1] \Pr[\{\mathbf{A}\mathbf{X}_1\}_p^T\mathbf{X}_2 - \varepsilon^T\mathbf{X}_2 = c_2, \mathbf{X}_1^T\mathbf{A}^T\mathbf{X}_2 \bmod (q/p) = a]}{\Pr[\mathbf{X}_1^T\mathbf{A}^T\mathbf{X}_2 \bmod (q/p) = a]}
\end{aligned}$$

By Theorem 7, conditioned on $\mathsf{Inv}(\mathbf{X}_1, \mathbf{X}_2)$ and $\mathbf{X}_1^T\mathbf{A}^T\mathbf{X}_2 \bmod (q/p) = a$, $\mathbf{X}_1^T\{\mathbf{A}^T\mathbf{X}_2\}_p$ is independent of $\{\mathbf{A}\mathbf{X}_1\}_p^T\mathbf{X}_2 - \boldsymbol{\varepsilon}^T\mathbf{X}_2$, which implies the second equality. The scripts are available from http://github.com/OKCN.

5.2 Parameter Selection and Evaluation

It is suggested in [ADPS16,BCD+16] that rounded Gaussian distribution can be replaced by discrete distribution that is very close to rounded Gaussian in the sense of Rényi divergence [BLL+15] (Table 1).

Table 1. Discrete distributions of every component in the LWR secret. We choose the standard variances "var." large enough to prevent potential combinational attacks.

dist.	Bits	var.	Probability of							Order	Divergence
			0	±1	±2	±3	±4	±5	±6		
D_R	16	2.00	18110	14249	6938	2090	389	44	3	500.0	1.0000270
D_P	16	1.40	21456	15326	5580	1033	97	4	0	500.0	1.0000277

Security Estimation. The dual attack tries to distinguish the distribution of LWE samples and the uniform distribution. Suppose $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}) \in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$ is an LWE sample, where $\mathbf{s}$ and $\mathbf{e}$ are drawn from discrete Gaussian of variance σ_s^2 and σ_e^2 respectively. Then we choose a positive real $c \in \mathbb{R}, 0 < c \leq q$, and construct $L_c(\mathbf{A}) = \{(\mathbf{x}, \mathbf{y}/c) \in \mathbb{Z}^m \times (\mathbb{Z}/c)^n \mid \mathbf{x}^T\mathbf{A} = \mathbf{y}^T \mod q\}$, which is a

Table 2. Parameters for LWR-Based key establishment with OKCN-simple. "bw." refers to the bandwidth in kilo-bytes. "err." refers to the overall error rate that is calculated by the algorithm developed in Sect. 5.1. "$|\mathbf{K}|$" refers to the length of consensus bits.

	n	q	p	l	m	g	distr.	bw.	err.	$\|\mathbf{K}\|$
Recommended	672	2^{15}	2^{12}	8	2^4	2^8	D_R	16.19	2^{-30}	256
Paranoid	832	2^{15}	2^{12}	8	2^4	2^8	D_P	20.03	2^{-34}	256

lattice with dimension $m+n$ and determinant $(q/c)^n$. For a short vector $(\mathbf{x}, \mathbf{y}) \in L_c(\mathbf{A})$ found by the BKZ algorithm, we have $\mathbf{x}^T\mathbf{b} = \mathbf{x}^T(\mathbf{A}\mathbf{s}+\mathbf{e}) = c \cdot \mathbf{y}^T\mathbf{s} + \mathbf{x}^T\mathbf{e} \mod q$. If $(\mathbf{A}, \mathbf{b})$ is an LWE sample, the distribution of the right-hand side will be very close to a Gaussian of standard deviation $\sqrt{c^2\|\mathbf{y}\|^2\sigma_s^2 + \|\mathbf{x}\|^2\sigma_e^2}$, otherwise the distribution will be uniform. $\|(\mathbf{x}, \mathbf{y})\|$ is about $\delta_0^{m+n}(q/c)^{\frac{n}{m+n}}$, where δ_0 is the root Hermite factor. We heuristically assume that $\|\mathbf{x}\| = \sqrt{\frac{m}{m+n}}\,\|(\mathbf{x}, \mathbf{y})\|$, and $\|\mathbf{y}\| = \sqrt{\frac{n}{m+n}}\,\|(\mathbf{x}, \mathbf{y})\|$. Then we can choose $c = \sigma_e/\sigma_s$ that minimizes the standard deviation of $\mathbf{x}^T\mathbf{b}$. The advantage of distinguishing $\mathbf{x}^T\mathbf{b}$ from uniform distribution is $\varepsilon = 4\exp(-2\pi^2\tau^2)$, where $\tau = \sqrt{c^2\|\mathbf{y}\|^2\sigma_s^2 + \|\mathbf{x}\|^2\sigma_e^2}/q$. This attack must be repeated $R = \max\{1, 1/(2^{0.2075b}\varepsilon^2)\}$ times to be successful.

The primal attack reduces the LWE problem to the unique-SVP problem. Let $\Lambda_w(\mathbf{A}) = \{(\mathbf{x}, \mathbf{y}, z) \in \mathbb{Z}^n \times (\mathbb{Z}^m/w) \times \mathbb{Z} \mid \mathbf{A}\mathbf{x} + w\mathbf{y} = z\mathbf{b} \mod q\}$, and a vector $\mathbf{v} = (\mathbf{s}, \mathbf{e}/w, 1) \in \Lambda_w(\mathbf{A})$. $\Lambda_w(\mathbf{A})$ is a lattice of $d = m + n + 1$ dimensions, and its determinant is $(q/w)^m$. From geometry series assumption, we can derive $\|\mathbf{b}_i^*\| \approx \delta_0^{d-2i-1}\det(\Lambda_w(\mathbf{A}))^{1/d}$. We heuristically assume that the length of projection of $\mathbf{v}$ onto the vector space spanned by the last b Gram-Schmidt vectors is about $\sqrt{\frac{b}{d}}\,\|(\mathbf{s}, \mathbf{e}/w, 1)\| \approx \sqrt{\frac{b}{d}\,(n\sigma_s^2 + m\sigma_e^2/w^2 + 1)}$. If this length is shorter than $\|\mathbf{b}_{d-b}^*\|$, this attack can be successful. Hence, the successful condition is $\sqrt{\frac{b}{d}\,(n\sigma_s^2 + m\sigma_e^2/w^2 + 1)} \le \delta_0^{2b-d-1}\left(\frac{q}{w}\right)^{m/d}$. We know that the optimal w balancing the secret $\mathbf{s}$ and the noise $\mathbf{e}$ is about σ_e/σ_s.

We aim at providing parameter sets for long term security, and estimate the concrete security *in a more conservative way* than [APS15] from the defender's point of view. We first consider the attacks of LWE whose secret and noise have different variances. Then, we treat the LWR problem as a special LWE problem whose noise is uniformly distributed over $[-q/2p, q/2p-1]$. In our security estimation, we simply ignore the difference between the discrete distribution and the rounded Gaussian, on the following grounds: the dual attack and the primal attack only concern about the standard deviation, and the Rényi divergence between the two distributions is very small (Table 3).

Table 3. Security estimation of the parameters described in Table 2. "C, Q, P" stand for "Classical, Quantum, Plausible" respectively.

Scheme	Attack	m'	b	C	Q	P
Recommended	Primal	665	459	143	**131**	104
	Dual	633	456	142	**130**	103
Paranoid	Primal	768	584	180	164	**130**
	Dual	746	580	179	163	**129**

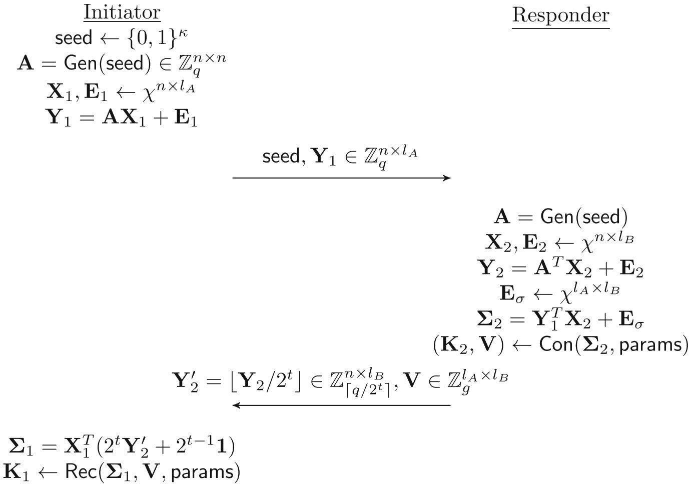
Initiator
$\mathsf{seed} \leftarrow \{0,1\}^{\kappa}$
$\mathbf{A} = \mathsf{Gen}(\mathsf{seed}) \in \mathbb{Z}_q^{n\times n}$
$\mathbf{X}_1, \mathbf{E}_1 \leftarrow \chi^{n\times l_A}$
$\mathbf{Y}_1 = \mathbf{A}\mathbf{X}_1 + \mathbf{E}_1$
Responder
$\mathsf{seed}, \mathbf{Y}_1 \in \mathbb{Z}_q^{n\times l_A}$
$\mathbf{A} = \mathsf{Gen}(\mathsf{seed})$
$\mathbf{X}_2, \mathbf{E}_2 \leftarrow \chi^{n\times l_B}$
$\mathbf{Y}_2 = \mathbf{A}^T\mathbf{X}_2 + \mathbf{E}_2$
$\mathbf{E}_\sigma \leftarrow \chi^{l_A\times l_B}$
$\mathbf{\Sigma}_2 = \mathbf{Y}_1^T\mathbf{X}_2 + \mathbf{E}_\sigma$
$(\mathbf{K}_2, \mathbf{V}) \leftarrow \mathsf{Con}(\mathbf{\Sigma}_2, \mathsf{params})$
$\mathbf{Y}_2' = \lfloor \mathbf{Y}_2/2^t \rfloor \in \mathbb{Z}_{\lceil q/2^t \rceil}^{n\times l_B}, \mathbf{V} \in \mathbb{Z}_g^{l_A\times l_B}$
$\mathbf{\Sigma}_1 = \mathbf{X}_1^T(2^t\mathbf{Y}_2' + 2^{t-1}\mathbf{1})$
$\mathbf{K}_1 \leftarrow \mathsf{Rec}(\mathbf{\Sigma}_1, \mathbf{V}, \mathsf{params})$

Fig. 2. LWE-based key establishment from KC and AKC, where $\mathbf{K}_1, \mathbf{K}_2 \in \mathbb{Z}_m^{l_A\times l_B}$ and $|\mathbf{K}_1| = |\mathbf{K}_2| = l_A\, l_B |m|$. $\mathbf{1}$ refers to the matrix which every elements are 1.

6 LWE-Based Key Establishment

In this section, following the protocol structure in [Pei14, ADPS16, BCD+16], we present the applications of OKCN and AKCN to key establishment protocols based on LWE. Denote by $(\lambda, n, q, \chi, KC, l_A, l_B, t)$ the underlying parameters, where λ is the security parameter, $q \geq 2$, n, l_A and l_B are positive integers that are polynomial in λ (for protocol symmetry, l_A and l_B are usually set to be equal and are actually small constant). To save bandwidth, we cut off t least significant bits of $\mathbf{Y}_2$ before sending it to Alice.

Let $KC = (\mathsf{params}, \mathsf{Con}, \mathsf{Rec})$ be a *correct* and *secure* KC scheme, where params is set to be (q, g, m, d). The KC-based key establishment protocol from LWE is depicted in Fig. 2, and the actual session-key is derived from $\mathbf{K}_1$ and $\mathbf{K}_2$ via some key derivation function KDF. There, for presentation simplicity, the Con and Rec functions are applied to matrices, meaning they are applied to each of the coordinates separately. Note that $2^t\mathbf{Y}_2' + 2^{t-1}\mathbf{1}$ is an approximation of $\mathbf{Y}_2$, so we have $\boldsymbol{\Sigma}_1 \approx \mathbf{X}_1^T\mathbf{Y}_2 = \mathbf{X}_1^T\mathbf{A}^T\mathbf{X}_2 + \mathbf{X}_1^T\mathbf{E}_2$, $\boldsymbol{\Sigma}_2 = \mathbf{Y}_1^T\mathbf{X}_2 + \mathbf{E}_\sigma =$

$\mathbf{X}_1^T\mathbf{A}^T\mathbf{X}_2 + \mathbf{E}_1^T\mathbf{X}_2 + \mathbf{E}_\sigma$. As we choose $\mathbf{X}_1, \mathbf{X}_2, \mathbf{E}_1, \mathbf{E}_2, \mathbf{E}_\sigma$ according to a small noise distribution χ, the main part of $\boldsymbol{\Sigma}_1$ and that of $\boldsymbol{\Sigma}_2$ are the same $\mathbf{X}_1^T\mathbf{A}^T\mathbf{X}_2$. Hence, the corresponding coordinates of $\boldsymbol{\Sigma}_1$ and $\boldsymbol{\Sigma}_2$ are close in the sense of $|\cdot|_q$, from which some key consensus can be reached. The failure probability depends upon the number of bits we cut t, the underlying distribution χ and the distance parameter d, which will be analyzed in detail in subsequent sections. In the following security definition and analysis, we simply assume that the output of the PRG Gen is truly random. For presentation simplicity, we have described the LWE-based key establishment protocol from a KC scheme. But it can be straightforwardly adapted to work on any correct and secure AKC scheme, as clarified in Sect. 5.

6.1 Noise Distributions and Correctness

For a *correct* KC with parameter d, if the distance of corresponding elements of $\boldsymbol{\Sigma}_1$ and $\boldsymbol{\Sigma}_2$ is less than d in the sense of $|\cdot|_q$, then the scheme depicted in Fig. 2 is correct. Denote $\varepsilon(\mathbf{Y}_2) = 2^t\lfloor \mathbf{Y}_2/2^t \rfloor + 2^{t-1}\mathbf{1} - \mathbf{Y}_2$. Then

$$\begin{aligned}\boldsymbol{\Sigma}_1 - \boldsymbol{\Sigma}_2 &= \mathbf{X}_1^T(2^t\mathbf{Y}_2' + 2^{t-1}\mathbf{1}) - \mathbf{Y}_1^T\mathbf{X}_2 - \mathbf{E}_\sigma \\ &= \mathbf{X}_1^T(\mathbf{Y}_2 + \varepsilon(\mathbf{Y}_2)) - \mathbf{Y}_1^T\mathbf{X}_2 - \mathbf{E}_\sigma \\ &= \mathbf{X}_1^T(\mathbf{A}^T\mathbf{X}_2 + \mathbf{E}_2 + \varepsilon(\mathbf{Y}_2)) - (\mathbf{A}\mathbf{X}_1 + \mathbf{E}_1)^T\mathbf{X}_2 - \mathbf{E}_\sigma \\ &= \mathbf{X}_1^T(\mathbf{E}_2 + \varepsilon(\mathbf{Y}_2)) - \mathbf{E}_1^T\mathbf{X}_2 - \mathbf{E}_\sigma\end{aligned}$$

We consider each pair of elements in matrix $\boldsymbol{\Sigma}_1, \boldsymbol{\Sigma}_2$ separately, then derive the overall error rate by *union bound*. Now, we only need to consider the case $l_A = l_B = 1$. In this case, $\mathbf{X}_i, \mathbf{E}_i, \mathbf{Y}_i, (i = 1, 2)$ are column vectors in $\mathbb{Z}_q^n$, and $\mathbf{E}_\sigma \in \mathbb{Z}_q$.

If $\mathbf{Y}_2$ is independent of $(\mathbf{X}_2, \mathbf{E}_2)$, then we can directly calculate the distribution of $\boldsymbol{\sigma}_1 - \boldsymbol{\sigma}_2$. But now $\mathbf{Y}_2$ depends on $(\mathbf{X}_2, \mathbf{E}_2)$. To overcome this difficulty, we show that $\mathbf{Y}_2$ is independent of $(\mathbf{X}_2, \mathbf{E}_2)$ under a condition of $\mathbf{X}_2$ that happens with very high probability.

Proposition 1. *For any positive integer q, n, and a column vector $\mathbf{s} \in \mathbb{Z}_q^n$, let $\phi_\mathbf{s}$ denote the map $\mathbb{Z}_q^n \to \mathbb{Z}_q : \phi_\mathbf{s}(\mathbf{x}) = \mathbf{x}^T\mathbf{s}$. If there exits a coordinate of $\mathbf{s}$ which is not* zero divisor *in ring $\mathbb{Z}_q$, then map $\phi_\mathbf{s}$ is surjective.*

For a column vector $\mathbf{s}$ composed by random variables, denote by $F(\mathbf{s})$ the event that $\phi_\mathbf{s}$ is surjective. The following proposition gives a lower bound of probability of $F(\mathbf{s})$, where $\mathbf{s} \leftarrow \chi^n$. In our application, this lower bound is very close to 1.

Proposition 2. *Let p_0 be the probability that e is a* zero divisor *in ring $\mathbb{Z}_q$, where e is subject to χ. Then* $\Pr[\mathbf{s} \leftarrow \chi^n : F(\mathbf{s})] \geq 1 - p_0^n$

Theorem 8. *If $\mathbf{s}, \mathbf{e} \leftarrow \chi^n, \mathbf{A} \leftarrow \mathbb{Z}_q^{n\times n}, \mathbf{y} = \mathbf{A}\mathbf{s} + \mathbf{e} \in \mathbb{Z}_q^n$, then under the condition $F(\mathbf{s})$, $\mathbf{y}$ is independent of $(\mathbf{s}, \mathbf{e})$, and is uniformly distributed over $\mathbb{Z}_q^n$.*

Proof. For all $\tilde{\mathbf{y}}, \tilde{\mathbf{s}}, \tilde{\mathbf{e}}$, $\Pr[\mathbf{y} = \tilde{\mathbf{y}} \mid \mathbf{s} = \tilde{\mathbf{s}}, \mathbf{e} = \tilde{\mathbf{e}}, F(\mathbf{s})] = \Pr[\mathbf{A}\tilde{\mathbf{s}} = \tilde{\mathbf{y}} - \tilde{\mathbf{e}} \mid \mathbf{s} = \tilde{\mathbf{s}}, \mathbf{e} = \tilde{\mathbf{e}}, F(\mathbf{s})]$. Let $\mathbf{A} = (\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n)^T, \tilde{\mathbf{y}} - \tilde{\mathbf{e}} = (c_1, c_2, \ldots, c_n)^T$, where $\mathbf{a}_i \in \mathbb{Z}_q^n$, and $c_i \in \mathbb{Z}_q$, for every $1 \leq i \leq n$. Since $\phi_{\mathbf{s}}$ is surjective, the number of possible choices of $\mathbf{a}_i$, satisfying $\mathbf{a}_i^T \cdot \tilde{\mathbf{s}} = c_i$, is $|\mathrm{Ker}\phi_{\mathbf{s}}| = q^{n-1}$. Hence, $\Pr[\mathbf{A}\tilde{\mathbf{s}} = \tilde{\mathbf{y}} - \tilde{\mathbf{e}} \mid \mathbf{s} = \tilde{\mathbf{s}}, \mathbf{e} = \tilde{\mathbf{e}}, F(\mathbf{s})] = (q^{n-1})^n / q^{n^2} = 1/q^n$. Since the right-hand side is the constant $1/q^n$, the distribution of $\mathbf{y}$ is uniform over $\mathbb{Z}_q^n$, and is irrelevant of $(\mathbf{s}, \mathbf{e})$. □

We now begin to analyze the error rate of the scheme presented in Fig. 2.

Denote by E the event $|\mathbf{X}_1^T(\mathbf{E}_2 + \varepsilon(\mathbf{Y}_2)) - \mathbf{E}_1^T\mathbf{X}_2 - \mathbf{E}_\sigma|_q > d$. Then $\Pr[E] = \Pr[E|F(\mathbf{S})]\ \Pr[F(\mathbf{S})] + \Pr[E|\neg F(\mathbf{S})]\ \Pr[\neg F(\mathbf{S})]$. From Theorem 8, we replace $\mathbf{Y}_2 = \mathbf{A}^T\mathbf{X}_2 + \mathbf{E}_2$ in the event $E|F(\mathbf{S})$ with uniformly distributed $\mathbf{Y}_2$. Then,

$$\begin{aligned}
\Pr[E] &= \Pr[\mathbf{Y}_2 \leftarrow \mathbb{Z}_q^n : E|F(\mathbf{S})]\ \Pr[F(\mathbf{S})] + \Pr[E|\neg F(\mathbf{S})]\ \Pr[\neg F(\mathbf{S})] \\
&= \Pr[\mathbf{Y}_2 \leftarrow \mathbb{Z}_q^n : E|F(\mathbf{S})]\ \Pr[F(\mathbf{S})] + \Pr[\mathbf{Y}_2 \leftarrow \mathbb{Z}_q^n : E|\neg F(\mathbf{S})]\ \Pr[\neg F(\mathbf{S})] \\
&\quad + \Pr[E|\neg F(\mathbf{S})]\ \Pr[\neg F(\mathbf{S})] - \Pr[\mathbf{Y}_2 \leftarrow \mathbb{Z}_q^n : E|\neg F(\mathbf{S})]\ \Pr[\neg F(\mathbf{S})] \\
&= \Pr[\mathbf{Y}_2 \leftarrow \mathbb{Z}_q^n : E] + \varepsilon
\end{aligned}$$

where $|\varepsilon| \leq \Pr[\neg F(\mathbf{S})]$. In our application, p_0 is far from 1, and n is very large, by Theorem 2, ε is very small, so we simply ignore ε. If $\mathbf{Y}_2$ is uniformly distributed, then $\varepsilon(\mathbf{Y}_2)$ is a centered uniform distribution. Then, the distribution of $\mathbf{X}_1^T(\mathbf{E}_2 + \varepsilon(\mathbf{Y}_2)) - \mathbf{E}_1^T\mathbf{X}_2 - \mathbf{E}_\sigma$ can be directly computed by programs.

Discrete Distributions. In this work, for LWE-based key establishment, we use the following discrete distributions, which are specified in Table 4, where "bits" refers to the number of bits required to sample the distribution and "var." means the standard variation of the Gaussian distribution approximated.

Table 4. Discrete distributions proposed in this work, and their Rényi divergences.

dist.	Bits	var.	Probability of						Order	Divergence
			0	±1	±2	±3	±4	±5		
D_1	8	1.10	94	62	17	2			15.0	1.0015832
D_2	12	0.90	1646	992	216	17			75.0	1.0003146
D_3	12	1.66	1238	929	393	94	12	1	30.0	1.0002034
D_4	16	1.66	19794	14865	6292	1499	200	15	500.0	1.0000274
D_5	16	1.30	22218	15490	5242	858	67	2	500.0	1.0000337

Instantiations, and Comparisons with Frodo. For "OKCN simple" proposed in Algorithm 2, it achieves a tight parameter constraint, specifically, $2md < q$. In comparison, the parameter constraint achieved by Frodo is $4md < q$. As we shall see, such a difference is one source that allows us to achieve better trade-offs among error probability, security, (computational and bandwidth) efficiency, and consensus range. In particular, it allows us to use q that is one bit shorter than that used in Frodo. Beyond saving bandwidth, employing a one-bit shorter q also much improves the computational efficiency (as the matrix $\mathbf{A}$ becomes shorter, and consequently the cost of generating $\mathbf{A}$ and the related matrix operations are more efficient), and can render stronger security levels simultaneously. Here, we briefly highlight one performance comparison: OKCN-T2 (resp., Frodo-recommended) has 18.58kB (resp., 22.57kB) bandwidth, 887.15kB (resp., 1060.32kB) matrix $\mathbf{A}$, at least 134-bit (resp., 130-bit) quantum security, and error rate 2^{-39} (resp., $2^{-38.9}$) (Table 5).

Table 5. Parameters proposed for OKCN-LWE with t least significant bits cut off.

	q	n	l	m	g	t	d	dist.	err.	bw. (kB)	$\|A\|$ (kB)	$\|K\|$	pq-sec
OKCN-T2	2^{14}	712	8	2^4	2^8	2	509	D_5	$2^{-39.0}$	18.58	887.15	256	134
OKCN-T1	2^{14}	712	8	2^4	2^8	1	509	D_5	$2^{-52.3}$	19.29	887.15	256	134

6.2 CCA-Secure AKCN-LWE, and Comparison with FrodoKEM

FrodoKEM [FrodoKEM] in submission to NIST PQC standardization is AKC-based and is a CCA-secure key encapsulation mechanism (KEM). The underlying AKC mechanism of FrodoKEM corresponds to the special case of AKCN for the parameters $\mathsf{params} = (q, m, g, d)$ where $g = q$ and $m = 4$ or $m = 8$. In addition, $\mathsf{FrodoKEM}$ chooses $t_2 = 0$, i.e., without compression of $\mathbf{Y}_2$. This means that, on the same parameters, AKCN-LWE outperforms FrodoKEM in bandwidth. We also note that the discrete distributions proposed by FrodoKEM, referred to as $\chi_{\mathsf{Frodo\text{-}640}}$ and $\chi_{\mathsf{Frodo\text{-}976}}$, are different from those of KC-based Frodo [BCD+16]. By replacing the underlying AKC mechanism of FrodoKEM with our AKCN, we get an AKCN-based CCA-secure KEM scheme. Two set of parameters for our AKCN-based CCA-secure KEM, referred to as AKCN-640 and AKCN-976 respectively, are briefly summaried in Table 6.

Table 6. Brief comparison between CCA-secure AKCN-LWE and FrodoKEM. The ciphertext size is the total length of bytes sent by Bob. For AKCN-640, its ciphertext is 7% smaller than Frodo-640. While its error probability is larger than Frodo-640, it's still under 2^{-130} that is sufficiently smaller for 103-bit pq-security. For AKCN-976, its ciphertext is 12.8% smaller than Frodo-976, and its error probability is still under 2^{-160} that is sufficiently smaller for 150-bit pq-security.

	n	q	m	g	t	dist	ciphertext	err.	$\|K\|$	C	Q
Frodo-640	640	2^{15}	2^2	2^{15}	0	$\chi_{\mathsf{Frodo\text{-}640}}$	9720	$2^{-148.8}$	128	144	103
AKCN-640	640	2^{15}	2^2	2^{10}	1	$\chi_{\mathsf{Frodo\text{-}640}}$	9040	$2^{-132.7}$	128	144	103
Frodo-976	976	2^{16}	2^3	2^{16}	0	$\chi_{\mathsf{Frodo\text{-}976}}$	15744	$2^{-199.6}$	192	209	150
AKCN-976	976	2^{16}	2^3	2^8	2	$\chi_{\mathsf{Frodo\text{-}976}}$	13728	$2^{-164.1}$	192	209	150

References

[APS15] Albrecht, M.R., Player, R., Scott, S.: On the concrete hardness of learning with errors. J. Math. Cryptol. **9**(3), 169–203 (2015)

[ADPS16] Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P.: Post-quantum key exchange — a new hope. USENIX Security, pp. 327–343 (2016)

[ACPS09] Applebaum, B., Cash, D., Peikert, C., Sahai, A.: Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 595–618. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-03356-8_35

[BLL+15] Bai, S., Langlois, A., Lepoint, T., Stehlé, D., Steinfeld, R.: Improved security proofs in lattice-based cryptography: using the Rényi divergence rather than the statistical distance. In: ASIACRYPT, pp. 3–24 (2015)

[BPR12] Banerjee, A., Peikert, C., Rosen, A.: Pseudorandom functions and lattices. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 719–737. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29011-4_42

[BGL+18] Bhattacharya, S., et al.: Round5: compact and fast post-quantum public-key encryption. Cryptology ePrint Archive, 2018/725

[BBG+17] Baan, H., et al.: Round2: KEM and PKE based on GLWR. Cryptology ePrint Archive, 2017/1183

[BGM+16] Bogdanov, A., Guo, S., Masny, D., Richelson, S., Rosen, A.: On the hardness of learning with rounding over small modulus. In: Kushilevitz, E., Malkin, T. (eds.) TCC 2016. LNCS, vol. 9562, pp. 209–224. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49096-9_9

[BCD+16] Bos, J., et al.: Frodo: take off the ring! Practical, quantum-secure key exchange from LWE. In: ACM CCS, pp. 1006–1018 (2016)

[CN11] Chen, Y., Nguyen, P.Q.: BKZ 2.0: better lattice security estimates. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 1–20. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-25385-0_1

[CGZ18] Cheng, L., Gong, B., Zhao, Y.: Lattice-based signature from key consensus. Cryptology ePrint Archive, Report 2018/1180

[CKLS16] Cheon, J.H., Kim, D., Lee, J., Song, Y.: Lizard: cut off the tail! practical post-quantum public-key encryption from LWE and LWR. Cryptology ePrint Archive, Report 2016/1126

[CW90] Coppersmith, D., Winograd, S.: Matrix multiplication via arithmetic progressions. J. Symb. Comput. **9**(3), 251–280 (1990)

[CDS94] Cramer, R., Damgård, I., Schoenmakers, B.: Proofs of partial knowledge and simplified design of witness hiding protocols. In: Desmedt, Y.G. (ed.) CRYPTO 1994. LNCS, vol. 839, pp. 174–187. Springer, Heidelberg (1994). https://doi.org/10.1007/3-540-48658-5_19

[DKRV17] D'Anvers, J., Karmakar, A., Roy, S.S., Vercauteren, F.: SABER: Mod-LWR based KEM. Proposal to NIST PQC Standardization

[DXL12] Ding, J., Xie, X., Lin, X.: A simple provably secure key exchange scheme based on the learning with errors problem. Cryptology ePrint Archive, Report 2012/688 (2012)

[DTV15] Duc, A., Tramèr, F., Vaudenay, S.: Better algorithms for LWE and LWR. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9056, pp. 173–202. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46800-5_8

[FS86] Fiat, A., Shamir, A.: How to prove yourself: practical solutions to identification and signature problems. In: Odlyzko, A.M. (ed.) CRYPTO 1986. LNCS, vol. 263, pp. 186–194. Springer, Heidelberg (1987). https://doi.org/10.1007/3-540-47721-7_12

[JZ16] Jin, Z., Zhao, Y.: Optimal key consensus in presence of noise. CoRR abs/1611.06150 (2016). https://arxiv.org/abs/1611.06150

[Kra03] Krawczyk, H.: SIGMA: the 'SIGn-and-MAc' approach to authenticated Diffie-Hellman and its use in the IKE protocols. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 400–425. Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-540-45146-4_24

[LP10] Lindner, R., Peikert, C.: Better key sizes (and attacks) for LWE-based encryption. In: Kiayias, A. (ed.) CT-RSA 2011. LNCS, vol. 6558, pp. 319–339. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19074-2_21

[LPR10] Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 1–23. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_1

[FrodoKEM] Naehrig, M., et al.: Supporting documentation: frodokem. Technical report, National Institute of Standards and Technology (2017). https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/Round-1-Submissions

[NIST] NIST: Post-Quantum Cryptography Standardization. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization

[Pei09] Peikert, C.: Public-Key Cryptosystems from the worst-case shortest vector problem. In: STOC, pp. 333–342 (2009)

[Pei14] Peikert, C.: Lattice cryptography for the internet. In: Mosca, M. (ed.) PQCrypto 2014. LNCS, vol. 8772, pp. 197–219. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-11659-4_12

[PG13] Pöppelmann, T., Güneysu, T.: Towards practical lattice-based public-key encryption on reconfigurable hardware. In: Lange, T., Lauter, K., Lisoněk, P. (eds.) SAC 2013. LNCS, vol. 8282, pp. 68–85. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-43414-7_4

[Reg09] Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. J. ACM **56**(6), 34–72 (2009)