Simulation-Secure Threshold PKE from Standard (Ring-)LWE

Hiroki Okada[1,2] and Tsuyoshi Takagi[2]

[1] KDDI Research, Inc., Japan
[2] The University of Tokyo, Japan

May 26, 2024

Abstract. Threshold public key encryption (ThPKE) is PKE that can be decrypted by collecting "partial decryptions" from t ($\leq N$) out of N parties. ThPKE based on the learning with errors problem (LWE) is particularly important because it can be extended to threshold fully homomorphic encryption (ThFHE). ThPKE and ThFHE are fundamental tools for constructing multiparty computation (MPC) protocols: In 2023, NIST initiated a project (NIST IR 8214C) to establish guidelines for implementing threshold cryptosystems. Because MPC often requires simulation-security (SS), ThPKE schemes that satisfy SS (SS-ThPKE) are also important. Recently, Micciancio and Suhl (ePrint 2023/1728) presented an efficient SS-ThPKE scheme based on LWE with a polynomial modulus. However, the scheme requires the use of a nonstandard problem called "known-norm LWE" for the security proof because the norm $\|\mathbf{e}\|$ of the error of the public key is leaked from the partial decryptions. This leads to the following two challenges: 1) The construction based on LWE relies on a nontight reduction from known-norm LWE to LWE. 2) No construction based on (standard) Ring-LWE has been presented. In this paper, we address both of these challenges: we propose an efficient SS-ThPKE scheme whose security is (directly) reduced from standard LWE/Ring-LWE with a polynomial modulus. The core technique of our construction is what we call "error sharing": We distribute shares of a small error $\boldsymbol{\zeta}$ via secret sharing, and use them to prevent leakage of $\|\mathbf{e}\|$ from partial decryptions.

1 Introduction

Threshold public key encryption (ThPKE) is public key encryption (PKE) whose ciphertexts can be decrypted by collecting "partial decryptions" from t out of N parties, where N is the total number of parties and $t(\leq N)$ is a threshold. One of the attractive applications of ThPKE is threshold fully homomorphic encryption (ThFHE), which can essentially be constructed by replacing the PKE of ThPKE with fully homomorphic encryption (FHE). ThPKE and ThFHE are fundamental tools for constructing multiparty computation (MPC) protocols: In 2023, the National Institute of Standards and Technology (NIST) initiated a project to establish guidelines and recommendations for implementing those

threshold cryptosystems [16]. ThFHE is a particularly important cryptographic tool that can be used to construct round optimal MPC protocols [5, 22, 24] and the universal thresholdizer [11], which can be used to add threshold functionality to many cryptosystems, such as CCA-secure PKE, signature schemes, pseudorandom functions (PRF) and functional encryptions.

The FHE was first realized by Gentry [27] based on ideal lattices. Constructions based on the learning with errors problem (LWE, Def. 3.6) [43] and Ring-LWE [31] (Def. 5.6) are efficient, leading to active research in this field [14, 18, 19]. Thus, ThPKE based on (Ring-)LWE is especially important because it can be extended to efficient ThFHE schemes. Moreover, ThPKE schemes with simulation-based security (SS) [17], which we call SS-ThPKE, are crucial because MPC is often formulated with SS.

However, existing SS-ThPKE schemes based on (Ring-)LWE, e.g., [4, 7, 11], are not efficient because they are based on (Ring-)LWE with a *superpolynomially* large modulus q; thus, the public key and the ciphertexts are superpolynomially long. Recently, Boudgoust and Scholl [12] and Chowdhury et al. [20] proposed ThPKE based on (Ring-)LWE with a polynomial modulus q, but their security proofs are game-based; thus, SS is not shown. Furthermore, the security proof of the schemes is not tight because it is based on the Rényi divergence technique [6, 42]. The technique basically incurs the loss of security bits, and moreover, it limits the adversary to accessing only a priori bounded numbers of queries of, e.g., partial decryptions. This also applies to the schemes of [12,20]. For example, [12] has a trade-off between the size of modulus q and security parameter (see Table 2,3 in [12]): if we want to suppress the security loss ($\simeq$ 3bits), q needs to be large (e.g., $q = 2^{23}$). Conversely, if we want to use small q (e.g., $q = 5 \cdot 3329$), a large security loss is incurred ($\simeq$ 111bits). Furthermore, [12] requires a query bound, i.e., the security is proven only for the (weak) adversary who can only query a priori bounded number of partial decryptions. Dahl et al. [21] also proposed an SS-ThPKE scheme based on (Ring-)LWE with a polynomial q; however, this scheme is not efficient because the modulus is switched to be superpolynomially large during decryption.

Micciancio and Suhl [37] recently proposed an efficient SS-ThPKE scheme based on LWE with a polynomial modulus q. However, the security proof of the scheme uses a nonstandard assumption called "known-norm LWE" (or "known-covariance Ring-LWE"), which is a problem to find the secret vector $\mathbf{s}$ from given LWE samples $(\mathbf{A}, \mathbf{b} := \mathbf{As} + \mathbf{e})$ and the norm $\|\mathbf{e}\|$ of the error $\mathbf{e}$, because partial decryptions of the scheme leak $\|\mathbf{e}\|$ to adversaries. As a consequence of relying on "known-norm LWE" (or "known-covariance Ring-LWE"), two challenges remain:

Question 1. *The SS-ThPKE scheme from LWE of [37] relies on a nontight reduction from LWE to "known-norm LWE". It incurs a security loss of approximately* 13 *bits in some typical parameters selected for* 128*-bit security. Can we construct SS-ThPKE based on LWE with a polynomial modulus q without this loss? (See the upper part of Fig. 1.)*

Fig. 1. Overview of the challenges (Questions 1 and 2) in ThPKE of [37] and our ThPKE schemes (Thms. 4.6 and 5.16).

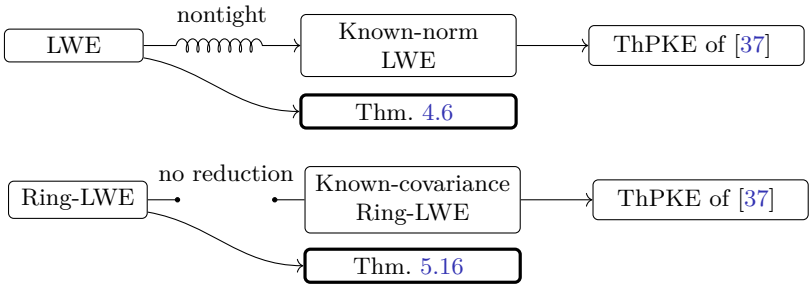

Table 1. Comparison of threshold PKE schemes from (Ring-)LWE

	$q = \text{poly}(\lambda)$	Simulation Security (SS)	Tightness	Ring-LWE
[7]	✗	✓	✓	✓
[11]	✗[1]	✓	✓	✓
[12]	✓	✗	✗	✓
[37]	✓	✓	✗	✗
Thm. 4.6	✓	✓	✓	-
Thm. 5.16	✓	✓	✓	✓

[1] [11, Constr. 5.6] (this is ThFHE, which subsumes ThPKE), requires a super-polynomial q to satisfy SS. [10, Constr. 8.29] is a generic construction of ThPKE from *universal thresholdizer*, which is constructed from ThFHE and NIZK.

Question 2. *The authors of [37] also proposed an SS-ThPKE scheme based on a nonstandard assumption called "known-covariance Ring-LWE", to which no reduction from standard assumptions such as Ring-LWE has been shown. Can we construct SS-ThPKE from standard Ring-LWE with a polynomial modulus q? (See the lower part of Fig. 1.)*

Question 1 results in an efficiency loss for the LWE-based scheme. Question 2 is crucial because most practical lattice-based PKE/FHE schemes (e.g., [14, 19, 30]) are constructed based on Ring-LWE.

Our Contributions. We address both Questions 1 and 2 above. We propose:

- Thm. 4.6: An SS-ThPKE scheme from LWE with a polynomial modulus q which does not use "known-norm LWE", and
- Thm. 5.16: An SS-ThPKE scheme from Ring-LWE with a polynomial modulus q (which does not rely on "known-covariance Ring-LWE").

In Fig. 1, we illustrate the relations among Questions 1 and 2 and our ThPKE schemes. We also briefly summarize the differences between the existing schemes and ours in Table 1.

In addition to the main contributions mentioned above, we provide the following supplementary contributions, which may be of independent interest:

- *Hardness of the Reused-A-LWE Problem for discrete Gaussians*: Micciancio and Suhl [37] introduced a variant of LWE called the *Reused-A-LWE problem* (Def. 3.11), where two LWE samples $(\mathbf{A}, \mathbf{b}_1 = \mathbf{A}\mathbf{s} + \mathbf{e}_1)$ and $(\mathbf{A}, \mathbf{b}_2 = \mathbf{A}\mathbf{s} + \mathbf{e}_2)$ of a common (i.e., "reused") $\mathbf{A}$ with different error distributions are given. While [37] showed a reduction from LWE to Reused-A-LWE, the error distribution was limited to a continuous Gaussian distribution. In this paper, we show a reduction from LWE to Reused-A-LWE for the discrete Gaussian distribution (Lem. 3.15). This result almost directly follows from a special case of the noise rerandomization lemma presented in [29, Lem. 1].
- *Discrete ThPKE Scheme*: In the ThPKE of [37], the ciphertext distribution is limited to be *continuous*. However, *discrete* distribution is desirable for implementation: If we "imitate" continuous distributions with floating-point numbers, we must discuss the (negative) effects of rounding errors. That is, we need to prove the security and correctness of the ThPKE scheme with the "rounded" distribution. In this paper, we construct a ThPKE scheme that can be instantiated solely with discrete distributions.
- *General Access Structure*: The ThPKE of [37] supports only (N, N)-threshold access structures (see Def. 2.29), where decryption is possible only when N out of N parties are involved. In contrast, our ThPKE supports all possible access structures achievable with binary coefficient linear secret sharing (BinLSS, see Def. 2.27), which include arbitrary (t, N)-access structures. This generalization is derived by simply adapting the techniques presented in [11].

Technical Overview. We explain how we modify the LWE-based ThPKE scheme proposed by Micciancio and Suhl [37]. Here, we do not explain our Ring-LWE-based ThPKE scheme since we can improve the "known-covariance Ring-LWE"-based ThPKE scheme of [37] with essentially the same modification.

The fundamental issue in the LWE-based ThPKE of [37] is that the adversary conducting chosen plaintext attack (CPA) can derive the norm $\|\mathbf{e}\|$ of the error in the public key, which is an LWE sample $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e})$. We address this issue in our scheme (Algo. 1) by what we call "error sharing" technique: we distribute the shares $(\mathsf{err}_1, \ldots, \mathsf{err}_N)$ of a short error $\mathsf{err} := \boldsymbol{\zeta}$ with secret sharing, in addition to the shares $(\mathsf{sk}_1, \ldots, \mathsf{sk}_N)$ of the secret key $\mathsf{sk} := \mathbf{s}$. This modification is made to secure the partial decryption process. The partial decryptions of our ThPKE ($\mathsf{PartDec}$: Line 8 in Algo. 1) include a randomized value derived from err_i in addition to the conventional "smudging noise" e_{sm}. Note that although the standard deviation of e_{sm} was superpolynomially large in conventional constructions such as [7, 11] (and that is why it is called "smudging"), polynomially small e_{sm} is sufficient in our scheme, as in [12, 37].

By this construction, the information exposed to adversaries is changed: while the scheme of [37] discloses the error norm $\|\mathbf{e}\|$, our scheme discloses $\sqrt{\|\mathbf{e}\|^2+\|\boldsymbol{\zeta}\|^2}$ (more generally, it discloses the distribution χ_{Sim} defined in (2)). Furthermore, we choose the short error $\boldsymbol{\zeta}$ conditioned on the fixed $\mathbf{e}$ generated by KeyGen so that $\sqrt{\|\mathbf{e}\|^2+\|\boldsymbol{\zeta}\|^2}=B$ holds, where B is a public constant that does not contain any information about $\|\mathbf{e}\|$. This technique can be described as applying "padding" to the value of $\|\mathbf{e}\|$, which varies depending on $\mathbf{e}$, to ensure that it reaches a constant value B. In addition, due to the (information-theoretic) security of secret sharing (Def. 2.26), no information about $\boldsymbol{\zeta}$ is revealed to adversaries who do not have a valid set of shares that enables decryption. Thus, our scheme does not leak any information about $\mathbf{e}$ to the adversary. Hence, the security of our scheme (Thm. 4.6) is "directly" reduced from (standard) LWE with $q=\mathrm{poly}(n)$ without using "known-norm LWE".

Related Works. Some readers may think we can use *multihint extended-LWE* (mheLWE) [2] to improve the reduction from LWE to known-norm LWE, but this is not known. Note that mheLWE is a multihint generalization of *extended-LWE* (extLWE) [3,15,40], and it is quite different from the multisecret generalization of extended-LWE, i.e., extLWE^t in [15]. $\mathsf{d\text{-}mheLWE}(n,m,q,\chi_{\mathsf{LWE}},\chi_{\mathsf{hint}})$ is a problem to distinguish between

$$(\mathbf{A},\mathbf{b},\{y_i,\mathbf{z}_i\}_{i\in[t]},\{y_i+\mathbf{z}_i^\intercal\mathbf{e}\}_{i\in[t]},)\text{ and }(\mathbf{A},\mathbf{u},\{y_i,\mathbf{z}_i\}_{i\in[t]},\{y_i+\mathbf{z}_i^\intercal\mathbf{e}\}_{i\in[t]}),$$

where $(\mathbf{A},\mathbf{b}:=\mathbf{A}\mathbf{s}+\mathbf{e})\leftarrow\mathsf{LWE}(n,m,q,\chi_{\mathsf{LWE}})$ (Def. 3.5), $(y_i,\mathbf{z}_i)\leftarrow\chi_{\mathsf{hint}}$, and χ_{hint} is an (efficiently samplable) distribution specified by the adversary. Note that the above mheLWE is more generalized than that of [3, 15] with the additional term y_i as in [40]. Although [2, Theorem 4] shows a reduction from $\mathsf{d\text{-}LWE}(n-t,m,q,\chi_{\mathsf{LWE}})$ to $\mathsf{d\text{-}mheLWE}(n,m,q,\chi_{\mathsf{LWE}},t,\chi_{\mathsf{hint}})$ which loses the advantage by at most $2^{\Omega(t-n)}$, it should be noted that the dimension of $\mathsf{d\text{-}LWE}$ is $n-t$. Thus, we require the number of hints $t<n$ to be a priori bounded. This condition on t is acceptable for applying mheLWE to some functional encryption schemes as demonstrated in [2]. In ThPKE of [37], the CPA adversary can obtain

$$(\mathbf{A},\mathbf{b}:=\mathbf{A}\mathbf{s}+\mathbf{e},\{e_i^{\mathsf{sm}}+\mathbf{r}_i^\intercal\mathbf{e}\}_{i\in[t]})\text{ for any (unbounded) }t=\mathrm{poly}(\lambda),\quad(1)$$

where $(\mathbf{A},\mathbf{b})\leftarrow\mathsf{LWE}(n,m,q,\chi_{\mathsf{LWE}})$, $e_i^{\mathsf{sm}}\leftarrow\mathcal{N}_{\sigma_{\mathsf{sm}}}$, and $\mathbf{r}_i\leftarrow\mathcal{N}_{\sigma_{\mathsf{enc}}}$. (Thus, the adversary can accurately estimate $\|\mathbf{e}\|$ because $e_i^{\mathsf{sm}}+\mathbf{r}_i^\intercal\mathbf{e}\sim\mathcal{N}_{\sqrt{\sigma_{\mathsf{sm}}^2+\sigma_{\mathsf{enc}}^2\|\mathbf{e}\|^2}}$.) We may simulate the distribution of (1) by $\mathsf{mheLWE}(n,m,q,\chi_{\mathsf{LWE}},t,\chi_{\mathsf{hint}})$:

$$(\mathbf{A},\mathbf{b}:=\mathbf{A}\mathbf{s}+\mathbf{e},\{y_i,\mathbf{z}_i\}_{i\in[t]},\{y_i+\mathbf{z}_i^\intercal\mathbf{e}\}_{i\in[t]}),$$

where $y_i\leftarrow\mathcal{N}_{\sigma_{\mathsf{sm}}}$ and $\mathbf{z}_i\leftarrow\mathcal{N}_{\sigma_{\mathsf{enc}}}$. However, to obtain a (nontrivial) reduction from LWE, we require t to be a priori bounded and less than n, which does not meet the standard definition of the CPA adversary.

Organization. The remainder of this paper is organized as follows: In Sect. 2, we provide necessary definitions and lemmas, and describe the construction

of linear secret sharing. In Sect. 3, we provide several lemmas related to the hardness of LWE, and then, we show a reduction from LWE to the Reused-A-LWE problem with discrete Gaussian errors. In Sect. 4 (and Sect. 5), we propose our LWE-based (and Ring-LWE-based) ThPKE scheme and prove its correctness and simulation-based security. Finally, we summarize this paper and discuss future works in Sect. 6.

2 Preliminaries

In Sect. 2.1, we provide notations used in this paper. Then, we provide necessary definitions and lemmas of the statistics, lattices, and the Gaussian distribution in Sect. 2.2, Sect. 2.3, and Sect. 2.4, respectively. Finally, we describe the construction of linear secret sharing in Sect. 2.5.

2.1 Notations

We denote the base 2 logarithm by log. For $N \in \mathbb{N}$, define $[N] := \{1, \ldots, N\}$. The number of elements in a set S is denoted by $|S|$. When the set $\{x_i\}_{i \in S}$ is given, the index set S is also given. We define $\mathbb{Z}_q := \mathbb{Z}/q\mathbb{Z}$ and $\mathbb{R}_q := \mathbb{R}/q\mathbb{R}$ for a modulus $q \in \mathbb{N}$.

We use bold lower-case for vectors and bold upper-case for matrices. For a vector $\mathbf{x} = (x_1, \ldots, x_n)$, we denote the ith component x_i by $\mathbf{x}[i]$. The transpose of $\mathbf{x}$ is written as $\mathbf{x}^\intercal$. We denote the l_2-norm and l_∞-norm of $\mathbf{x}$ by $\|\mathbf{x}\|$ and $\|\mathbf{x}\|_\infty$, respectively. The identity matrix is denoted by $\mathbf{I}_n \in \mathbb{Z}^{n \times n}$. We write $\mathbf{\Sigma} \succ 0$ if $\mathbf{\Sigma}$ is positive definite. We say that $\mathbf{\Sigma}_1 \succ \mathbf{\Sigma}_2$ if $\mathbf{\Sigma}_1 - \mathbf{\Sigma}_2 \succ 0$. A square root of $\mathbf{\Sigma} \succ 0$ is a nonsingular matrix $\mathbf{S}$ such that $\mathbf{S}\mathbf{S}^\intercal = \mathbf{\Sigma}$, which is written as $\mathbf{S} = \sqrt{\mathbf{\Sigma}}$. Note that $(\sqrt{\mathbf{\Sigma}})^{-1} = \mathbf{S}^{-1} = (\mathbf{S}^{-\intercal})^\intercal = (\sqrt{\mathbf{\Sigma}^{-1}})^\intercal$ holds. The largest and smallest singular values of a matrix $\mathbf{S}$ are denoted by $\sigma_{\max}(\mathbf{S})$ and $\sigma_{\min}(\mathbf{S})$, respectively. We denote by $\|\mathbf{S}\|$ the matrix norm of $\mathbf{S}$ induced by the l_2-norm. Note that we have $\sigma_{\max}(\mathbf{S}) = \|\mathbf{S}\|$, and if $\sigma_{\min}(\mathbf{S}) \neq 0$, i.e., $\mathbf{S}$ is nonsingular, $\sigma_{\min}(\mathbf{S}) = \|\mathbf{S}^{-1}\|$ holds. The Frobenius norm of $\mathbf{S}$ is $\|\mathbf{S}\|_F = \sqrt{\mathrm{tr}(\mathbf{S}^\intercal\mathbf{S})}$. Let $\|\mathbf{S}\|_{\mathrm{len}} = \max_{i \in [n]} \|\mathbf{s}_i\|$, where $\mathbf{s}_i$ is the i-th column vector of $\mathbf{S}$, then we have:

Fact 2.1. $\|\mathbf{S}\|_{\mathrm{len}} \leq \|\mathbf{S}\| \leq \|\mathbf{S}\|_F$, $\|\mathbf{S}_1\mathbf{S}_2\|_{\mathrm{len}} \leq \|\mathbf{S}_1\| \cdot \|\mathbf{S}_2\|_{\mathrm{len}} \leq \|\mathbf{S}_1\|\|\mathbf{S}_2\|$.

Unless otherwise specified, we treat λ or $n \in \mathbb{N}$ as a security parameter. We write $\mathrm{negl}(n) = n^{-\omega(1)}$ for the set of negligible functions and $\mathrm{poly}(n) = n^{O(1)}$ for the set of polynomial functions. We call $1 - \mathrm{negl}(n)$ overwhelming functions. The term "probabilistic polynomial time" is abbreviated as PPT. For problems P_1 and P_2, we denote the PPT reduction from P_1 to P_2 by $\mathsf{P}_1 \leq \mathsf{P}_2$.

2.2 Statistics

We write $X_1, X_2 \overset{\mathrm{iid}}{\sim} \chi$ when variables X_1 and X_2 are independent and identically distributed (i.i.d.) according to χ. We denote the uniform distribution over a set S by $\mathcal{U}(S)$, and denote the random variable X sampled from $\mathcal{U}(S)$ by $X \xleftarrow{\$} S$.

For any distributions χ_1 and χ_2, we denote by $\chi_1+\chi_2$ the distribution $\{X_1+X_2 \mid X_1 \leftarrow \chi_1$ and $X_2 \leftarrow \chi_2$ are mutually independent$\}$.

We provide the necessary definitions, lemmas, and facts as follows:

Definition 2.2. *The statistical distance between χ_1 and χ_2 is defined as $\Delta(\chi_1,\chi_2) := \frac{1}{2}\sum_{x\in\Omega}|f_{\chi_1}(x) - f_{\chi_2}(x)|$, where $f_{\chi_1}(x)$ and $f_{\chi_2}(x)$ are the probability functions of χ_1 and χ_2, respectively, and $\Omega := \mathrm{Supp}(\chi_1)\cup\mathrm{Supp}(\chi_2)$. This definition is naturally extended to continuous distributions.*

Definition 2.3 ($\approx_{\mathsf{s}}$). *The distributions χ_1 and χ_2 are* statistically indistinguishable *and are denoted as $\chi_1 \approx_{\mathsf{s}} \chi_2$ if we have $\Delta(\chi_1,\chi_2) = \mathrm{negl}(\lambda)$.*

Definition 2.4 ($\approx_{\mathsf{c}}$). *The distributions χ_1 and χ_2 over the set Ω are computationally indistinguishable and are denoted as $\chi_1 \approx_{\mathsf{c}} \chi_2$ if $|\Pr[\mathcal{A}(\chi_1) = 1] - \Pr[\mathcal{A}(\chi_2) = 1]| = \mathrm{negl}(\lambda)$ holds for any PPT algorithm $\mathcal{A} : \Omega \to \{0,1\}$.*

Definition 2.5. *The min-entropy of a discrete distribution χ is defined as $H_\infty(\chi) = \log \min_{x\in\mathrm{Supp}(\chi)}(1/\Pr_{X\leftarrow\chi}[X = x])$.*

Lemma 2.6 (Leftover hash lemma [13, Lemma 2.1]). *Let q be prime and $m,n \in \mathbb{N}$. Let $\mathbf{r}$ be a random variable over $\mathbb{Z}_q^m$ and $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{m\times n}$. Then, we have $\Delta((\mathbf{A},\mathbf{r}^\intercal\mathbf{A}),(\mathbf{A},\mathcal{U}(\mathbb{Z}_q^n))) \le \sqrt{q^n 2^{-H_\infty(\mathbf{r})}}$.*

Fact 2.7. *For $m \ge n\log q + 2\lambda$ and $\mathbf{r} \sim \mathcal{U}(\{0,1\}^m)$, $\sqrt{q^n 2^{-H_\infty(\mathbf{r})}} \le 2^{-\lambda}$ holds.*

Lemma 2.8 (used in [32, Lemma 4.8]). *For any $m \ge n + \omega(\log n)$, the rows of $\mathbf{A} \leftarrow \mathcal{U}(\mathbb{Z}_q^{m\times n})$ generate $\mathbb{Z}_q^n$ with overwhelming probability.*

Definition 2.9. *Let χ be a (continuous / discrete) distribution over $\mathbb{R}$. We say that χ is B-*bounded *if $\Pr_{X\leftarrow\chi}[|X| \ge B] = \mathrm{negl}(n)$ holds.*

2.3 Lattices

A lattice $\mathcal{L}$ is the set of all integer linear combinations of linearly independent vectors $\mathbf{b}_1,\cdots,\mathbf{b}_n \in \mathbb{R}^m$, i.e., $\mathcal{L} = \{\sum_{i=1}^n z_i\mathbf{b}_i \mid \mathbf{z} \in \mathbb{Z}^n\}$. If we arrange the vectors $\mathbf{b}_i$ as the columns of a matrix $\mathbf{B} \in \mathbb{R}^{m\times n}$, then we can write $\mathcal{L} := \mathcal{L}(\mathbf{B}) = \{\mathbf{Bz} \mid \mathbf{z} \in \mathbb{Z}^n\} = \mathbf{B}\mathbb{Z}^n$. The rank of this lattice is n and its dimension is m. If $n = m$, the lattice is called full rank. For arbitrary $\mathbf{c} \in \mathbb{R}^m$, a coset of lattice $\mathcal{L}$ is defined as $\mathcal{L} + \mathbf{c} := \{\mathbf{v} + \mathbf{c} \mid \mathbf{v} \in \mathcal{L}\}$. The dual of a lattice $\mathcal{L}$ is $\widehat{\mathcal{L}} := \{\mathbf{x} \mid \forall \mathbf{y} \in \mathcal{L}, \langle\mathbf{x},\mathbf{y}\rangle \in \mathbb{Z}\}$. We denote the volume of the fundamental parallelepiped of $\mathcal{L}$ as $\det(\mathcal{L})$. We have $\det(\widehat{\mathcal{L}}) = 1/\det(\mathcal{L})$. For a full-rank lattice $\mathcal{L}(\mathbf{B})$, we have $\det(\mathcal{L}(\mathbf{B})) = |\det(\mathbf{B})|$. For n-rank lattice $\mathcal{L}$ and $i = 1,\ldots,n$, the successive minimum $\lambda_i(\mathcal{L})$ is defined as the radius of the smallest ball that contains i linearly independent vectors in $\mathcal{L}$. The integer lattice $\mathcal{L} := \mathbb{Z}^n$ is the primary focus of this paper.

2.4 Gaussians

The continuous Gaussian distribution with a mean of 0 and a standard deviation $\sigma > 0$ is denoted as $\mathcal{N}_\sigma$.

For a rank-n matrix $\mathbf{S} \in \mathbb{R}^{n\times m}$, the (centered) ellipsoid Gaussian function on $\mathbb{R}^n$ with the (scaled) covariance matrix $\mathbf{\Sigma} = \mathbf{S}\mathbf{S}^\intercal \in \mathbb{R}^{n\times n}$ is defined as: $\rho_{\mathbf{S}}(\mathbf{x}) := \exp(-\pi\mathbf{x}^\intercal(\mathbf{S}\mathbf{S}^\intercal)^{-1}\mathbf{x})$. Since the function $\rho_{\mathbf{S}}(\mathbf{x})$ is determined exactly by $\mathbf{\Sigma}$, we have $\rho_{\mathbf{S}} = \rho_{\sqrt{\mathbf{\Sigma}}}$. When $\mathbf{S} = s\mathbf{I}_n$, we write $\rho_{\mathbf{S}}$ as ρ_s. For any set $A \subseteq \mathbb{R}^n$, we define $\rho_{\mathbf{S}}(A) := \sum_{\mathbf{x}\in A}\rho_{\mathbf{S}}(\mathbf{x})$.

We define the discrete Gaussian distribution over the lattice $\mathcal{L}$ as follows:

Definition 2.10 (Discrete Gaussian). *For a full column-rank matrix $\mathbf{S}$, the (centered) discrete Gaussian distribution over a lattice $\mathcal{L}$ is defined as $\forall\mathbf{x} \in \mathcal{L}, D_{\mathcal{L},\mathbf{S}}(\mathbf{x}) = \rho_{\mathbf{S}}(\mathbf{x})/\rho_{\mathbf{S}}(\mathcal{L})$. In particular, when $\mathbf{S}\mathbf{S}^\intercal = s^2\mathbf{I}_n$ for some $s > 0$, we write $D_{\mathcal{L},\mathbf{S}}$ as $D_{\mathcal{L},s}$ and call it as the spherical discrete Gaussian distribution.*

Note that the n-dimensional vector whose elements are i.i.d 1-dimensional discrete Gaussian $D_{\mathbb{Z},s}$ follows $D_{\mathbb{Z}^n,s}$:

Fact 2.11. *Let $x_1,\ldots,x_n \overset{\text{iid}}{\sim} D_{\mathbb{Z},s}$ and $\mathbf{x} := (x_1,\ldots,x_n)^\intercal$; then $\mathbf{x} \sim D_{\mathbb{Z}^n,s}$.*

Proof. The joint distribution function of $\mathbf{x}$ is $\prod_{i=1}^n(\rho_s(x_i)/\sum_{y_i\in\mathbb{Z}}\rho_s(y_i)) = \rho_s(\mathbf{x})/\sum_{\mathbf{y}\in\mathbb{Z}^n}\rho_s(\mathbf{y}) = D_{\mathbb{Z}^n,s}(\mathbf{x})$. □

The *smoothing parameter* of $\mathcal{L}$ is defined as $\eta_\epsilon(\mathcal{L}) = \min\{s \mid \rho_{1/s}(\widehat{\mathcal{L}}) \le 1+\epsilon\}$ for $\epsilon > 0$. Unless otherwise specified, we set $\epsilon = \mathrm{negl}(\lambda)$. An upper-bound of $\eta_\epsilon(\mathcal{L})$ is obtained by successive minimum[3] $\lambda_n(\mathcal{L})$:

Lemma 2.12 ([36, Lemma 3.3]). *Define $\eta^+_\epsilon(\mathbb{Z}^n) := \sqrt{\ln(2n(1+1/\epsilon))/\pi}$. For any rank-$n$ lattice $\mathcal{L}$ and any $\epsilon > 0$, we have $\eta_\epsilon(\mathcal{L}) \le \lambda_n(\mathcal{L})\cdot\eta^+_\epsilon(\mathbb{Z}^n)$. In particular, $\eta_\epsilon(\mathbb{Z}^n) \le \eta^+_\epsilon(\mathbb{Z}^n)$ holds.*

For simplicity of notation, we also define $\tilde{\eta}_\epsilon(\cdot) := \sqrt{2}\eta_\epsilon(\cdot)$ and $\tilde{\eta}^+_\epsilon(\mathbb{Z}^n) := \sqrt{2}\eta^+_\epsilon(\mathbb{Z}^n)$. Note that we have $\tilde{\eta}^+_\epsilon(\mathbb{Z}) > \eta^+_\epsilon(\mathbb{Z}^2)$. The smoothing parameter is extend to matrices:

Definition 2.13 ([41, Definition 2.3]). *Let $\mathbf{\Sigma} \succ 0$ be any positive definite matrix. For any lattice $\mathcal{L}$, we say that $\sqrt{\mathbf{\Sigma}} \ge \eta_\epsilon(\mathcal{L})$ if $\eta_\epsilon(\sqrt{\mathbf{\Sigma}}^{-1}\mathcal{L}) \le 1$.*

For a full-rank lattice, we obtain a sufficient condition as follows:

Fact 2.14. *For any full-rank lattice $\mathcal{L}(\mathbf{B})$ and $\mathbf{\Sigma} \succ 0$, $\sqrt{\mathbf{\Sigma}} \ge \eta_\epsilon(\mathcal{L})$ holds if $1 \ge \|\sqrt{\mathbf{\Sigma}}^{-1}\|\|\mathbf{B}\|_{\mathrm{len}}\eta^+_\epsilon(\mathbb{Z}^n)$.*

Proof. By Fact 2.1, Lem. 2.12 and the hypothesis, we have $\eta_\epsilon(\sqrt{\mathbf{\Sigma}}^{-1}\mathcal{L}) \le \lambda_n(\sqrt{\mathbf{\Sigma}}^{-1}\mathcal{L})\eta^+_\epsilon(\mathbb{Z}^n) \le \|\sqrt{\mathbf{\Sigma}}^{-1}\mathbf{B}\|_{\mathrm{len}}\eta^+_\epsilon(\mathbb{Z}^n) \le \|\sqrt{\mathbf{\Sigma}}^{-1}\|\|\mathbf{B}\|_{\mathrm{len}}\eta^+_\epsilon(\mathbb{Z}^n) \le 1$. □

The linear sum of discrete Gaussians is close to a discrete Gaussian:

Lemma 2.15 (Special case of [34, Theorem 3.3]). *Let $\mathbf{c} \in \mathbb{Z}^m$ be a nonzero vector such that $\gcd(\mathbf{c}) = 1$. For $i = 1,\ldots,m$, let $s_i \ge \|\mathbf{c}\|_\infty\tilde{\eta}^+_\epsilon(\mathbb{Z})$ and $r_i \sim D_{\mathbb{Z},s_i}$ (mutually independent), and define $\mathbf{r} := (r_1,\ldots,r_m)^\intercal$. Then, we have $\mathbf{c}^\intercal\mathbf{r} \approx_{\mathbf{s}} D_{\mathbb{Z},\tilde{s}}$, where $\tilde{s} = \sqrt{\sum_{i=1}^m(c_is_i)^2}$.*

[3] Although [28, Lemma 3.1] provides a sharper bound with the *Gram–Schmidt minimum*, we rely on Lem. 2.12 for ease of analysis.

The linear transformation of a discrete Gaussian is as follows:

Lemma 2.16 (Special case of [26, Lemma 1]). *For any nonsingular matrices* $\mathbf{S}, \mathbf{T} \in \mathbb{Z}^{n\times n}$*, we have* $\mathbf{T} \cdot D_{\mathbb{Z}^n,\mathbf{S}} = D_{\mathbf{T}\cdot\mathbb{Z}^n,\mathbf{TS}}$.

The sum of two discrete Gaussians over different integer lattices is statistically close to a discrete Gaussian over the union.

Lemma 2.17 (Special case of [8, Lemma 4.12]). *Let* $\mathcal{L}_1, \mathcal{L}_2 \subseteq \mathbb{Z}^n$ *be full rank integer lattices and let* $s_1, s_2 > 0$ *be such that* $(s_1^{-2}+s_2^{-2})^{-1/2} \geq \eta_\epsilon(\mathcal{L}_1 \cap \mathcal{L}_2)$*. Then,* $D_{\mathcal{L}_1,s_1} + D_{\mathcal{L}_2,s_2} \approx_{\mathsf{s}} D_{\mathcal{L}_1+\mathcal{L}_2,\sqrt{s_1^2+s_2^2}}$.

In particular, for the integer lattice $\mathcal{L}_2 := \mathbb{Z}^n$ and its (integer) linear transformation $\mathcal{L}_1 := \mathbf{T} \cdot \mathbb{Z}^n \subseteq \mathbb{Z}^n$, we obtain the following corollary:

Corollary 2.18. *Let* $\mathbf{T} \in \mathbb{Z}^{n\times n}$ *be a nonsingular integer matrix. Let* $s_1, s_2 > 0$ *be such that* $(s_1^{-2} + s_2^{-2})^{-1/2} \geq \|\mathbf{T}\|_{\mathrm{len}}\eta_\epsilon^+(\mathbb{Z}^n)$*. Then,* $D_{\mathbf{T}\mathbb{Z}^n,s_1} + D_{\mathbb{Z}^n,s_2} \approx_{\mathsf{s}} D_{\mathbb{Z}^n,\sqrt{s_1^2+s_2^2}}$.

Proof. We have $\mathbf{T}\mathbb{Z}^n \subseteq \mathbb{Z}^n$ since $\mathbf{T}$ is an integer matrix. By Lem. 2.12, $\eta_\epsilon(\mathbf{T}\mathbb{Z}^n) \leq \|\mathbf{T}\|_{\mathrm{len}}\eta_\epsilon^+(\mathbb{Z}^n)$ holds. Thus, we obtain the corollary by Lem. 2.17. □

More generally, the sum of two ellipsoid discrete Gaussians is statistically close to an ellipsoid discrete Gaussian:

Lemma 2.19 (Special case of [41, Thm. 3.1]). *Let* $\mathbf{\Sigma}_1, \mathbf{\Sigma}_2 \succ 0$ *be positive definite matrices and define* $\mathbf{\Sigma}_3 := (\mathbf{\Sigma}_1^{-1} + \mathbf{\Sigma}_2^{-1})^{-1}$*. Let* $\mathcal{L}_1$*,* $\mathcal{L}_2$ *be full-rank lattices such that* $\sqrt{\mathbf{\Sigma}_2} \geq \eta_\epsilon(\mathcal{L}_2)$ *and* $\sqrt{\mathbf{\Sigma}_3} \geq \eta_\epsilon(\mathcal{L}_1)$*, and let* $X := \{(\mathbf{x}_1, \mathbf{x}_2) \mid \mathbf{x}_1 \leftarrow D_{\mathcal{L}_1,\sqrt{\mathbf{\Sigma}_1}}, \mathbf{x}_2 \leftarrow \mathbf{x}_1 + D_{\mathcal{L}_2-\mathbf{x}_1,\sqrt{\mathbf{\Sigma}_2}}\}$*. The marginal distribution of* $\mathbf{x}_2$ *in* X *is statistically close to* $D_{\mathcal{L}_2,\sqrt{\mathbf{\Sigma}_1+\mathbf{\Sigma}_2}}$.

In particular, when $\mathcal{L}_1 \subseteq \mathcal{L}_2$, we can simplify Lem. 2.19 because the coset $\mathcal{L}_2 - \mathbf{x}_1$ is equal to $\mathcal{L}_2$ itself for any $\mathbf{x}_1 \in \mathcal{L}_1$:

Corollary 2.20. *Let* $\mathbf{\Sigma}_1, \mathbf{\Sigma}_2 \succ 0$ *be positive definite matrices and define* $\mathbf{\Sigma}_3 := (\mathbf{\Sigma}_1^{-1}+\mathbf{\Sigma}_2^{-1})^{-1}$*. Let* $\mathcal{L}_1$*,* $\mathcal{L}_2$ *be full-rank lattices such that* $\mathcal{L}_1 \subseteq \mathcal{L}_2$*,* $\sqrt{\mathbf{\Sigma}_2} \geq \eta_\epsilon(\mathcal{L}_2)$ *and* $\sqrt{\mathbf{\Sigma}_3} \geq \eta_\epsilon(\mathcal{L}_1)$*. Then, we have* $D_{\mathcal{L}_1,\sqrt{\mathbf{\Sigma}_1}} + D_{\mathcal{L}_2,\sqrt{\mathbf{\Sigma}_2}} \approx_{\mathsf{s}} D_{\mathcal{L}_2,\sqrt{\mathbf{\Sigma}_1+\mathbf{\Sigma}_2}}$.

The tail bound of $D_{\mathcal{L},\mathbf{S}}$, $D_{\mathcal{L},s}$ and $D_{\mathbb{Z},s}$ can be obtained as follows:

Lemma 2.21 ([1, Lemma 3]). *For any* n*-rank lattice* $\mathcal{L}$*,* $\epsilon \in (0,1)$ *and matrix* $\mathbf{S}$ *s.t.* $\sigma_{\min}(\mathbf{S}) \geq \eta_\epsilon(\mathcal{L})$*, we have* $\Pr_{\mathbf{x}\leftarrow D_{\mathcal{L},\mathbf{S}}}[\|\mathbf{x}\| > \sigma_{\max}(\mathbf{S})\sqrt{n}] \leq \frac{1+\epsilon}{1-\epsilon} \cdot 2^{-n}$.

Lemma 2.22 ([36, Lem. 4.4]). *For any* n*-rank lattice* $\mathcal{L}$*,* $\epsilon \in (0,1)$ *and* $s \geq \eta_\epsilon(\mathcal{L})$*, we have* $\Pr_{\mathbf{x}\leftarrow D_{\mathcal{L},s}}[\|\mathbf{x}\| > s\sqrt{n}] \leq \frac{1+\epsilon}{1-\epsilon} \cdot 2^{-n}$.

Lemma 2.23. *For any* $\epsilon \in (0,1)$*,* $s \geq \eta_\epsilon^+(\mathbb{Z})$ *and* $t \in \mathbb{N}$*, we have* $\Pr_{x\leftarrow D_{\mathbb{Z},s}}[|x| \geq t] \leq \frac{s}{(1-\epsilon)\pi t}e^{-\pi t^2/s^2}$*. In particular, for any* $t = s\cdot\Omega(\sqrt{\lambda})$*, we have* $\Pr_{x\leftarrow D_{\mathbb{Z},s}}[|x| \geq t] = \mathrm{negl}(\lambda)$*, i.e.,* $D_{\mathbb{Z},s}$ *is* $s\cdot\Omega(\sqrt{\lambda})$*-bounded (Def. 2.9).*

2.5 Linear Secret Sharing (LSS)

In this subsection, we describe the construction of linear secret sharing based on [11], which we use in our proposed scheme. Unless otherwise specified, we let

$P = \{P_1, \ldots, P_N\}$ be a set of parties. The power set of a set S is $\mathbb{P}(S) = \{A \mid A \subseteq S\}$.

Definition 2.24 (Monotone access structure). *A collection $\mathbb{A} \subseteq \mathbb{P}(P)$ is monotone if $B \in \mathbb{A}$ implies $C \in \mathbb{A}$ for any $B \subseteq C (\subseteq P)$. A monotone access structure on P is a monotone collection $\mathbb{A} \subseteq \mathbb{P}(P) \backslash \varnothing$.*

Definition 2.25 (Valid party set). *Let $\mathbb{A}$ be a monotone access structure on P. The sets $S \in \mathbb{A}$ are called the valid sets and the sets $S \in \mathbb{P}(P) \backslash \mathbb{A}$ are called the invalid sets. Furthermore, we define the maximal invalid party set as $\{S \notin \mathbb{A} \mid \forall P_i \in P \backslash S, S \cup \{P_i\} \in \mathbb{A}\}$, and the minimal valid party set as $\{S \in \mathbb{A} \mid \forall S' \subsetneq S, S' \notin \mathbb{A}\}$.*

We define the syntax of secret sharing and the necessary conditions:

Definition 2.26 (Secret sharing (SS)). *A secret sharing scheme SS for a secret space $\mathcal{K}$ and an access structure $\mathbb{A}$ is a tuple of PPT algorithms $\mathsf{SS} = (\mathsf{SS.Share}, \mathsf{SS.Combine})$ defined as follows:*

- $\mathsf{SS.Share}(\mathsf{k} \in \mathcal{K}, \mathbb{A}) \to (\mathsf{s}_1, \ldots, \mathsf{s}_N)$*: On the input of a secret $\mathsf{k} \in \mathcal{K}$ and an access structure $\mathbb{A}$, a set of shares $\mathsf{s}_1, \ldots, \mathsf{s}_N$ is returned for each $P_1, \ldots, P_N$.*
- $\mathsf{SS.Combine}(\{\mathsf{s}_i\}_{i \in S}) \to \mathsf{k}$*: On the input of a set of shares $\{\mathsf{s}_i\}_{i \in S}$, the combining algorithm outputs a secret $\mathsf{k} \in \mathcal{K}$.*

Furthermore, SS schemes must satisfy correctness and privacy: Correctness: For all $S \in \mathbb{A}$, $\mathsf{k} \in \mathcal{K}$, $(\mathsf{s}_1, \ldots, \mathsf{s}_N) \leftarrow \mathsf{SS.Share}(\mathsf{k}, \mathbb{A})$, $\mathsf{SS.Combine}(\{\mathsf{s}_i\}_{i \in S}) = \mathsf{k}$ holds. Privacy: For all $S \notin \mathbb{A}$, and $\mathsf{k}_0, \mathsf{k}_1 \in \mathcal{K}$, $(\mathsf{s}_{b,1}, \ldots, \mathsf{s}_{b,N}) \leftarrow \mathsf{SS.Share}(\mathsf{k}_b, \mathbb{A})$ for $b \in \{0, 1\}$, the following distributions are identical: $\{\mathsf{s}_{0,i}\}_{i \in S} \approx \{\mathsf{s}_{1,i}\}_{i \in S}$.

We describe the construction of linear secret sharing in [11], which we use in our ThPKE schemes, as follows:

Definition 2.27 (BinLSS). *Let $\mathbb{S}$ be a class of efficient access structures on P. A secret sharing scheme BinLSS with secret space $\mathcal{K} = \mathbb{Z}_p$ for some prime p is called a binary coefficient linear secret sharing scheme[4] if the following properties are satisfied:*

- $\mathsf{BinLSS.Share}(\mathsf{k} \in \mathbb{Z}_p, \mathbb{A} \in \mathbb{S}) \to (\mathsf{s}_1, \ldots \mathsf{s}_N)$*: There exists a matrix $\mathbf{M} \in \mathbb{Z}_p^{l \times N}$ called the share matrix, and each party P_i is associated with a partition $T_i \subseteq [l]$. To create the shares on a secret k, the sharing algorithm first samples $r_2, \ldots, r_N \xleftarrow{\$} \mathbb{Z}_p$, and calculates $\mathbf{w} := (w_1, \ldots, w_l)^\intercal$ defined as $\mathbf{w} = \mathbf{M} \cdot (\mathsf{k}, r_2, \ldots, r_N)^\intercal$. Then, $\mathsf{s}_i := \{w_j\}_{j \in T_i}$ is output as the share for P_i.*
- $\mathsf{BinLSS.Combine}(\{\mathsf{s}_i\}_{i \in S})$*: Any valid set of parties $S \in \mathbb{A}$ can efficiently find the binary coefficients $\{c_j \in \{0, 1\}\}_{j \in \bigcup_{i \in S} T_i}$ satisfying $\sum_{j \in \bigcup_{i \in S} T_i} c_j \cdot \mathbf{M}[j] = (1, 0, \ldots, 0)$. Thus, the secret is recovered by computing $\mathsf{k} = \sum_{j \in \bigcup_{i \in S} T_i} c_j w_j$.*

We define an analogue of Def. 2.25 for the set of shares as follows:

[4] While [11] defines $\{0, 1\}$-LSSS as the class of access structure, we define BinLSS as $\{0, 1\}$-linear secret sharing scheme itself.

Definition 2.28 (Valid share set). *Let $\mathbb{S}$ be a class of efficient access structures on P, and let* SS *be a* BinLSS *for $\mathbb{S}$ with share matrix $\mathbf{M} \in \mathbb{Z}_q^{l \times N}$. For a set of indices $T \subseteq [l]$, we say that T is a valid share set if there exist binary coefficients $\{c_j \in \{0,1\}\}_{j \in T}$ satisfying $\sum_{j \in T} c_j \cdot \mathbf{M}[j] = (1, 0, \ldots, 0)$. Otherwise, T is an invalid share set. We also define the maximal invalid share set as $\{\text{invalid } T \subseteq [l] \mid \forall i \in [l] \backslash T, (T \cup i) \text{ is valid}\}$, and define the minimal valid share set as $\{\text{valid } T \subseteq [l] \mid \forall T' \subsetneq T, T \text{ is invalid}\}$.*

The access structure used in threshold cryptosystems is defined as follows:

Definition 2.29 (Threshold access structures). *An access structure $\mathbb{A}_{(t,N)}$ is called a (t, N)-threshold access structure if for every set of parties $S \subseteq P$, we have $S \in \mathbb{A}_{(t,N)}$ if $|S| \geq t$.*

The following Thm. 2.30 proves that BinLSS (Def. 2.27) corresponds to any threshold access structure. Therefore, constructing PKE with a decryption access structure following BinLSS is sufficient for constructing ThPKE.

Theorem 2.30 ([11, Theorem 4.15]). *There exists an efficient* BinLSS *for any (t, N)-threshold access structure.*

Secret Sharing Vectors. Although we described only how to share a single scalar in $\mathbb{Z}_p$, we can also share a vector $\mathbf{s} \in \mathbb{Z}_p^n$ by sharing each entry of the vector using independent randomness. It is easy to see that correctness and privacy hold even when we share a vector.

3 Hardness of Reused-A-LWE for Discrete Gaussian

Micciancio and Suhl [37] introduced *the Reused-A-LWE problem* (Def. 3.11), but the error distribution used in the problem is restricted to the *continuous* Gaussian distribution. The main goal of this section is to show Lem. 3.15, which is a reduction from LWE to Reused-A-LWE with the discrete Gaussian distribution. This reduction is used in Sect. 4 to prove the security of our ThPKE scheme from LWE with discrete Gaussian errors.

We first define a quasi-order between probability distributions, which is useful to describe the self-reduction of LWE (and the variants), in Sect. 3.1. Then, in Sect. 3.2, we define the LWE problem [43] and present Lems. 3.9 and 3.10 by using the quasi-order. The lemmas are also used to prove the security of our ThPKE scheme in Sect. 4. Finally, we define the Reused-A-LWE problem and show Lem. 3.15 in Sect. 3.3.

3.1 Quasi-Order between Distributions

The purpose of this subsection is to provide Def. 3.1, which is used to prove Lems. 3.9 and 3.10 in Sect. 3.2. We define a binary relation $\leq$ on probability distributions and show that it is a quasi-order:

Definition 3.1 (Quasi-order between distributions). *Let $n \in \mathbb{N}$. For (continuous or discrete) distributions χ_1 and χ_2 over $\mathbb{R}^n$, if there exists a distribution χ_δ such that $(\chi_1 + \chi_\delta) \approx_{\mathsf{s}} \chi_2$, we write $\chi_1 \leq \chi_2$.*

Fact 3.2. *The relation $\leq$ defined in Def. 3.1 is quasi-order but not partial order.*

Proof. We show that $\leq$ defined in Def. 3.1 is reflexive and transitive but is not antisymmetric, as follows:

Reflexive: Let χ_δ be a distribution such that $\Pr_{X \leftarrow \chi_\delta}[X = \mathbf{0}] = 1$, then, for any χ, $\chi \leq \chi + \chi_\delta = \chi$ holds.

Transitive: Let χ_1, χ_2, and χ_3 be distributions such that $\chi_1 \leq \chi_2$ and $\chi_2 \leq \chi_3$ hold; then, there exist χ_{δ_1} and χ_{δ_2} such that $\chi_1 + \chi_{\delta_1} \approx_{\mathsf{s}} \chi_2$ and $\chi_2 + \chi_{\delta_2} \approx_{\mathsf{s}} \chi_3$ hold. Thus, $\chi_1 \leq \chi_3$ holds because $\chi_1 + \chi_{\delta_1} + \chi_{\delta_2} \approx_{\mathsf{s}} \chi_2 + \chi_{\delta_2} \approx_{\mathsf{s}} \chi_3$.

Not Antisymmetric: We show that there exist some $\chi_1 \neq \chi_2$ such that $\chi_1 \leq \chi_2$ and $\chi_2 \leq \chi_1$ hold. Let χ_δ and χ'_δ be distributions such that $\chi_\delta \neq \chi'_\delta$ and $\Pr_{X \leftarrow \chi_\delta}[X = \mathbf{0}] = 1 - \mathrm{negl}(\lambda)$, $\Pr_{X \leftarrow \chi'_\delta}[X = \mathbf{0}] = 1 - \mathrm{negl}(\lambda)$. Let χ_1 be an arbitrary distribution and define $\chi_2 := \chi_1 + \chi_\delta$, then $\chi_2 \neq \chi_1$ and $\chi_1 \leq \chi_2$ hold. We also have $\chi_2 \leq \chi_1$ because $\chi_2 + \chi'_\delta = \chi_1 + \chi_\delta + \chi'_\delta \approx_{\mathsf{s}} \chi_1$. □

As a typical example, the quasi-order between (continuous / discrete) Gaussians is determined by the order of the parameter σ or s in $\mathbb{R}$.

Fact 3.3. *For any $0 < \sigma_1 < \sigma_2$, we have $\mathcal{N}_{\sigma_1} \leq \mathcal{N}_{\sigma_2}$.*

Fact 3.4. *Let $\epsilon = \mathrm{negl}(\lambda)$. For any $\tilde{\eta}^+_\epsilon(\mathbb{Z}) < s_1 < s_2$ such that $\tilde{\eta}^+_\epsilon(\mathbb{Z}) < s_\delta := \sqrt{s_2^2 - s_1^2}$, we have $D_{\mathbb{Z},s_1} \leq D_{\mathbb{Z},s_2}$.*

Proof. $D_{\mathbb{Z},s_1} + D_{\mathbb{Z},s_\delta} \approx_{\mathsf{s}} D_{\mathbb{Z},s_2}$ holds by Lem. 2.15. □

3.2 Learning with Errors (LWE)

The goal of this subsection is to present Lems. 3.9 and 3.10, by utilizing the quasi-order defined in Def. 3.1. These lemmas can be applied to any (continuous or discrete) error distributions, which may be of independent interest. First, we define the LWE distribution and the LWE problem.

Definition 3.5 (LWE distribution). *Let $n \in \mathbb{N}$ be a security parameter and $m = \mathrm{poly}(n)$ and the modulus $q = q(n) \geq 2$ be integers. Let $\mathbb{X}_q$ be $\mathbb{Z}_q$ or $\mathbb{R}_q$, and let χ be an error distribution over $\mathbb{X}_q$. The LWE distribution for a fixed secret vector $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$ is defined as $\mathsf{LWE}_{\mathbf{s}}(n, m, q, \chi) := \left\{ (\mathbf{A}, \mathbf{As} + \mathbf{e}) \mid \mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{m \times n}, \mathbf{e} \leftarrow \chi^m \right\}$.*

Definition 3.6 (Decision-LWE). *$\mathsf{d\text{-}LWE}_{\mathbf{s}}(n, m, q, \chi)$ is the problem to distinguish $\mathsf{LWE}_{\mathbf{s}}(n, m, q, \chi)$ from the uniform distribution $\mathcal{U}(\mathbb{Z}_q^{m \times n} \times \mathbb{X}_q^m)$. The* advantage *of an algorithm $\mathcal{A} : \mathbb{Z}_q^{m \times n} \times \mathbb{X}_q^m \to \{0, 1\}$ for solving $\mathsf{d\text{-}LWE}$ is defined as $\mathrm{Adv}^{\mathsf{d\text{-}LWE}}_{\mathcal{A}} = |\Pr[\mathcal{A}(\mathsf{LWE}_{\mathbf{s}}(n, m, q, \chi)) = 1] - \Pr[\mathcal{A}(\mathcal{U}(\mathbb{Z}_q^{m \times n} \times \mathbb{X}_q^n)) = 1]|$. We say that $\mathsf{d\text{-}LWE}$ is hard if $\mathrm{Adv}^{\mathsf{d\text{-}LWE}}_{\mathcal{A}} = \mathrm{negl}(n)$ for any PPT algorithm $\mathcal{A}$ (i.e., $\mathsf{LWE}_{\mathbf{s}}(n, m, q, \chi)$ is pseudorandom).*

Definition 3.7 (Search-LWE). $\mathsf{s\text{-}LWE}_{\mathbf{s}}(n, m, q, \chi)$ *is the problem to find the vector* $\mathbf{s}$ *from a sample* $(\mathbf{A}, \mathbf{b}) \leftarrow \mathsf{LWE}_{\mathbf{s}}(n, m, q, \chi)$. *We say that* $\mathsf{s\text{-}LWE}$ *is* hard *if any PPT algorithm can solve it with only* $\mathrm{negl}(n)$ *probability.*

It is shown in [43] that $\mathsf{s\text{-}LWE}$ and $\mathsf{d\text{-}LWE}$ are hard if the error distribution χ is a continuous or discretized Gaussian distribution under the hardness assumption of worst-case lattice problems (e.g., the approximate shortest vector problem (GapSVP)). The hardness of $\mathsf{s\text{-}LWE}$/$\mathsf{d\text{-}LWE}$ with discrete Gaussian (Def. 2.10) is also shown by the LWE self-reduction presented in [26, 41].

The reduction from $\mathsf{d\text{-}LWE}$ to $\mathsf{s\text{-}LWE}$ is trivial. We provide the proof for completeness.

Fact 3.8 ($\mathsf{d\text{-}LWE} \leq \mathsf{s\text{-}LWE}$). *If there exists a PPT algorithm* $\mathcal{A}$ *that solves* $\mathsf{s\text{-}LWE}_{\mathbf{s}}(n, m, q, \chi)$, *there exists a PPT algorithm that solves* $\mathsf{d\text{-}LWE}_{\mathbf{s}}(n, m, q, \chi)$.

Proof. Let $(\mathbf{A}, \mathbf{b})$ be a sample drawn from $\mathsf{LWE}_{\mathbf{s}}(n, m, q, \chi)$ or $\mathcal{U}(\mathbb{Z}_q^{m \times n} \times \mathbb{X}_q^m)$. Using $\mathcal{A}$, construct $\mathcal{A}'(\mathbf{A}, \mathbf{b})$ as follows: compute $\overline{\mathbf{s}} \leftarrow \mathcal{A}(\mathbf{A}, \mathbf{b})$ and determine whether the distribution of $\mathbf{b} - \mathbf{A}\overline{\mathbf{s}}$ is χ^m or $\mathcal{U}(\mathbb{X}_q^m)$ via statistical tests. □

The reverse reduction, i.e., $\mathsf{s\text{-}LWE} \leq \mathsf{d\text{-}LWE}$ is shown in [32,43]. The following lemma shows that, if LWE is hard, the probability of the error being extremely small, such as $\mathbf{e} = \mathbf{0}$, is negligible. This lemma is used in Thm. 4.5 to prove the security of our ThPKE scheme.

Lemma 3.9. *If* $\mathsf{d/s\text{-}LWE}_{\mathbf{s}}(n, m, q, \chi)$ *is hard, then, for any* $m \geq n + \omega(\log n)$, *the probability* $P := \Pr_{\mathbf{e} \leftarrow \chi^m}[\forall e \in \mathbf{e}, e \in [0, 1)]$ *is negligible.*

Proof. We prove this by contradiction: We show that, if P is nonnegligible, there exists a PPT algorithm that solves $\mathsf{s\text{-}LWE}$. Let $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}) \leftarrow \mathsf{LWE}_{\mathbf{s}}(n, m, q, \chi)$; then, we have $\forall e \in \mathbf{e}$, $e \in [0, 1)$ with probability P. We calculate $\mathbf{b}'$ as follows: When $\mathbb{X}_q = \mathbb{R}_q$, define $\mathbf{b}' := \lfloor \mathbf{b} - 1/2 \cdot \mathbf{1} \rceil$ ($\mathbf{1} := (1, \ldots, 1)^\intercal \in \mathbb{Z}^m$), then we have $\mathbf{b}' = \lfloor \mathbf{A}\mathbf{s} + \mathbf{e} - 1/2 \cdot \mathbf{1} \rceil = \mathbf{A}\mathbf{s}$. When $\mathbb{X}_q = \mathbb{Z}_q$, $\forall e \in \mathbf{e}, e \in [0, 1)$ simply means $\mathbf{e} = \mathbf{0}$. Thus, we define $\mathbf{b}' := \mathbf{b} = \mathbf{A}\mathbf{s}$. By Lem. 2.8, with a probability of $1 - \mathrm{negl}(n)$, there exists a matrix $\mathbf{A}' \in \mathbb{Z}_q^{n \times m}$ such that $\mathbf{A}'\mathbf{A} = \mathbf{I}_n$. Calculate $\mathbf{A}'$, and then output $\mathbf{A}'\mathbf{b}' = \mathbf{s}$. Hence, $\mathsf{d\text{-}LWE}_{\mathbf{s}}(n, m, q, \chi)$ is also not hard by Fact 3.8. Since this contradicts the hypothesis, we complete the proof. □

There exists a reduction from LWE with a "small" error distribution to LWE with a "large" error distribution, where "small" and "large" are defined by the quasi-order defined in Def. 3.1:

Lemma 3.10. *If* $\mathsf{d/s\text{-}LWE}_{\mathbf{s}}(n, m, q, \chi_1)$ *is hard, then for any* $\chi_2 \geq \chi_1$, $\mathsf{d/s\text{-}LWE}_{\mathbf{s}}(n, m, q, \chi_2)$ *is also hard.*

Proof. By the definition of $\chi_2 \geq \chi_1$, there exists a distribution χ_δ such that $\chi_2 \approx_{\mathsf{s}} \chi_1 + \chi_\delta$. Let $(\mathbf{A}, \mathbf{b}) \leftarrow \mathsf{LWE}_{\mathbf{s}}(n, m, q, \chi_1)$, then sample $\mathbf{e}' \leftarrow \chi_\delta^m$ and define $\mathbf{b}' := \mathbf{b} + \mathbf{e}'$. Then, $(\mathbf{A}, \mathbf{b}') \approx_{\mathsf{s}} \mathsf{LWE}_{\mathbf{s}}(n, m, q, \chi_2)$ holds. Note that $\mathbf{b}' := \mathbf{b} + \mathbf{e}' \sim \mathcal{U}(\mathbb{X}_q^m)$ when $(\mathbf{A}, \mathbf{b}) \leftarrow \mathcal{U}(\mathbb{Z}_q^{m \times n} \times \mathbb{X}_q^m)$. □

3.3 Reused-A-LWE

We define the Reused-A-LWE problem [37] in Def. 3.11. Then, we show a self-reduction of Reused-A-LWE (Lem. 3.14) and a reduction from LWE to Reused-A-LWE for the discrete Gaussian distribution (Lem. 3.15).

Definition 3.11 (Reused-A-LWE (adapted from [12, Definition 5])). *Let n, m, $q \in \mathbb{N}$. Let $\mathbb{X}_q$ be either $\mathbb{Z}_q$ or $\mathbb{R}_q$, and let χ_1 and χ_2 be distributions on $\mathbb{X}_q$. For a fixed $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$, we define the Reused-A-LWE distribution $\mathsf{Reused\text{-}A\text{-}LWE}_{\mathbf{s}}(n, m, q, \chi_1, \chi_2)$ as follows:*

$$\left\{(\mathbf{A}, \mathbf{b}_1 := \mathbf{A}\mathbf{s} + \mathbf{e}_1, \mathbf{b}_2 := \mathbf{A}\mathbf{s} + \mathbf{e}_2) \;\middle|\; \mathbf{A} \sim \mathcal{U}(\mathbb{Z}_q^{m \times n}), \mathbf{e}_1 \sim \chi_1^m, \mathbf{e}_2 \sim \chi_2^m \right\}$$

Definition 3.12 (d-Reused-A-LWE). *$\mathsf{d\text{-}Reused\text{-}A\text{-}LWE}(n, m, q, \chi_1, \chi_2)$ is a problem to distinguish $\mathsf{Reused\text{-}A\text{-}LWE}_{\mathbf{s}}(n, m, q, \chi_1, \chi_2)$ from the following distribution:*

$$\mathcal{V} := \left\{ (\mathbf{A}, \mathbf{u}, \mathbf{v}) \;\middle|\; \begin{array}{l} \mathbf{A} \sim \mathcal{U}(\mathbb{Z}_q^{m \times n}), \mathbf{e}_1 \sim \chi_1^m, \mathbf{e}_2 \sim \chi_2^m \\ \mathbf{u} \sim \mathcal{U}(\mathbb{X}_q^m), \mathbf{v} := \mathbf{u} - (\mathbf{e}_1 - \mathbf{e}_2) \end{array} \right\}$$

The advantage *of an algorithm $\mathcal{A} : \mathbb{Z}_q^{m \times n} \times \mathbb{X}_q^m \times \mathbb{X}_q^m \to \{0, 1\}$ for solving $\mathsf{d\text{-}Reused\text{-}A\text{-}LWE}$ is defined as $\mathrm{Adv}_{\mathcal{A}}^{\mathsf{d\text{-}Reused\text{-}A\text{-}LWE}} = |\Pr[\mathcal{A}(\mathsf{Reused\text{-}A\text{-}LWE}_{\mathbf{s}}(n, m, q, \chi_1, \chi_2)) = 1] - \Pr[\mathcal{A}(\mathcal{V}) = 1]|$. We say that $\mathsf{d\text{-}Reused\text{-}A\text{-}LWE}$ is hard if $\mathrm{Adv}_{\mathcal{A}}^{\mathsf{d\text{-}Reused\text{-}A\text{-}LWE}} = \mathrm{negl}(n)$ for any PPT algorithm $\mathcal{A}$.*

Definition 3.13 (s-Reused-A-LWE). *$\mathsf{s\text{-}Reused\text{-}A\text{-}LWE}(n, m, q, \chi_1, \chi_2)$ is a problem to find $\mathbf{s}$ given samples from $\mathsf{Reused\text{-}A\text{-}LWE}_{\mathbf{s}}(n, m, q, \chi_1, \chi_2)$. We say that $\mathsf{s\text{-}Reused\text{-}A\text{-}LWE}$ is hard if any PPT algorithm can solve it only with $\mathrm{negl}(n)$ probability.*

Similar to Lem. 3.10, we obtain the self-reduction of Reused-A-LWE:

Lemma 3.14. *If $\mathsf{d\text{-}/s\text{-}Reused\text{-}A\text{-}LWE}(n, m, q, \chi_1, \chi_2)$ is hard, for any (mutually independent) $\chi_3 \geq \chi_1, \chi_4 \geq \chi_2$, $\mathsf{d\text{-}/s\text{-}Reused\text{-}A\text{-}LWE}(n, m, q, \chi_3, \chi_4)$ is also hard.*

Proof. By hypothesis, there exists χ_δ and χ'_δ such that $\chi_3 \approx_{\mathsf{s}} \chi_1 + \chi_\delta$ and $\chi_4 \approx_{\mathsf{s}} \chi_2 + \chi'_\delta$. Thus, we can (efficiently) transform $\mathsf{Reused\text{-}A\text{-}LWE}(n, m, q, \chi_1, \chi_2)$ to $\mathsf{Reused\text{-}A\text{-}LWE}(n, m, q, \chi_3, \chi_4)$ by adding errors from χ_δ and χ'_δ. □

We show a reduction from LWE to Reused-A-LWE for discrete Gaussian errors in the following Lem. 3.15. Although this is essentially a discrete analogue of prior work [37, Corollary 3], it is not straightforward: In the subsequent Lem. 3.16, we need to carefully choose Gaussian parameters that satisfy the required conditions regarding the smoothing parameter:

Lemma 3.15 (LWE $\leq$ Reused-A-LWE). *Let $s_2 > s_1 > 0$ be reals such that $s_0, s_\delta \geq 2\tilde{\eta}_\epsilon^+(\mathbb{Z})$, where $s_0 := s_1/2$ and $s_\delta := \sqrt{s_2^2 - s_1^2}$. If there exists a PPT algorithm that solves $\mathsf{d\text{-}/s\text{-}Reused\text{-}A\text{-}LWE}(n, m, q, D_{\mathbb{Z}, s_1}, D_{\mathbb{Z}, s_2})$ with advantage (resp. probability) ε, then there exists a PPT algorithm that solves $\mathsf{d\text{-}/s\text{-}LWE}(n, m, q, D_{\mathbb{Z}, s_0})$ with advantage (resp. probability) $\varepsilon - \mathrm{negl}(\lambda)$.*

Proof. Sample $(\mathbf{A}, \mathbf{b} := \mathbf{A}\mathbf{s}+\mathbf{e}) \leftarrow \mathsf{LWE}(n, m, q, D_{\mathbb{Z},s_0})$, $\mathbf{e}' \leftarrow (D_{\mathbb{Z},s_0})^m$, $\mathbf{e}_3, \mathbf{e}_4 \leftarrow (D_{\mathbb{Z},\sqrt{2}s_0})^m$, $\mathbf{e}_\delta \leftarrow (D_{\mathbb{Z},s_\delta})^m$ and define $\mathbf{b}_1 := \mathbf{b}+\mathbf{e}'+\mathbf{e}_3$, $\mathbf{b}_2 := \mathbf{b}-\mathbf{e}'+\mathbf{e}_4+\mathbf{e}_\delta$: We have $(\mathbf{A}, \mathbf{b}_1, \mathbf{b}_2) = (\mathbf{A}, \mathbf{A}\mathbf{s}+\mathbf{e}+\mathbf{e}'+\mathbf{e}_3, \mathbf{A}\mathbf{s}+\mathbf{e}-\mathbf{e}'+\mathbf{e}_4+\mathbf{e}_\delta)$. Hence, by subsequent Lem. 3.16, we obtain $(\mathbf{A}, \mathbf{b}_1, \mathbf{b}_2) \approx_\mathsf{s} (\mathbf{A}, \mathbf{A}\mathbf{s}+\mathbf{e}_1, \mathbf{A}\mathbf{s}+\mathbf{e}_2)$, where $\mathbf{e}_1 \sim (D_{\mathbb{Z},s_1})^m$ and $\mathbf{e}_2 \sim (D_{\mathbb{Z},s_2})^m$ are mutually independent and $\mathbf{b}_1 - \mathbf{b}_2 \approx_\mathsf{s} (D_{\mathbb{Z},\sqrt{s_1^2+s_2^2}})^m$. Thus, $(\mathbf{A}, \mathbf{b}_1, \mathbf{b}_2) \approx_\mathsf{s} \mathsf{Reused\text{-}A\text{-}LWE}(n, m, q, D_{\mathbb{Z},s_1}, D_{\mathbb{Z},s_2})$.

The above (efficient) algorithm transforms uniform $(\mathbf{A}, \mathbf{b}) \leftarrow \mathcal{U}(\mathbb{Z}_q^m, \mathbb{X}_q^m)$ to $(\mathbf{A}, \mathbf{u}, \mathbf{v})$ where $\mathbf{u} \sim \mathcal{U}(\mathbb{X}_q^m)$ and $\mathbf{v} = \mathbf{u} - (2\mathbf{e}' - \mathbf{e}_3 + \mathbf{e}_4 + \mathbf{e}_\delta)$. Thus, we obtain $\mathsf{d\text{-}LWE} \le \mathsf{d\text{-}Reused\text{-}A\text{-}LWE}$. Obviously, $\mathsf{s\text{-}LWE} \le \mathsf{s\text{-}Reused\text{-}A\text{-}LWE}$ also holds. □

The proof of Lem. 3.15 is completed by proving the deferred Lem. 3.16. Note that this is essentially a special case of [29, Lem. 1]. We provide the proof for the completeness.

Lemma 3.16. *Let $s_2 > s_1 > 0$ be reals such that $s_0, s_\delta \ge 2\tilde{\eta}_\epsilon^+(\mathbb{Z})$, where $s_0 := s_1/2$ and $s_\delta := \sqrt{s_2^2 - s_1^2}$. Then, we have*

$$
\begin{aligned}
X &:= \{(e_1, e_2) \mid e_1 \sim D_{\mathbb{Z},s_1}, e_2 \sim D_{\mathbb{Z},s_2}\} \\
\approx_\mathsf{s} Y &:= \{(e_1, \bar{e}_2 + e_\delta) \mid e_1, \bar{e}_2 \overset{\text{iid}}{\sim} D_{\mathbb{Z},s_1}, e_\delta \sim D_{\mathbb{Z},s_\delta}\} \\
\approx_\mathsf{s} Z &:= \left\{ (e - e' + e_3, e + e' + e_4 + e_\delta) \,\middle|\, \begin{array}{l} e, e' \overset{\text{iid}}{\sim} D_{\mathbb{Z},s_0}, e_3, e_4 \overset{\text{iid}}{\sim} D_{\mathbb{Z},\sqrt{2}s_0} \\ e_\delta \sim D_{\mathbb{Z},s_\delta} \end{array} \right\}
\end{aligned}
$$

and $(e + e' + e_4 + e_\delta) - (e - e' + e_3) = 2e' - e_3 + e_4 + e_\delta \approx_\mathsf{s} D_{\mathbb{Z},\sqrt{s_1^2+s_2^2}}$.

Proof. We obtain $\bar{e}_2 + e_\delta \approx_\mathsf{s} D_{\mathbb{Z},s_2}$ by Lem. 2.15 since $s_1, s_\delta > \tilde{\eta}_\epsilon^+(\mathbb{Z})$. Thus, $X \approx_\mathsf{s} Y$ holds. Let $\mathbf{T} = \left(\begin{smallmatrix} 1 & -1 \\ 1 & 1 \end{smallmatrix}\right)$ and $(e, e')^\intercal \sim D_{\mathbb{Z}^2,s_0}$. Then, we have $\mathbf{T}(e, e')^\intercal = (e-e', e+e') \sim D_{\mathbf{T}\mathbb{Z}^2,s_0\mathbf{T}}$ by Lem. 2.16. Since $s_0^2\mathbf{T}\mathbf{T}^\intercal = 2s_0^2\mathbf{I}$, we have $D_{\mathbf{T}\mathbb{Z}^2,s_0\mathbf{T}} = D_{\mathbf{T}\mathbb{Z}^2,\sqrt{2}s_0}$. We obtain $(e - e' + e_3, e + e' + e_4) \sim D_{\mathbf{T}\mathbb{Z}^2,\sqrt{2}s_0} + D_{\mathbb{Z}^2,\sqrt{2}s_0} \approx_\mathsf{s} D_{\mathbb{Z}^2,s_1}$ by Cor. 2.18 since $s_0 \ge 2\tilde{\eta}_\epsilon^+(\mathbb{Z}) > \|\mathbf{T}\|_{\text{len}}\eta_\epsilon^+(\mathbb{Z}^2)$. Thus, $Y \approx_\mathsf{s} Z$ holds. Finally, we obtain $2e' - e_3 + e_4 + e_\delta \approx_\mathsf{s} D_{\mathbb{Z},\sqrt{s_1^2+s_2^2}}$ by Lem. 2.15 since $s_0, s_\delta \ge 2\tilde{\eta}_\epsilon^+(\mathbb{Z})$. □

4 Simulation-Secure ThPKE from LWE

In this section, we present an efficient SS-ThPKE scheme whose security is "directly" reduced from the (standard) LWE problem.

We describe the construction of our scheme in Sect. 4.1. Then, we define and prove the correctness and security in Sect. 4.2 and Sect. 4.3, respectively. Finally, we provide an instantiation that satisfies correctness and security in Sect. 4.4.

4.1 Construction

Our ThPKE scheme is presented in Algo. 1. This scheme is constructed based on the ThPKE of [37] instantiated with the Regev-like PKE [43]. We modify the scheme by distributing shares $(\mathsf{err}_1, \ldots, \mathsf{err}_N)$ of a small error $\mathsf{err} := \boldsymbol{\zeta} \leftarrow \chi_\mathsf{err}$ for

Algorithm 1: Our LWE-based $\mathsf{ThPKE} := (\mathsf{Params}, \mathsf{KeyGen}, \mathsf{Setup}, \mathsf{Enc}, \mathsf{PartDec}, \mathsf{FinDec})$

$\underline{\mathsf{Params}(1^\lambda, 1^N) \to \mathsf{pp}}$:

1 Choose public parameters $\mathsf{pp} := (n, m, q, \chi_{\mathsf{pk}}, \chi_{\mathsf{enc}}, \chi_{\mathsf{sm}}, \chi_{\mathsf{err}})$.
Note: The following functions implicitly take pp as an argument.

$\underline{\mathsf{KeyGen}() \to (\mathsf{pk}, \mathsf{sk}, \mathsf{err}, \chi_{\mathsf{Sim}})}$:

2 $\mathsf{sk} := \mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$, $\mathsf{pk} := (\mathbf{A}, \mathbf{b} := \mathbf{As} + \mathbf{e}) \leftarrow \mathsf{LWE}_{\mathbf{s}}(n, m, q, \chi_{\mathsf{pk}})$
3 $\mathsf{err} := \boldsymbol{\zeta} \leftarrow \chi_{\mathsf{err}}$, and define a distribution $\chi_{\mathsf{Sim}}(\mathbf{e}, \boldsymbol{\zeta})$ as follows:

$$\chi_{\mathsf{Sim}}(\mathbf{e}, \boldsymbol{\zeta}) := \{e^{\mathsf{sm}} + \mathbf{r}_1^\intercal \boldsymbol{\zeta} - \mathbf{r}_2^\intercal \mathbf{e} \mid e^{\mathsf{sm}} \sim \chi_{\mathsf{sm}}, \mathbf{r}_1, \mathbf{r}_2 \overset{\text{iid}}{\sim} \chi_{\mathsf{enc}}^m\} \tag{2}$$

Note: χ_{Sim} is only used for the security proof (Algo. 2)

$\underline{\mathsf{Setup}(\mathsf{sk}, \mathsf{err}, \mathbb{A}) \to (\mathsf{sk}_1, \ldots, \mathsf{sk}_N, \mathsf{err}_1, \ldots, \mathsf{err}_N)}$:

4 $\mathsf{BinLSS.Share}((\mathbf{s}, \boldsymbol{\zeta}), \mathbb{A}) \to \{(\mathsf{sk}_i, \mathsf{err}_i) := \{(\mathbf{s}_j, \boldsymbol{\zeta}_j)\}_{j \in T_i}\}_{i \in [N]}$ (Def. 2.27)

$\underline{\mathsf{Enc}(\mathsf{pk}, \mu \in \mathcal{M} := \{0,1\}) \to \mathsf{ct}}$:

5 Define $\mathsf{msg} := \lfloor \frac{q}{2} \rfloor \cdot \mu$, and sample $\mathbf{r}, \mathbf{r}_{\mathsf{aux}} \leftarrow \chi_{\mathsf{enc}}^m$
6 Calculate $(\mathbf{a}', b') := (\mathbf{r}^\intercal \mathbf{A}, \mathbf{r}^\intercal \mathbf{b} + \mathsf{msg})$ and output a ciphertext $\mathsf{ct} := (\mathbf{a}', b', \mathbf{r}_{\mathsf{aux}})$
Note: $\mathbf{r}_{\mathsf{aux}}$ is auxiliary information which will be used in $\mathsf{PartDec}$.

$\underline{\mathsf{PartDec}(\mathsf{ct}, \mathsf{sk}_i, \mathsf{err}_i) \to \mathsf{pd}_i}$:

7 Parse $\mathsf{sk}_i = \{\mathbf{s}_j\}_{j \in T_i}$ and $\mathsf{err}_i = \{\boldsymbol{\zeta}_j\}_{j \in T_i}$
8 **for** $j \in T_i$ **do** Sample $e_j^{\mathsf{sm}} \leftarrow \chi_{\mathsf{sm}}$, and define $\mathbf{p}_j := (\mathbf{a}')^\intercal \mathbf{s}_j + e_j^{\mathsf{sm}} + \mathbf{r}_{\mathsf{aux}}^\intercal \boldsymbol{\zeta}_j$
9 Output a partial decryption $\mathsf{pd}_i := \{\mathbf{p}_j\}_{j \in T_i}$

$\underline{\mathsf{FinDec}(\{\mathsf{pd}_i\}_{i \in S}) \to \overline{\mu} \in \{0,1\} \text{ or } \bot}$:

10 **if** $S \notin \mathbb{A}$ **then** Output $\bot$ and **break**
11 Otherwise, parse $\{\mathsf{pd}_i\}_{i \in S} = \{\{\mathbf{p}_j\}_{j \in T_i}\}_{i \in S}$
12 Calculate a minimal valid share set $T \subseteq \bigcup_{i \in S} T_i$ (Def. 2.28)
13 Output $\overline{\mu} := \lfloor (b' - \sum_{i \in T} \mathbf{p}_i) / \lfloor \frac{q}{2} \rfloor \rceil$

"masking" the partial decryption to the parties with secret sharing, in addition to the shares $(\mathsf{sk}_1, \ldots, \mathsf{sk}_N)$ of the secret key $\mathsf{sk} := \mathbf{s}$. Then, we add a randomized value of err_i (specifically, $\mathbf{r}_{\mathsf{aux}}^\intercal \boldsymbol{\zeta}_j$) in the partial decryption ($\mathsf{PartDec}$, Line 8), in addition to the conventional "smudging noise" ($e^{\mathsf{sm}} \sim \chi_{\mathsf{sm}}$).

Our construction supports any access structure $\mathbb{A}$ that can be constructed with BinLSS (Def. 2.27), which includes any threshold access structures (Def. 2.29), as shown in Thm. 2.30.

4.2 Correctness

We define the correctness of ThPKE in Def. 4.1, and show a sufficient condition for our scheme to be correct in Lem. 4.2.

Definition 4.1 (Correctness). *We say that the ThPKE scheme defined in Algo. 1 is* correct *if* $\mathsf{FinDec}(\{\mathsf{pd}_i\}_{i \in S}) = \mu$ *holds with overwhelming probability for any* $S \in \mathbb{A}$ *and an overwhelming proportion of* $(\mathsf{pk}, \mathsf{sk}, \mathsf{err}) \leftarrow \mathsf{KeyGen}()$.

As preparation, we define a distribution $\chi_{\mathsf{Sim},t}(\mathbf{e},\boldsymbol{\zeta})$ with a parameter $t \in \mathbb{N}$ ($t \leq N$), which is a generalization of χ_{Sim} that is defined in (2):

$$\chi_{\mathsf{Sim},t}(\mathbf{e},\boldsymbol{\zeta}) := \left\{ \sum_{i=1}^{t} e_i^{\mathsf{sm}} + \mathbf{r}_1^{\intercal}\boldsymbol{\zeta} - \mathbf{r}_2^{\intercal}\mathbf{e} \;\middle|\; e_1^{\mathsf{sm}},\ldots,e_t^{\mathsf{sm}} \overset{\text{iid}}{\sim} \chi_{\mathsf{sm}}, \mathbf{r}_1,\mathbf{r}_2 \overset{\text{iid}}{\sim} \chi_{\mathsf{enc}}^{m} \right\} \quad (3)$$

Then, we derive the sufficient condition for Algo. 1 to be correct:

Lemma 4.2. *The ThPKE scheme defined in Algo. 1 is correct if we have* $\Pr_{x\leftarrow\chi_{\mathsf{Sim},t}}\left[|x| < \lfloor \frac{q}{4} \rfloor\right] = 1 - \mathrm{negl}(\lambda)$ *for an overwhelming proportion of* $(\mathsf{pk} := (\mathbf{A}, \mathbf{A}\mathbf{s}+\mathbf{e}), \mathsf{sk} := \mathbf{s}, \mathsf{err} := \boldsymbol{\zeta}) \leftarrow \mathsf{KeyGen}()$*, where* $\chi_{\mathsf{Sim},t}(\mathbf{e},\boldsymbol{\zeta})$ *is defined as in* (3) *and* $t = |T| (\leq N)$*.*

Proof. At Line 13 in Algo. 1, we have:

$$\begin{aligned} b' - \textstyle\sum_{i\in T}\mathbf{p}_i &= b' - (\mathbf{a}')^{\intercal}\mathbf{s} - \textstyle\sum_{i\in T} e_i^{\mathsf{sm}} - \mathbf{r}_{\mathsf{aux}}^{\intercal}\boldsymbol{\zeta} \\ &= \mathsf{msg} + \mathbf{r}^{\intercal}\mathbf{e} - \textstyle\sum_{i\in T} e_i^{\mathsf{sm}} - \mathbf{r}_{\mathsf{aux}}^{\intercal}\boldsymbol{\zeta} \end{aligned} \quad (4)$$

By hypothesis, $|\mathbf{r}^{\intercal}\mathbf{e} - \sum_{i\in T} e_i^{\mathsf{sm}} - \mathbf{r}_{\mathsf{aux}}^{\intercal}\boldsymbol{\zeta}| < \lfloor \frac{q}{4} \rfloor$ holds with overwhelming probability. Thus, $\overline{\mu} := \lfloor (b' - \sum_{i\in T}\mathbf{p}_i)/\lfloor \frac{q}{2} \rfloor \rceil = \mu + \lfloor (\mathbf{r}^{\intercal}\mathbf{e} - \sum_{i\in T} e_i^{\mathsf{sm}} - \mathbf{r}_{\mathsf{aux}}^{\intercal}\boldsymbol{\zeta})/\lfloor \frac{q}{2} \rfloor \rceil = \mu$ also holds with overwhelming probability. □

We provide a typical example of parameters that satisfy the correctness.

Example 4.3. *Let* χ_{pk} *and* χ_{err} *be the* B_{pk}*- and* B_{err}*-bounded (Def. 2.9) distributions over* $\mathbb{Z}_q$*, respectively. Let* $s_{\mathsf{enc}}, s_{\mathsf{sm}} \geq \max(B_{\mathsf{pk}}, B_{\mathsf{err}})\tilde{\eta}_{\epsilon}^{+}(\mathbb{Z})$*. The ThPKE scheme defined in Algo. 1 is correct for any* N*,* $m = \mathrm{poly}(n)$*,* q*,* B_{pk}*,* B_{err}*,* s_{enc} *and* s_{sm} *such that* $\sqrt{\lambda(Ns_{\mathsf{sm}}^2 + B^2 s_{\mathsf{enc}}^2)} < \lfloor \frac{q}{4} \rfloor$*, where* $B := B(m) := \sqrt{m(B_{\mathsf{pk}}^2 + B_{\mathsf{err}}^2)}$*.*

Proof. Define $\chi_{\mathsf{Sim},|T|}$ as in (3). We have $\chi_{\mathsf{Sim},|T|} \approx_{\mathsf{s}} D_{\mathbb{Z},\sqrt{|T|s_{\mathsf{sm}}^2 + s_{\mathsf{enc}}^2(\|\mathbf{e}\|^2 + \|\boldsymbol{\zeta}\|^2)}}$ holds by Lem. 2.15 since χ_{pk} and χ_{err} are bounded by B_{pk} and B_{err}, respectively. Furthermore, we have $\chi_{\mathsf{Sim},|T|} \leq D_{\mathbb{Z},\sqrt{Ns_{\mathsf{sm}}^2 + B^2 s_{\mathsf{enc}}^2}}$ by Def. 3.1 and Fact 3.4 since $\|\mathbf{e}\| < B_{\mathsf{pk}}\sqrt{m}$ and $\|\boldsymbol{\zeta}\| < B_{\mathsf{err}}\sqrt{m}$ holds with overwhelming probability and $|T| \leq N$. Thus, by Lem. 2.23, we have $\Pr_{x\leftarrow\chi_{\mathsf{Sim},|T|}}[x < \sqrt{\lambda(Ns_{\mathsf{sm}}^2 + B^2 s_{\mathsf{enc}}^2)}] = 1 - \mathrm{negl}(\lambda)$. □

4.3 Simulation Security

We define the simulation security of our ThPKE scheme:

Definition 4.4 (Simulation security (SS)). *We say that the ThPKE scheme is simulation secure if, for any PPT distinguisher* $\mathcal{D}$ *and the stateful*[5] *PPT algorithm* $\mathcal{A} := (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$*, there exists a PPT algorithm* Sim *such that*

$$\mathrm{Adv}^{\mathsf{SS\text{-}ThPKE}}_{\mathcal{D},\mathcal{A},\mathsf{Sim}}(1^\lambda) := \left| \begin{array}{c} \Pr[\mathcal{D}(\mathsf{Expt}_{\mathcal{A},\mathsf{Real}}(1^\lambda)) = 1] \\ -\Pr[\mathcal{D}(\mathsf{Expt}_{\mathcal{A},\mathsf{Sim},\mathsf{Ideal}}(1^\lambda)) = 1] \end{array} \right| = \mathrm{negl}(\lambda), \quad (5)$$

where the experiments $\mathsf{Expt}_{\mathcal{A},\mathsf{Real}}(1^\lambda)$ *and* $\mathsf{Expt}_{\mathcal{A},\mathsf{Sim},\mathsf{Ideal}}(1^\lambda)$ *are defined as in Algo. 2. Additionally, for fixed outputs of Lines 1 to 3 of Algo. 2, the adversary can repeat Lines 4 to 6 for arbitrary* $\mathrm{poly}(\lambda)$ *times.*

Algorithm 2: Experiments ($\mathsf{Expt}_{\mathcal{A},\mathsf{Real}}$ and $\mathsf{Expt}_{\mathcal{A},\mathsf{Sim},\mathsf{Ideal}}$) that define the simulation security (Def. 4.4) of our ThPKE and the hybrid experiments ($\mathsf{Expt}_{\mathcal{A},\mathsf{Sim},\mathsf{Hybrid}_{\{1,2\}}}$). Note that $\mathcal{A} := (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ is a stateful algorithm although we omit writing state in the inputs and outputs.

$\underline{\mathsf{Expt}_{\mathcal{A},\mathsf{Real}}(1^\lambda)}$:
1 $\mathsf{pp} \leftarrow \mathsf{Params}(1^\lambda, 1^N)$, $(\mathsf{sk}, \mathsf{err}, \mathsf{pk}, \chi_{\mathsf{Sim}}) \leftarrow \mathsf{KeyGen}()$
2 $(\mathsf{sk}_1, \dots, \mathsf{sk}_N, \mathsf{err}_1, \dots, \mathsf{err}_N) \leftarrow \mathsf{Setup}(\mathsf{sk}, \mathsf{err}, \mathbb{A})$
3 $\mu \in \mathcal{M}$ and a maximal invalid party set $S_{\mathsf{mal}} \subsetneq [N] \leftarrow \mathcal{A}_1(\mathsf{pp}, \mathsf{pk}, \chi_{\mathsf{Sim}})$
4 $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, \mu)$
5 A (valid) party set $S \subseteq [N] \leftarrow \mathcal{A}_2(\{\mathsf{sk}_i, \mathsf{err}_i\}_{i \in S_{\mathsf{mal}}}, \mathsf{ct})$
6 **for** $i \in S$ **do** $\mathsf{pd}_i \leftarrow \mathsf{PartDec}(\mathsf{pk}, \mathsf{ct}, \mathsf{sk}_i, \mathsf{err}_i)$
7 **return** $\{0,1\} \leftarrow \mathcal{A}_3(\{\mathsf{pd}_i\}_{i \in S})$

$\underline{\mathsf{Expt}_{\mathcal{A},\mathsf{Sim},\mathsf{Hybrid}_1}(1^\lambda)}$: Same as $\mathsf{Expt}_{\mathcal{A},\mathsf{Real}}$ except that Line 6 is replaced with:
8 $\{\mathsf{pd}_i\}_{i \in S} \leftarrow \mathsf{Sim}(\{\mathsf{sk}_i, \mathsf{err}_i\}_{i \in S_{\mathsf{mal}}}, \mathsf{ct}, \mu, \chi_{\mathsf{Sim}})$

$\underline{\mathsf{Expt}_{\mathcal{A},\mathsf{Sim},\mathsf{Hybrid}_2}(1^\lambda)}$: In addition, Line 2 in $\mathsf{Expt}_{\mathcal{A},\mathsf{Real}}$ is replaced with:
9 $(\mathsf{sk}_1, \dots, \mathsf{sk}_N, \mathsf{err}_1, \dots, \mathsf{err}_N) \leftarrow \mathsf{Setup}(\mathbf{0}, \mathbf{0}, \mathbb{A})$

$\underline{\mathsf{Expt}_{\mathcal{A},\mathsf{Sim},\mathsf{Ideal}}(1^\lambda)}$: In addition, Line 4 in $\mathsf{Expt}_{\mathcal{A},\mathsf{Real}}$ is replaced with:
10 $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, \overline{\mu})$, where $\overline{\mu} \xleftarrow{\$} \mathcal{M}$ is independent of μ

Here, we prove the security of our ThPKE scheme under an ad-hoc assumption that $\chi_{\mathsf{Sim}}(\mathbf{e}, \boldsymbol{\zeta})$ (defined in (2)) does not leak any information about the fixed $\mathbf{e}$ and $\boldsymbol{\zeta}$ generated by KeyGen. In addition, the $\mathsf{d\text{-}Reused\text{-}A\text{-}LWE}$ assumption is also needed. These assumption are removed in subsequent Thm. 4.6. by instantiating the error distributions χ_{pk}, χ_{enc}, χ_{sm} and χ_{err} appropriately.

Theorem 4.5. *Let $m \geq n \log q + 2\lambda$, and assume both $\mathsf{d\text{-}LWE}(n, m, q, \chi_{\mathsf{pk}})$ and $\mathsf{d\text{-}Reused\text{-}A\text{-}LWE}(n, m, q, \chi_{\mathsf{enc}}, \chi_{\mathsf{sm}})$ are hard. In addition, assume it is hard to obtain any information about $\mathbf{e}$ and $\boldsymbol{\zeta}$ (other than $\mathbf{e} \sim \chi_{\mathsf{pk}}$) given samples from $\chi_{\mathsf{Sim}}(\mathbf{e}, \boldsymbol{\zeta})$ defined in (2). Then, Algo. 1 satisfies SS (Def. 4.4).*

Proof. We show that, for any PPT distinguisher $\mathcal{D}$ and the stateful PPT algorithm $\mathcal{A}$, there exists a PPT simulator Sim such that (5) holds. In addition to $\mathsf{Expt}_{\mathcal{A},\mathsf{Real}}$ and $\mathsf{Expt}_{\mathcal{A},\mathsf{Sim},\mathsf{Ideal}}$, we also define an intermediate hybrid experiments $\mathsf{Expt}_{\mathcal{A},\mathsf{Sim},\mathsf{Hybrid}_1}$ and $\mathsf{Expt}_{\mathcal{A},\mathsf{Sim},\mathsf{Hybrid}_2}$ as described in Algo. 2. Then, it is sufficient to show that there exists Sim such that the following hold:

$$\mathsf{Expt}_{\mathcal{A},\mathsf{Real}} \approx_{\mathsf{c}} \mathsf{Expt}_{\mathcal{A},\mathsf{Sim},\mathsf{Hybrid}_1} \tag{6}$$

$$\mathsf{Expt}_{\mathcal{A},\mathsf{Sim},\mathsf{Hybrid}_1} \approx_{\mathsf{c}} \mathsf{Expt}_{\mathcal{A},\mathsf{Sim},\mathsf{Hybrid}_2} \tag{7}$$

$$\mathsf{Expt}_{\mathcal{A},\mathsf{Sim},\mathsf{Hybrid}_2} \approx_{\mathsf{c}} \mathsf{Expt}_{\mathcal{A},\mathsf{Sim},\mathsf{Ideal}} \tag{8}$$

[5] means $\mathcal{A}_i$ inherits the inputs, outputs, and internal states of $\mathcal{A}_1, \dots, \mathcal{A}_{i-1}$ for $i = 2, 3$.

Eq. (7) follows by definition of the privacy of BinLSS (Defs. 2.26 and 2.27). Additionally, Thm. 2.30 shows that BinLSS supports any threshold access structure (Def. 2.29). Eq. (8) follows from the semantic security of the underlying $\mathsf{PKE} := (\mathsf{ThPKE.KeyGen}, \mathsf{ThPKE.Enc})$ (without decryption), which is proved by [43, Lem. 5.4] since $\mathsf{d\text{-}LWE}(n, m, q, \chi_{\mathsf{pk}})$ is hard by hypothesis. Therefore, we only have to prove (6). We show how to construct a simulator Sim that satisfies (6) in the following.

The adversary $\mathcal{A}$ can calculate a maximal invalid share set T_{mal} (Def. 2.28) from given $\bigcup_{i\in S_{\mathsf{mal}}} T_i$ because $S_{\mathsf{mal}} \subsetneq \{P_1, \ldots, P_N\}$ in Line 2 is a maximal invalid party set (Def. 2.25). Now, we (conservatively) assume that $\mathcal{A}_2$ chooses a *valid* party set S in Line 5 and analyze the distribution of $\mathbf{p}_j$ in $\{\mathsf{pd}_i\}_{i\in S} = \{\{\mathbf{p}_j\}_{j\in T_i} \leftarrow \mathsf{PartDec}(\mathsf{pk}, \mathsf{ct}, \mathsf{sk}_i, \mathsf{err}_i)\}_{i\in S}$ such that $j \notin T_{\mathsf{mal}}$. Let $T := T_{\mathsf{mal}} \cup \{j\}$; then, T is a minimal valid share set because T_{mal} is a maximal invalid share set. Thus, by the correctness of BinLSS (Def. 2.26), we have $\sum_{i\in T}\mathbf{s}_i = \sum_{i\in T_{\mathsf{mal}}}\mathbf{s}_i + \mathbf{s}_j = \mathbf{s}^{\mathsf{mal}} + \mathbf{s}_j = \mathbf{s}$ and $\sum_{i\in T}\boldsymbol{\zeta}_i = \sum_{i\in T_{\mathsf{mal}}}\boldsymbol{\zeta}_i + \boldsymbol{\zeta}_j = \boldsymbol{\zeta}^{\mathsf{mal}} + \boldsymbol{\zeta}_j = \boldsymbol{\zeta}$, where $\mathbf{s}^{\mathsf{mal}} := \sum_{i\in T_{\mathsf{mal}}}\mathbf{s}_i$ and $\boldsymbol{\zeta}^{\mathsf{mal}} := \sum_{i\in T_{\mathsf{mal}}}\boldsymbol{\zeta}_i$. Then, by (4),

$$b' - (\mathbf{a}')^{\intercal}\mathbf{s} - \mathsf{msg} = \mathbf{r}^{\intercal}\mathbf{e} \Leftrightarrow b' - (\mathbf{a}')^{\intercal}\mathbf{s}^{\mathsf{mal}} - \mathsf{msg} = (\mathbf{a}')^{\intercal}\mathbf{s}_j + \mathbf{r}^{\intercal}\mathbf{e} \tag{9}$$

holds. The left-hand side of this equation can be computed from $\mathbf{s}^{\mathsf{mal}}$, ct, and μ, which are given to the adversary. We define this as:

$$\mathsf{Atk}_j := \mathsf{Atk}_j(\mathbf{s}^{\mathsf{mal}}, \mathsf{ct}, \mu) := (\mathbf{a}')^{\intercal}\mathbf{s}_j + \mathbf{r}^{\intercal}\mathbf{e} \tag{10}$$

We also define Real_j, which can also be calculated by the adversary, as follows:

$$\mathsf{Real}_j := \mathbf{p}_j + \mathbf{r}_{\mathsf{aux}}^{\intercal}\boldsymbol{\zeta}^{\mathsf{mal}} = (\mathbf{a}')^{\intercal}\mathbf{s}_j + e_j^{\mathsf{sm}} + \mathbf{r}_{\mathsf{aux}}^{\intercal}\boldsymbol{\zeta}. \tag{11}$$

Combining (10) and (11) yields:

$$(\mathbf{a}', \mathsf{Real}_j, \mathsf{Atk}_j) = (\mathbf{a}', (\mathbf{a}')^{\intercal}\mathbf{s}_j + e_j^{\mathsf{sm}} + \mathbf{r}_{\mathsf{aux}}^{\intercal}\boldsymbol{\zeta}, (\mathbf{a}')^{\intercal}\mathbf{s}_j + \mathbf{r}^{\intercal}\mathbf{e})$$

We have $\mathbf{a}' \approx_{\mathsf{s}} \mathcal{U}(\mathbb{Z}_q^n)$ from Lem. 2.6 and Fact 2.7, and $\mathbf{s}_j \sim \mathcal{U}(\mathbb{Z}_q^n)$ from Def. 2.27. Thus, we have $\mathsf{Real}_j \approx_{\mathsf{s}} \mathsf{LWE}_{\mathbf{s}_j}(n, 1, q, \chi_{\mathsf{Real}})$, $\mathsf{Atk}_j \approx_{\mathsf{s}} \mathsf{LWE}_{\mathbf{s}_j}(n, 1, q, \chi_{\mathsf{Atk}})$, and

$$(\mathbf{a}', \mathsf{Real}_j, \mathsf{Atk}_j) \approx_{\mathsf{s}} \mathsf{Reused\text{-}A\text{-}LWE}_{\mathbf{s}_j}(n, 1, q, \chi_{\mathsf{Real}}, \chi_{\mathsf{Atk}}), \tag{12}$$

where $\mathsf{Reused\text{-}A\text{-}LWE}$ is defined as in Def. 3.11 and

$$\chi_{\mathsf{Real}} := \chi_{\mathsf{Real}}(\boldsymbol{\zeta}) := \{e^{\mathsf{sm}} + \mathbf{r}_{\mathsf{aux}}^{\intercal}\boldsymbol{\zeta} \mid e^{\mathsf{sm}} \sim \chi_{\mathsf{sm}}, \mathbf{r}_{\mathsf{aux}} \sim \chi_{\mathsf{enc}}^m\}, \text{ and}$$
$$\chi_{\mathsf{Atk}} := \chi_{\mathsf{Atk}}(\mathbf{e}) := \{\mathbf{r}^{\intercal}\mathbf{e} \mid \mathbf{r} \sim \chi_{\mathsf{enc}}^m\}.$$

Note that the adversary can obtain fresh $(\mathbf{a}', \mathsf{Real}_j, \mathsf{Atk}_j)$ for any $m' = \mathrm{poly}(\lambda)$ ciphertexts for a fixed pk. In this case, we have $\{\mathbf{a}'^k, \mathsf{Real}_j^k, \mathsf{Atk}_j^k\}_{k\in[m']} \approx_{\mathsf{s}} \mathsf{Reused\text{-}A\text{-}LWE}_{\mathbf{s}_j}(n, m', q, \chi_{\mathsf{Real}}, \chi_{\mathsf{Atk}})$, and the rest of the proof follows similarly.

We now show that $\mathsf{d\text{-}Reused\text{-}A\text{-}LWE}_{\mathbf{s}_j}(n, 1, q, \chi_{\mathsf{Real}}, \chi_{\mathsf{Atk}})$ is hard by Lem. 3.14: Since $\mathsf{d\text{-}Reused\text{-}A\text{-}LWE}_{\mathbf{s}}(n, m, q, \chi_{\mathsf{sm}}, \chi_{\mathsf{enc}})$ is hard by hypothesis, we only need

to prove that $\chi_{\mathsf{sm}} \leq \chi_{\mathsf{Real}}$ and $\chi_{\mathsf{enc}} \leq \chi_{\mathsf{Atk}}$ (Def. 3.1). We have $\chi_{\mathsf{sm}} \leq \chi_{\mathsf{Real}}$ because $e_{\mathsf{sm}} \leftarrow \chi_{\mathsf{sm}}$ is sampled independently of $\mathbf{r}_{\mathsf{aux}}^{\intercal}\boldsymbol{\zeta}$. By Lem. 3.9, at least one element in $\mathbf{e}$ is larger than 1 with overwhelming probability over the choice of $\mathsf{pk} \leftarrow \mathsf{KeyGen}()$. Thus, we have $\chi_{\mathsf{enc}} \leq \chi_{\mathsf{Atk}}$.

Therefore, by Def. 3.12 and (12), we have:

$$(\mathbf{a}', \mathsf{Real}_j, \mathsf{Atk}_j) \approx_{\mathsf{c}} \mathcal{V} := \left\{ (\mathbf{a}', \mathbf{u}, \mathbf{v}) \;\middle|\; \begin{array}{l} \mathbf{u} \sim \mathcal{U}(\mathbb{X}_q^m), \\ \mathbf{v} = \mathbf{u} - (e_j^{\mathsf{sm}} + \mathbf{r}_{\mathsf{aux}}^{\intercal}\boldsymbol{\zeta} - \mathbf{r}^{\intercal}\mathbf{e}) \end{array} \right\}$$

Because $\mathbf{p}_j = \mathsf{Real}_j - \mathbf{r}_{\mathsf{aux}}^{\intercal}\boldsymbol{\zeta}^{\mathsf{mal}}$ by (11), we also have:

$$(\mathbf{a}', \mathbf{p}_j, \mathsf{Atk}_j - \mathbf{r}_{\mathsf{aux}}^{\intercal}\boldsymbol{\zeta}^{\mathsf{mal}}) \approx_{\mathsf{c}} \mathcal{V}' := \left\{ (\mathbf{a}', \mathbf{u}', \mathbf{v}') \;\middle|\; \begin{array}{l} \mathbf{u}' \sim \mathcal{U}(\mathbb{X}_q^m), \\ \mathbf{v}' = \mathbf{u}' - (e_j^{\mathsf{sm}} + \mathbf{r}_{\mathsf{aux}}^{\intercal}\boldsymbol{\zeta} - \mathbf{r}^{\intercal}\mathbf{e}) \end{array} \right\}$$

This means that, from $\mathbf{p}_j$ and $\mathsf{Atk}_j - \mathbf{r}_{\mathsf{aux}}^{\intercal}\boldsymbol{\zeta}^{\mathsf{mal}}$, it is computationally hard to obtain any information other than that we have

$$\mathbf{p}_j - (\mathsf{Atk}_j - \mathbf{r}_{\mathsf{aux}}^{\intercal}\boldsymbol{\zeta}^{\mathsf{mal}}) = (e_j^{\mathsf{sm}} + \mathbf{r}_{\mathsf{aux}}^{\intercal}\boldsymbol{\zeta} - \mathbf{r}^{\intercal}\mathbf{e}) \sim \chi_{\mathsf{Sim}},$$

where χ_{Sim} is defined as in (2). Let $e_{\mathsf{sim}} \leftarrow \chi_{\mathsf{Sim}}$ and define

$$\mathsf{Sim}'_j := \mathsf{Sim}'_j(\{\mathbf{s}_i, \boldsymbol{\zeta}_i\}_{i \in T_{\mathsf{mal}}}, \mathsf{ct}, \mu, \chi_{\mathsf{Sim}}) := \mathsf{Atk}_j - \mathbf{r}_{\mathsf{aux}}^{\intercal}\boldsymbol{\zeta}^{\mathsf{mal}} + e_{\mathsf{sim}}.$$

Then, we have $\mathsf{Sim}'_j \approx_{\mathsf{c}} \mathbf{p}_j$. Hence, we construct Sim in Line 8 of Algo. 2 as $\mathsf{Sim}(\{\mathsf{sk}_i, \mathsf{err}_i\}_{i \in S_{\mathsf{mal}}}, \mathsf{ct}, \mu, \chi_{\mathsf{Sim}}) = \{\{\mathsf{Sim}_j\}_{j \in T_i}\}_{i \in S}$, where:

$$\mathsf{Sim}_j := \mathsf{Sim}_j(\{\mathbf{s}_i, \boldsymbol{\zeta}_i\}_{i \in T_{\mathsf{mal}}}, \mathsf{ct}, \mu, \chi_{\mathsf{Sim}}) := \begin{cases} \mathbf{p}_j & (j \in T_{\mathsf{mal}}) \\ \mathsf{Sim}'_j & (\text{otherwise}) \end{cases}$$

Then, $\{\mathsf{pd}_i\}_{i \in S}$ in Line 6 and Line 8 are computationally indistinguishable. Thus, we obtain (6) for Sim constructed as above. □

4.4 Instantiation: ThPKE without Known-norm LWE

In this subsection, we show in Thm. 4.6 that there exist an instance that simultaneously satisfies correctness (Lem. 4.2) and security (Thm. 4.5).

We disclose χ_{Sim} (defined in (2)) to the adversary $\mathcal{A}$ (and Sim) in Algo. 2 because the adversary can obtain samples that follow χ_{Sim} repeatedly for any $\mathrm{poly}(\lambda)$ iterations by calculating $\mathsf{Real}_j - \mathsf{Atk}_j$, where Atk_j and Real_j are defined in (10) and (11), respectively. In the construction of [37], χ_{Sim} corresponds to $\mathcal{N}_{\sqrt{\sigma_{\mathsf{sm}}^2 + \sigma_{\mathsf{enc}}^2 \|\mathbf{e}\|^2}}$. Hence, the adversary can accurately estimate $\|\mathbf{e}\|$ by calculating the variance of χ_{Sim}. Thus, the ThPKE scheme of [37] requires "known-norm LWE" to prove the security of the underlying PKE.

In contrast, we show in subsequent Thm. 4.6 that there exist distributions χ_{enc}, χ_{sm} and χ_{err} such that no information about $\mathbf{e} \leftarrow \chi_{\mathsf{pk}}$ can be obtained from χ_{Sim}. We first let $\chi_{\mathsf{enc}} = D_{\mathbb{Z}, s_{\mathsf{enc}}}$ and $\chi_{\mathsf{sm}} = D_{\mathbb{Z}, s_{\mathsf{sm}}}$. Then, by Lem. 2.15, we have

$$\chi_{\mathsf{Sim}} \approx_{\mathsf{s}} D_{\mathbb{Z}, \sqrt{s_{\mathsf{sm}}^2 + s_{\mathsf{enc}}^2 (\|\mathbf{e}\|^2 + \|\boldsymbol{\zeta}\|^2)}}$$

(for sufficiently large s_{enc} and s_{sm}). Furthermore, in KeyGen, we sample $\boldsymbol{\zeta} \leftarrow \chi_{\mathsf{err}} := \chi_{\mathsf{err}}(\mathbf{e}, B)$ conditioned on a fixed $\mathbf{e} \leftarrow \chi_{\mathsf{pk}}$ so that $\|\mathbf{e}\|^2 + \|\boldsymbol{\zeta}\|^2 = B^2$ holds, where B is a (sufficiently large) *public* constant. Then, we have

$$\chi_{\mathsf{Sim}} \approx_{\mathsf{s}} D_{\mathbb{Z}, \sqrt{s_{\mathsf{sm}}^2 + s_{\mathsf{enc}}^2 B^2}}.$$

Thus, χ_{Sim} contains no information about $\mathbf{e}$. Note that we instantiate $\chi_{\mathsf{pk}} := D_{\mathbb{Z}, s_{\mathsf{pk}}}$ in Thm. 4.6 only for concreteness: Other bounded distributions over $\mathbb{Z}$ can also be used.

Theorem 4.6. *Let* $s_{\mathsf{pk}} \geq \tilde{\eta}_\epsilon^+(\mathbb{Z})$, $s_{\mathsf{sm}}, s_{\mathsf{enc}} \geq \sqrt{\lambda} s_{\mathsf{pk}} \tilde{\eta}_\epsilon^+(\mathbb{Z})$ *such that* $\sqrt{|s_{\mathsf{sm}}^2 - s_{\mathsf{enc}}^2|} \geq 2\tilde{\eta}_\epsilon^+(\mathbb{Z})$. *Select parameters* N, n, q, $m \geq n \log q + 2\lambda$, *such that* $\sqrt{\lambda(N s_{\mathsf{sm}}^2 + B^2 s_{\mathsf{enc}}^2)} < \lfloor \frac{q}{4} \rfloor$, *where* $B := \sqrt{\lceil 2m s_{\mathsf{pk}}^2 \rceil}$. *Let* $\chi_{\mathsf{pk}} = D_{\mathbb{Z}, s_{\mathsf{pk}}}$, *and* $\chi_{\mathsf{sm}} = D_{\mathbb{Z}, s_{\mathsf{sm}}}$. *In* $\mathsf{KeyGen}()$, *we generate and fix* $\mathsf{pk} := (\mathbf{A}, \mathbf{b} := \mathbf{A}\mathbf{s} + \mathbf{e})$, *and then, define* $\chi_{\mathsf{err}} := \chi_{\mathsf{err}}(\mathbf{e}, B)$ *as a distribution over*

$$\mathcal{B}_{\mathbf{e}, B} := \{\boldsymbol{\zeta} \in \mathbb{Z}_q^m \mid \|\boldsymbol{\zeta}\|^2 = B^2 - \|\mathbf{e}\|^2, \|\boldsymbol{\zeta}\|_\infty < 2s_{\mathsf{pk}}\}. \tag{13}$$

Assume $\mathsf{d\text{-}LWE}_{\mathsf{s}}(n, m, q, \chi_{\mathsf{pk}})$ *is hard. Then, Algo. 1 instantiated (and modified) as above satisfies SS (Def. 4.4) and correctness (Def. 4.1).*

Proof. We have $\|\mathbf{e}\|_\infty \leq \sqrt{\lambda} s_{\mathsf{pk}}$ with overwhelming probability by Lem. 2.23, and $\|\boldsymbol{\zeta}\|_\infty < 2s_{\mathsf{pk}} < \sqrt{\lambda} s_{\mathsf{pk}}$ by definition. Hence, by Lem. 2.15, we have $\chi_{\mathsf{Sim}} \approx_{\mathsf{s}} D_{\mathbb{Z}, \sqrt{s_{\mathsf{sm}}^2 + (\|\mathbf{e}\|^2 + \|\boldsymbol{\zeta}\|^2) s_{\mathsf{enc}}^2}} = D_{\mathbb{Z}, \sqrt{s_{\mathsf{sm}}^2 + B^2 s_{\mathsf{enc}}^2}}$ since $s_{\mathsf{enc}}, s_{\mathsf{sm}} \geq \sqrt{\lambda} s_{\mathsf{pk}} \tilde{\eta}_\epsilon^+(\mathbb{Z})$, where χ_{Sim} is defined in (2). Thus, χ_{Sim} has no information about $\mathbf{e}$ because $B^2 = \lceil 2m s_{\mathsf{pk}}^2 \rceil$ is a public constant. Furthermore, since $\mathsf{d\text{-}LWE}(n, m, q, \chi_{\mathsf{pk}})$ is hard by hypothesis, $\mathsf{d\text{-}Reused\text{-}A\text{-}LWE}(n, m, q, \chi_{\mathsf{enc}}, \chi_{\mathsf{sm}})$ is also hard by Lem. 3.15 and Lem. 3.10 as $s_{\mathsf{enc}}, s_{\mathsf{sm}} > 2s_{\mathsf{pk}} \geq 2\tilde{\eta}_\epsilon^+(\mathbb{Z})$ and $\sqrt{|s_{\mathsf{enc}}^2 - s_{\mathsf{sm}}^2|} \geq 2\tilde{\eta}_\epsilon^+(\mathbb{Z})$. Hence, SS is satisfied by Thm. 4.5.

The proof of the correctness is similar to that of Ex. 4.3. As we showed $\chi_{\mathsf{Sim}} \approx_{\mathsf{s}} D_{\mathbb{Z}, \sqrt{s_{\mathsf{sm}}^2 + B^2 s_{\mathsf{enc}}^2}}$, we also have $\chi_{\mathsf{Sim}, N} \approx_{\mathsf{s}} D_{\mathbb{Z}, \sqrt{N s_{\mathsf{sm}}^2 + B^2 s_{\mathsf{enc}}^2}}$, where $\chi_{\mathsf{Sim}, t}$ is defined as in (3). By Lem. 2.23, we have $\Pr_{x \leftarrow \chi_{\mathsf{Sim}, |T|}}[x < \sqrt{\lambda(N s_{\mathsf{sm}}^2 + B^2 s_{\mathsf{enc}}^2)}] = 1 - \mathrm{negl}(n)$. Thus, the correctness holds by Lem. 4.2.

By Lem. 2.22, $\|\mathbf{e}\| \leq s_{\mathsf{pk}} \sqrt{m}$ holds with overwhelming probability. Thus, $R := \sqrt{B^2 - \|\mathbf{e}\|^2} \in (\sqrt{m} s_{\mathsf{pk}}, \sqrt{2m} s_{\mathsf{pk}})$ and $\beta := \lfloor R / \sqrt{\frac{m}{2}} \rfloor < 2s_{\mathsf{pk}}$ also holds with overwhelming probability. Hence, as shown in subsequent Lem. 4.7, there exists a distribution χ_{err} over $\mathcal{B}_{\mathbf{e}, B}$ defined in (13). □

We complete the proof of Thm. 4.6 by proving deferred Lem. 4.7: We show an example of the distribution χ_{err} that satisfies (13):

Lemma 4.7. *Let* $m \geq 2\lambda$, $q \in \mathbb{N}$ *and* R *be a real number such that* $R^2 \in \mathbb{N}$, $10\sqrt{\frac{m}{2}} < R < \sqrt{m} q$ *and* $R < \sqrt{\frac{m}{2}} \cdot 2^{\frac{m}{4} - 6}$. *Define a set* $\mathcal{B}_R := \{\boldsymbol{\zeta} \in \mathbb{Z}_q^m \mid \|\boldsymbol{\zeta}\|^2 = R^2\}$. *Then, there exists a (efficiently samplable) distribution* χ_{err} *over* $\mathcal{B}_R$ *that satisfies* $\|\boldsymbol{\zeta}\|_\infty \leq \beta := \lfloor R / \sqrt{\frac{m}{2}} \rfloor$ *for any* $\boldsymbol{\zeta} \leftarrow \chi_{\mathsf{err}}$.

Algorithm 3: An algorithm to sample $\boldsymbol{\zeta} \in S_R$

Input : $R \in \mathbb{R}$ s.t. $R^2 \in \mathbb{N}$, $10\sqrt{\frac{m}{2}} \leq R < \sqrt{mq}$ and $R < \sqrt{\frac{m}{2}} \cdot 2^{\frac{m}{4}-6}$
Output : $\boldsymbol{\zeta} \in S_R := \{\boldsymbol{\zeta} \in \mathbb{Z}_q^m \mid \|\boldsymbol{\zeta}\|^2 = R^2\}$ s.t. $\|\boldsymbol{\zeta}\|_\infty \leq \beta$

1 Define $\beta := \lfloor R/\sqrt{\frac{m}{2}} \rfloor \geq 10$ // $\beta\sqrt{\frac{m}{2}} \leq R < (\beta+1)\sqrt{\frac{m}{2}}$
2 Sample $\boldsymbol{\zeta}_1 \xleftarrow{\$} \{(\beta-1), \beta\}^{\frac{m}{2}}$ // $\|\boldsymbol{\zeta}_1\|^2 \geq (\beta-1)^2\frac{m}{2}$
3 $\overline{R} := \sqrt{R^2 - \|\boldsymbol{\zeta}_1\|^2} \in \mathbb{R}$ // $\overline{R}^2 \leq R^2 - (\beta-1)^2\frac{m}{2} < 2\beta m$
4 $m' := \lfloor \overline{R}^2 / \lceil\sqrt{8\beta}\rceil^2 \rfloor$ // $m' \leq \overline{R}^2/8\beta < \frac{m}{4}$
5 $u_1, \ldots, u_{m'} := \lceil\sqrt{8\beta}\rceil$ // $\sum_{i=1}^{m'} u_i^2 = \lceil\sqrt{8\beta}\rceil^2 m' \leq \overline{R}^2 < \lceil\sqrt{8\beta}\rceil^2(m'+1)$
6 $r_1 := \sqrt{\overline{R}^2 - \sum_{i=1}^{m'} u_i^2} \in \mathbb{R}$ // $0 \leq r_1 < \lceil\sqrt{8\beta}\rceil \leq \beta$
7 $t := \lfloor \log r_1 \rfloor - 1$ // $t \leq \log r_1 < \log\beta < \frac{m}{4} - 6$
8 **for** $i = 2$ **to** $t+7$ **do** $r_i := \sqrt{r_{i-1}^2 - \lfloor r_{i-1} \rfloor^2}$
9 $\boldsymbol{\zeta}_2 := (u_1, \ldots, u_{m'}, \lfloor r_1 \rfloor, \ldots, \lfloor r_{t+6} \rfloor, 0, \ldots, 0) \in \mathbb{Z}_q^{m/2}$ // $r_{t+7} = 0, \|\boldsymbol{\zeta}_2\|^2 = \overline{R}^2$
10 **return** $\boldsymbol{\zeta} := (\boldsymbol{\zeta}_1 \parallel \boldsymbol{\zeta}_2) \in \mathbb{Z}_q^m$, *which is the concatenation of* $\boldsymbol{\zeta}_1, \boldsymbol{\zeta}_2 \in \mathbb{Z}_q^{m/2}$

Proof. We define χ_{err} as the distribution formed by $\boldsymbol{\zeta}$ sampled by Algo. 3. The algorithm first samples binary random numbers $\boldsymbol{\zeta}_1 \xleftarrow{\$} \{(\beta-1), \beta\}^{\frac{m}{2}}$.Then it deterministically selects $\boldsymbol{\zeta}_2 \in \mathbb{Z}_q^{m/2}$ such that $\boldsymbol{\zeta} := (\boldsymbol{\zeta}_1 \parallel \boldsymbol{\zeta}_2)$ satisfy $\|\boldsymbol{\zeta}\|^2 = R^2$ and $\|\boldsymbol{\zeta}\|_\infty \leq \beta$.

As you can see from the comments written in Algo. 3, we can show that $r_1 \leq \beta$ holds at Line 8 by construction. Here, we show that $r_{t+7} = 0$ holds at Line 9. For any $t \geq 2$,

$$r_t := \sqrt{r_{t-1}^2 - \lfloor r_{t-1} \rfloor^2} < \sqrt{2r_{t-1}} \tag{14}$$

holds because we have $x^2 - \lfloor x \rfloor^2 = x^2 - (x-\xi)^2 = 2x\xi - \xi^2 < 2x$ ($\xi := x - \lfloor x \rfloor \in [0,1)$) for any $x \in \mathbb{R}_{>0}$. Hence, because $\sqrt{2x} \leq x/2$ for any $x \geq 8$, we have $r_t < \sqrt{2r_{t-1}} \leq \frac{1}{2}r_{t-1} < \frac{1}{2}\sqrt{2r_{t-2}} \leq \frac{1}{2^2}r_{t-2} < \cdots \leq \frac{1}{2^{t-1}}r_1$, when $r_{t-1} \geq 8$. Therefore, let $t := \lfloor \log r_1 \rfloor - 1$, then we have $r_t < \frac{1}{2^{t-1}}r_1 < 8$ because $\log r_1 < t + 2 \Leftrightarrow r_1 < 2^{t+2}$. Furthermore, again by (14), we have $r_t < 8, r_{t+1} < 4, r_{t+2} < \sqrt{8}$. Additionally, note that $r_t^2 \in \mathbb{Z}$ holds for any t by (14) because r_1^2 is an integer. Thus, $r_{t+2}^2 \in \{0, 1, \ldots, 7\}$. Furthermore, $r_t < r_{t-1}$ holds for any $r_{t-1} \geq 1$ because we have: $r_t := \sqrt{r_{t-1}^2 - \lfloor r_{t-1} \rfloor^2} < r_{t-1} \Leftrightarrow 1 \leq r_{t-1}$. Thus, we have $r_{t+3} < \sqrt{7}, r_{t+4} < \sqrt{6}, r_{t+5} < \sqrt{5}, r_{t+6} < \sqrt{4} = 2$. Hence, $r_{t+6}^2 \in \{0, 1\}$, i.e., $r_{t+6} \in \{0, 1\}$ holds, and this implies that $r_{t+7} = 0$. Because $\sqrt{\frac{m}{2}} \cdot 2^{\frac{m}{4}-6}$ by hypothesis, we have $t + 6 < \log r_1 + 6 < \log\beta + 6 < \log 2^{\frac{m}{4}-6} + 6 = \frac{m}{4}$. Thus, we have $m' + t + 6 < \frac{m}{2}$; this $\boldsymbol{\zeta}_2$ defined as in Line 9 is in $\mathbb{Z}_q^{m/2}$. By $r_t^2 := r_{t-1}^2 - \lfloor r_{t-1} \rfloor^2$, $\sum_{i=1}^{t-1} \lfloor r_i \rfloor^2 = r_1^2 - r_t^2$ holds. Hence, we have $\sum_{i=1}^{t+6} \lfloor r_i \rfloor^2 = r_1^2 - r_{t+7}^2 = r_1^2$ and $\|\boldsymbol{\zeta}_2\|^2 = r_1^2 + \sum_{i=1}^{m'} u_i^2 = \overline{R}^2$. Note that every element in $\boldsymbol{\zeta}$ is $\leq \beta$, i.e., $\|\boldsymbol{\zeta}\|_\infty \leq \beta$. □

5 Simulation-Secure ThPKE from Ring-LWE

In this section, we present an efficient SS-ThPKE whose security is (directly) reduced from the (standard) Ring-LWE problem.

We first provide definitions and preliminaries related to the Ring-LWE problem in Sect. 5.1. Then, we present our Ring-LWE-based ThPKE in Sect. 5.2. We define and prove correctness and security of our scheme in Sect. 5.3 and Sect. 5.4, respectively. Finally, in Sect. 5.5, we provide a concrete scheme instantiated with discrete Gaussian error distributions and prove its correctness and security.

5.1 Preliminaries for Ring-LWE

We define $\mathcal{R} = \mathbb{Z}[X]/(X^n+1)$ and $\mathcal{R}_q = \mathbb{Z}_q[X]/(X^n+1)$ for n a power of 2 and $q \in \mathbb{N}$. We define the *coefficient vector*, *coefficient matrix* and *coefficient Gram matrix* as follows:

Definition 5.1. *Let* $a = \sum_{i=0}^{n-1} a_i X^i \in \mathcal{R}$*, and define the coefficient vector of* a *as* $\mathbf{a} := \mathsf{vec}(a) := (a_0, a_1, \ldots, a_{n-1})^\intercal \in \mathbb{Z}^n$*. Let* $\mathbf{P} := \left(\begin{array}{c|c} \mathbf{0} & -1 \\ \hline \mathbf{I}_{n-1} & \mathbf{0} \end{array}\right) \in \mathbb{Z}^{n\times n}$ *(negacyclic permutation), and define the coefficient matrix of* a *as* $\mathbf{A} := \mathsf{mat}(a) := \left(\mathbf{a}\ \mathbf{Pa} \cdots \mathbf{P}^{n-1}\mathbf{a}\right) \in \mathbb{Z}^{n\times n}$*. The coefficient Gram matrix of* a *is defined as* $\mathbf{\Sigma}_a := \mathsf{Gram}(a) := \mathbf{A}\mathbf{A}^\intercal \in \mathbb{Z}^{n\times n}$*.*

We also define $\|a\| := \|\mathbf{a}\|$ and $\|a\|_\infty := \|\mathbf{a}\|_\infty$. For a distribution χ over $\mathbb{Z}$ and $a \in \mathcal{R}$, we write $a \sim \chi^n$ (resp. $a \leftarrow \chi^n$) to mean $\mathbf{a} \sim \chi^n$ (resp. $\mathbf{a} \leftarrow \chi^n$). The coefficient matrix is useful for deriving the coefficient vector of a product:

Fact 5.2. *For* $r, e \in \mathcal{R}$*, we have* $\mathsf{vec}(re) = \mathbf{Re} = \mathbf{Er}$*, where* $\mathbf{R} := \mathsf{mat}(r)$*,* $\mathbf{r} := \mathsf{vec}(r)$*,* $\mathbf{E} := \mathsf{mat}(e)$ *and* $\mathbf{e} := \mathsf{vec}(e)$*.*

Due to the structure of $\mathcal{R}$, we obtain the following useful facts:

Fact 5.3. *Let* $a \in \mathcal{R}$ *and define* $\mathbf{a} := \mathsf{vec}(a)$ *and* $\mathbf{A} := \mathsf{mat}(a)$*. Then, we have* $\|\mathbf{a}\| = \|\mathbf{A}\|_{\mathrm{len}} (\leq \|\mathbf{A}\|) \leq \|\mathbf{A}\|_F = \sqrt{n} \cdot \|\mathbf{a}\|$*.*

Fact 5.4. *For* $a, b \in \mathcal{R}$*, we have* $ab = 0$ *if and only if* $a = 0$ *or* $b = 0$*. Thus,* $\mathbf{A} := \mathsf{mat}(a)$ *is nonsingular for any* $a \neq 0$*.*

The Ring-LWE problem is defined as follows:

Definition 5.5 (Ring-LWE). *Let* n *be a power of* 2 *and let* $q \geq 2$ *be an integer. Let* χ *be an error distribution over* $\mathbb{Z}$*. The Ring-LWE distribution for a fixed secret* $s \leftarrow \chi^n$ *is defined as follows:*

$$\mathsf{RLWE}_s(n, q, \chi) := \{(a, b) \mid a \xleftarrow{\$} \mathcal{R}_q, b = s \cdot a + e, e \leftarrow \chi^n\}$$

Definition 5.6 (Decision Ring-LWE). $\mathsf{d\text{-}RLWE}_s(n, q, \chi)$ *is a problem to distinguish* $\mathsf{RLWE}_s(n, q, \chi)$ *and* $\mathcal{U}(\mathcal{R}_q \times \mathcal{R}_q)$*.*

We also define a slight variant of RLWE where $s \leftarrow \mathcal{U}(\mathbb{Z}_q^n)$ instead of $s \leftarrow \chi^n$, which is denoted by $\mathsf{RLWE}_{s\sim\mathcal{U}}$. Note that $\mathsf{d\text{-}RLWE}_{s\sim\mathcal{U}}(n, q, \chi)$ is at least as hard as $\mathsf{d\text{-}RLWE}_s(n, q, \chi)$:

Lemma 5.7. *If* $\mathsf{d\text{-}RLWE}_s(n, q, \chi)$ *is hard, then* $\mathsf{d\text{-}RLWE}_{s\sim\mathcal{U}}(n, q, \chi)$ *is also hard.*

Proof. Given $(a, b) \leftarrow \mathsf{RLWE}_s(n, q, \chi)$, sample $\tilde{s} \leftarrow \mathcal{U}(\mathbb{Z}_q^n)$ and output $(a, b') := (a, b + a\tilde{s})$. Then, $(a, b') \sim \mathsf{RLWE}_{s' \sim \mathcal{U}}(n, q, \chi)$, where $s' := s + \tilde{s} \sim \mathcal{U}(\mathbb{Z}_q^n)$. □

We also obtain the counterpart of Lems. 3.9 and 3.10 for Ring-LWE:

Corollary 5.8. *If* $\mathsf{d\text{-}RLWE}_s(n, q, \chi)$ *is hard,* $\Pr_{e \leftarrow \chi^n}[e = 0]$ *is negligible.*

Corollary 5.9. *If* $\mathsf{d\text{-}RLWE}_{s_1}(n, q, \chi_1)$ *is hard, then for any* $\chi_2 \geq \chi_1$, $\mathsf{d\text{-}RLWE}_{s_2}(n, q, \chi_2)$ *is also hard.*

Proof. By Def. 3.1, there exists χ_δ such that $\chi_2 \approx_{\mathsf{s}} \chi_1 + \chi_\delta$. Given $(a, b = as_1 + e_1) \leftarrow \mathsf{RLWE}_{s_1}(n, q, \chi_1)$, sample $s_\delta, e_\delta \leftarrow \chi_\delta^n$ and output $(a, b') := (a, b + as_\delta + e_\delta) = (a, a(s_1 + s_\delta) + (e_1 + e_\delta))$; then, $(a, b') \approx_{\mathsf{s}} \mathsf{RLWE}_{s_2}(n, q, \chi_2)$. □

We define the "Reused-A" variant of RLWE, which is a counterpart of Def. 3.11. For simplicity, we define it only for uniformly random s.

Definition 5.10 (Reused-A-RLWE). *Let* n, $q \in \mathbb{N}$. *Let* χ_1, χ_2 *be distributions over* $\mathbb{Z}$. *For fixed* $s \leftarrow \mathcal{U}(\mathbb{Z}_q^n)$, $\mathsf{Reused\text{-}A\text{-}RLWE}_s(n, q, \chi_1, \chi_2)$ *is defined as follows:*

$$\{(a, b_1 := as + e_1, b_2 := as + e_2) \mid a \sim \mathcal{U}(\mathcal{R}_q), e_1 \sim \chi_1^n, e_2 \sim \chi_2^n\}$$

Definition 5.11 (d-Reused-A-LWE). $\mathsf{d\text{-}Reused\text{-}A\text{-}LWE}(n, q, \chi_1, \chi_2)$ *is a problem to distinguish* $\mathsf{Reused\text{-}A\text{-}LWE}_s(n, q, \chi_1, \chi_2)$ *from*

$$\mathcal{V} := \{(a, u, v) \mid a, u \sim \mathcal{U}(\mathcal{R}_q), e_1 \sim \chi_1^n, e_2 \sim \chi_2^n, v := u - (e_1 - e_2)\}.$$

We obtain a counterpart of Lems. 3.14 and 3.15 as follows:

Corollary 5.12 (d-RLWE $\leq$ d-Reused-A-RLWE). *Let* $s_2 > s_1 > 0$ *be reals such that* $s_0, s_\delta \geq 2\tilde{\eta}_\epsilon^+(\mathbb{Z})$, *where* $s_0 := s_1/2$ *and* $s_\delta := \sqrt{s_2^2 - s_1^2}$. *If there exists a PPT algorithm that solves* $\mathsf{d\text{-}Reused\text{-}A\text{-}RLWE}(n, q, D_{\mathbb{Z}, s_1}, D_{\mathbb{Z}, s_2})$ *with advantage* ε, *then there exists a PPT algorithm that solves* $\mathsf{d\text{-}RLWE}(n, q, D_{\mathbb{Z}, s_0})$ *with advantage* $\varepsilon - \mathrm{negl}(\lambda)$.

Proof. By Lem. 5.7, we can transform $\mathsf{RLWE}_s(n, q, D_{\mathbb{Z}, s_0})$ to $\mathsf{RLWE}_{s \sim \mathcal{U}}(n, q, D_{\mathbb{Z}, s_0})$. The rest of the proof is identical to that of Lem. 3.15. □

Corollary 5.13. *If* $\mathsf{d\text{-}Reused\text{-}A\text{-}RLWE}(n, q, \chi_1, \chi_2)$ *is hard, for any (mutually independent)* $\chi_3 \geq \chi_1, \chi_4 \geq \chi_2$, $\mathsf{d\text{-}Reused\text{-}A\text{-}RLWE}(n, q, \chi_3, \chi_4)$ *is also hard.*

5.2 Construction

We present our construction of ThPKE from Ring-LWE in Algo. 4. This is essentially equivalent to Algo. 1, except that the underlying PKE is replaced with the Ring-LWE-based PKE presented by Lyubashevsky, Peikert and Regev [31].

Because the syntax of Algo. 4 is identical to that of Algo. 1, correctness and simulation security of Algo. 4 are also defined by Def. 4.1 and Def. 4.4, respectively.

Algorithm 4: Our Ring-LWE-based $\mathsf{ThPKE} := (\mathsf{Params}, \mathsf{KeyGen}, \mathsf{Setup}, \mathsf{Enc}, \mathsf{PartDec}, \mathsf{FinDec})$

$\underline{\mathsf{Params}(1^\lambda, 1^N) \to \mathsf{pp}}$:

Output public parameters $\mathsf{pp} := (n, m, q, \chi_{\mathsf{pk}}, \chi_{\mathsf{enc}}, \chi_{\mathsf{sm}}, \chi_{\mathsf{err}})$.

Note: The following functions implicitly take pp as an argument.

$\underline{\mathsf{KeyGen}() \to (\mathsf{pk}, \mathsf{sk}, \mathsf{err}, \chi_{\mathsf{Sim}})}$:

$\mathsf{sk} := s \leftarrow \chi_{\mathsf{pk}}^n$, $\mathsf{pk} := (a, b := sa + e) \leftarrow \mathsf{RLWE}_s(n, q, \chi_{\mathsf{pk}})$

$\mathsf{err} := \zeta \leftarrow \chi_{\mathsf{err}}$, and define a distribution χ_{Sim} as follows:

$$\chi_{\mathsf{Sim}}(s, e, \zeta) := \{e^{\mathsf{sm}} + r_{\mathsf{aux}}\zeta - re - e_1 s - e_2 \mid e^{\mathsf{sm}} \sim \chi_{\mathsf{sm}}^n, r, r_{\mathsf{aux}}, e_1, e_2 \overset{\text{iid}}{\sim} \chi_{\mathsf{enc}}^n\} \quad (15)$$

Note: χ_{Sim} is only used for the security proof (Algo. 2).

$\underline{\mathsf{Setup}(\mathsf{sk}, \mathsf{err}, \mathbb{A}) \to (\mathsf{sk}_1, \ldots, \mathsf{sk}_N, \mathsf{err}_1, \ldots, \mathsf{err}_N)}$:

Perform $\mathsf{BinLSS.Share}((s, \zeta), \mathbb{A}) \to \{(\mathsf{sk}_i, \mathsf{err}_i) := \{(s_j, \zeta_j)\}_{j \in T_i}\}_{i \in [N]}$

Note: BinLSS is performed for the coefficient vectors.

$\underline{\mathsf{Enc}(\mathsf{pk}, \mu \in \mathcal{M} := R_2) \to \mathsf{ct}}$:

Sample $r_{\mathsf{aux}}, r, e_1, e_2 \leftarrow \chi_{\mathsf{enc}}^n$, and define $\mathsf{msg} := \lfloor \frac{q}{2} \rfloor \cdot \mu$

$(a', b') := (ar - e_1, br + e_2 + \mathsf{msg})$

Output $\mathsf{ct} := (a', b', r_{\mathsf{aux}})$

$\underline{\mathsf{PartDec}(\mathsf{ct}, \mathsf{sk}_i, \mathsf{err}_i) \to \mathsf{pd}_i}$:

Parse $\mathsf{sk}_i = \{s_j\}_{j \in T_i}$ and $\mathsf{err}_i = \{\zeta_j\}_{j \in T_i}$

for $j \in T_i$ **do** Sample $e_j^{\mathsf{sm}} \leftarrow \chi_{\mathsf{sm}}^n$, and calculate $p_j := a' s_j + e_j^{\mathsf{sm}} + r_{\mathsf{aux}}\zeta_j$

Output $\mathsf{pd}_i := \{p_j\}_{j \in T_i}$

$\underline{\mathsf{FinDec}(\{\mathsf{pd}_i\}_{i \in S}) \to \overline{\mu} \in \{0, 1\} \text{ or } \perp}$:

if $S \notin \mathbb{A}$ **then** Output $\perp$ and **break**

Otherwise, parse $\{\mathsf{pd}_i\}_{i \in S} = \{\{p_j\}_{j \in T_i}\}_{i \in S}$

Calculate a minimal valid share set $T \subseteq \bigcup_{i \in S} T_i$ (Def. 2.28)

Output $\overline{\mu} := \lfloor (b' - \sum_{i \in T} p_i) / \lfloor \frac{q}{2} \rfloor \rceil$

5.3 Correctness

As preparation, we define a distribution $\chi_{\mathsf{Sim},t}(s, e, \zeta)$ with a parameter $t \leq N$, which is a generalization of χ_{Sim} that is defined in (15):

$$\chi_{\mathsf{Sim},t}(s, e, \zeta) := \left\{ \sum_{i=1}^t e_i^{\mathsf{sm}} + r_{\mathsf{aux}}\zeta - re - e_1 s - e_2 \;\middle|\; \begin{array}{l} e_1^{\mathsf{sm}}, \ldots, e_t^{\mathsf{sm}} \overset{\text{iid}}{\sim} \chi_{\mathsf{sm}}^n \\ r, r_{\mathsf{aux}}, e_1, e_2 \overset{\text{iid}}{\sim} \chi_{\mathsf{enc}}^n \end{array} \right\} \quad (16)$$

Then, we show a sufficient condition for Algo. 4 to be correct, i.e., the counterpart of Lem. 4.2:

Lemma 5.14. *The ThPKE scheme defined in Algo. 4 is correct if we have* $\Pr_{x \leftarrow \chi_{\mathsf{Sim},t}}\left[\|x\|_\infty < \lfloor \frac{q}{4} \rfloor\right] = 1 - \mathrm{negl}(\lambda)$ *for an overwhelming proportion of* $(\mathsf{pk}, \mathsf{sk}, \mathsf{err}) \leftarrow \mathsf{KeyGen}()$*, where* $\chi_{\mathsf{Sim},t}(s, e, \zeta)$ *is defined in* (16) *and* $t = |T| (\leq N)$.

Proof. At Line 14 in Algo. 4, we have:

$$\begin{aligned} b' - \textstyle\sum_{i\in T} p_i &= b' - a's - \textstyle\sum_{i\in T} e_i^{\mathsf{sm}} - r_{\mathsf{aux}}\zeta \\ &= \mathsf{msg} - (\textstyle\sum_{i\in T} e_i^{\mathsf{sm}} + r_{\mathsf{aux}}\zeta - re - e_1 s - e_2) \end{aligned} \tag{17}$$

By hypothesis, $\|\sum_{i\in T} e_i^{\mathsf{sm}} + r_{\mathsf{aux}}\zeta - re - e_1 s - e_2\|_\infty < \lfloor \frac{q}{4} \rfloor$ holds with overwhelming probability. Thus, $\overline{\mu} := \lfloor (b' - \sum_{i\in T} p_i)/\lfloor \frac{q}{2} \rfloor \rceil = \mu$ also holds with overwhelming probability. □

5.4 Simulation Security

We prove the security of Algo. 4, which is a counterpart of Thm. 4.5. Note that the following Thm. 5.15 also relies on ad-hoc assumptions, which are removed by instantiating the error distributions χ_{pk}, χ_{enc}, χ_{sm} and χ_{err} in Thm. 5.16.

Theorem 5.15. *Let $\chi_{\mathsf{pk}} \leq \chi_{\mathsf{enc}}$ and assume that both* $\mathsf{d\text{-}RLWE}(n, q, \chi_{\mathsf{pk}})$ *and* $\mathsf{d\text{-}Reused\text{-}A\text{-}RLWE}(n, q, \chi_{\mathsf{enc}}, \chi_{\mathsf{sm}})$ *are hard. In addition, assume it is hard to obtain any information about e, s from samples of $\chi_{\mathsf{Sim}}(s, e, \zeta)$ defined in (15), where $s, e \leftarrow \chi_{\mathsf{pk}}^n$ and $\zeta \leftarrow \chi_{\mathsf{err}}$. Then, Algo. 4 satisfies SS (Def. 4.4).*

Proof. Since the proof is almost identical to that of Thm. 4.5, we only describe different parts. Eq. (8) follows from the semantic security of the underlying $\mathsf{PKE} := (\mathsf{ThPKE.KeyGen}, \mathsf{ThPKE.Enc})$ (without decryption), which is identical to that of [31]. The semantic security holds by $\mathsf{d\text{-}RLWE}(n, q, \chi_{\mathsf{pk}})$ assumption.

Next, we proceed from the counterpart of (9). The shares of s and ζ are denoted by $\{s_i\}_{i\in T}$ and $\{\zeta_i\}_{i\in T}$. We have $\sum_{i\in T} s_i = s$ and $\sum_{i\in T} \zeta_i = \zeta$. We also define $\sum_{i\in T_{\mathsf{mal}}} s_i = s^{\mathsf{mal}}$ and $\sum_{i\in T_{\mathsf{mal}}} \zeta_i = \zeta^{\mathsf{mal}}$. By (17) and $s = s^{\mathsf{mal}} + s_j$, we have $b' - a's - \mathsf{msg} = re + e_1 s + e_2 \Leftrightarrow b' - a's^{\mathsf{mal}} - \mathsf{msg} = a's_j + re + e_1 s + e_2$. We define the right-hand side of the above as:

$$\mathsf{Atk}_j := \mathsf{Atk}_j(s^{\mathsf{mal}}, \mathsf{ct}, \mu) := a's_j + re + e_1 s + e_2 \tag{18}$$

Furthermore, we define:

$$\mathsf{Real}_j := p_j + r_{\mathsf{aux}}\zeta^{\mathsf{mal}} = a's_j + e_j^{\mathsf{sm}} + r_{\mathsf{aux}}\zeta \tag{19}$$

Combining (18) and (19) yields:

$$(a', \mathsf{Real}_j, \mathsf{Atk}_j) = (a', a's_j + e_j^{\mathsf{sm}} + r_{\mathsf{aux}}\zeta, a's_j + re + e_1 s + e_2)$$

$\mathsf{d\text{-}RLWE}_r(n, q, \chi_{\mathsf{enc}})$ is hard by Cor. 5.9 since $\mathsf{d\text{-}RLWE}_s(n, q, \chi_{\mathsf{pk}})$ is hard by hypothesis. Thus, we have $a' = ar - e_1 \approx_{\mathsf{c}} \mathcal{U}(\mathbb{Z}_q^n)$ (as in [31]). We also have $s_j \sim \mathcal{U}(\mathbb{Z}_q^n)$ by Def. 2.27. Hence, we have $\mathsf{Real}_j \approx_{\mathsf{c}} \mathsf{RLWE}_{s_j \sim \mathcal{U}}(n, q, \chi_{\mathsf{Real}})$, $\mathsf{Atk}_j \approx_{\mathsf{c}} \mathsf{RLWE}_{s_j \sim \mathcal{U}}(n, q, \chi_{\mathsf{Atk}})$, and

$$(a', \mathsf{Real}_j, \mathsf{Atk}_j) \approx_{\mathsf{c}} \mathsf{Reused\text{-}A\text{-}RLWE}_{s_j}(n, q, \chi_{\mathsf{Real}}, \chi_{\mathsf{Atk}}), \tag{20}$$

where Reused-A-RLWE is defined as in Def. 5.10 and

$$\chi_{\mathsf{Real}} := \chi_{\mathsf{Real}}(\zeta) := \{e^{\mathsf{sm}} + r_{\mathsf{aux}}\zeta \mid e^{\mathsf{sm}} \sim \chi_{\mathsf{sm}}^n, r_{\mathsf{aux}} \sim \chi_{\mathsf{enc}}^n\}, \text{ and}$$
$$\chi_{\mathsf{Atk}} := \chi_{\mathsf{Atk}}(s,e) := \left\{re + e_1 s + e_2 \mid r, e_1, e_2 \overset{\text{iid}}{\sim} \chi_{\mathsf{enc}}^n\right\}.$$

Since $\mathsf{d\text{-}Reused\text{-}A\text{-}RLWE}_s(n, q, \chi_{\mathsf{enc}}, \chi_{\mathsf{sm}})$ is hard by hypothesis, $\mathsf{d\text{-}Reused\text{-}A\text{-}RLWE}_{s_j}(n, q, \chi_{\mathsf{Real}}, \chi_{\mathsf{Atk}})$ is also hard by Cor. 5.13 and the fact that $\chi_{\mathsf{sm}} \le \chi_{\mathsf{Real}}$ and $\chi_{\mathsf{enc}} \le \chi_{\mathsf{Atk}}$ holds. Therefore, by (20) and Def. 5.11, we have

$$(a', \mathsf{Real}_j, \mathsf{Atk}_j) \approx_{\mathsf{c}} \mathcal{V} := \left\{(a', u, v) \;\middle|\; \begin{array}{l} u \sim \mathcal{U}(\mathcal{R}_q), \\ v = u - (e_j^{\mathsf{sm}} + r_{\mathsf{aux}}\zeta - re) \end{array}\right\}.$$

Since $p_j = \mathsf{Real}_j - r_{\mathsf{aux}}\zeta^{\mathsf{mal}}$ by (19), we also have

$$(a', p_j, \mathsf{Atk}_j - r_{\mathsf{aux}}\zeta^{\mathsf{mal}}) \approx_{\mathsf{c}} \mathcal{V}' := \left\{(a', u', v') \;\middle|\; \begin{array}{l} u' \sim \mathcal{U}(\mathcal{R}_q), \\ v' = u' - (e_j^{\mathsf{sm}} + r_{\mathsf{aux}}\zeta - re) \end{array}\right\}.$$

The rest of the proof is identical to that of Thm. 4.5. □

5.5 Instantiation: ThPKE without Known-covariance Ring-LWE

Finally, we show the counterpart of Thm. 4.6: we show an instance that satisfies SS and correctness:

Theorem 5.16. *Let* $s_{\mathsf{pk}} \ge \tilde{\eta}_\epsilon^+(\mathbb{Z}^n)$, $s_{\mathsf{sm}} \ge 2s_{\mathsf{pk}}$, $s_{\mathsf{enc}} \ge 2ns_{\mathsf{pk}}^2\eta_\epsilon^+(\mathbb{Z}^n)$ *such that* $\sqrt{s_{\mathsf{enc}}^2 - s_{\mathsf{sm}}^2} \ge 2\tilde{\eta}_\epsilon^+(\mathbb{Z})$ *and set* $\chi_{\mathsf{pk}} = D_{\mathbb{Z},s_{\mathsf{pk}}}$, $\chi_{\mathsf{sm}} = D_{\mathbb{Z},s_{\mathsf{sm}}}$, *and* $\chi_{\mathsf{enc}} = D_{\mathbb{Z},s_{\mathsf{enc}}}$. *Let* $\beta_{\mathsf{pub}} \in \mathcal{R}$ *be a fixed public polynomial such that* $\mathbf{\Sigma}_{\beta_{\mathsf{pub}}} := \mathsf{Gram}(\beta_{\mathsf{pub}})$ *satisfies* $\mathbf{\Sigma}_{\beta_{\mathsf{pub}}} \succ 2(\mathbf{\Sigma}_e + \mathbf{\Sigma}_s)$ *for an overwhelming proportion of* $e, s \leftarrow \chi_{\mathsf{pk}}^n$ *and* $\|\boldsymbol{\beta}_{\mathsf{pub}}\|^2 = \mathrm{poly}(\lambda)$, *where* $\boldsymbol{\beta}_{\mathsf{pub}} := \mathsf{vec}(\beta_{\mathsf{pub}})$, $\mathbf{\Sigma}_e := \mathsf{Gram}(e)$, *and* $\mathbf{\Sigma}_s := \mathsf{Gram}(s)$. *Select parameters* N, n, q *such that* $\|\sqrt{\mathbf{\Sigma}}\|\sqrt{n} < \lfloor \frac{q}{4} \rfloor$, *where* $\mathbf{\Sigma} := (Ns_{\mathsf{sm}}^2 + s_{\mathsf{enc}}^2)\mathbf{I}_n + s_{\mathsf{enc}}^2\mathbf{\Sigma}_{\beta_{\mathsf{pub}}}$. *In* KeyGen, *conditioned on fixed* $s, e \leftarrow \chi_{\mathsf{pk}}$, *we define* $\chi_{\mathsf{err}}(s, e, \mathbf{\Sigma}_{\beta_{\mathsf{pub}}})$ *as a distribution over* $\{\zeta \in \mathcal{R} \mid \mathsf{Gram}(\zeta) := \mathbf{\Sigma}_\zeta = \mathbf{\Sigma}_{\beta_{\mathsf{pub}}} - \mathbf{\Sigma}_e - \mathbf{\Sigma}_s, \|\boldsymbol{\zeta}\| \le 2s_{\mathsf{pk}}\sqrt{n}\}$.

Assume $\mathsf{d\text{-}RLWE}_s(n, q, D_{\mathbb{Z},s_{\mathsf{pk}}})$ *is hard. Then, Algo. 4 instantiated (and modified) as above satisfies SS (Def. 4.4) and correctness (Def. 4.1).*

Proof. By subsequent Lem. 5.17, we obtain $\chi_{\mathsf{Sim}}(s, e, \zeta) = \chi_{\mathsf{Sim},1}(s, e, \zeta) \approx_{\mathsf{s}} D_{\mathbb{Z}^n, \sqrt{(s_{\mathsf{sm}}^2 + s_{\mathsf{enc}}^2)\mathbf{I}_n + s_{\mathsf{enc}}^2\mathbf{\Sigma}_{\beta_{\mathsf{pub}}}}}$, which has no information about e or s. Note that there exist efficient (PPT) algorithms for sampling ellipsoid discrete Gaussians, e.g., [23, 25, 28, 33, 38, 41]. Since $\mathsf{d\text{-}RLWE}_s(n, q, D_{\mathbb{Z},s_{\mathsf{pk}}})$ is hard by hypothesis, $\mathsf{d\text{-}Reused\text{-}A\text{-}RLWE}(n, q, D_{\mathbb{Z},s_{\mathsf{enc}}}, D_{\mathbb{Z},s_{\mathsf{sm}}})$ is also hard by Cor. 5.12. Hence, we can prove SS by Thm. 5.15.

Let $x \leftarrow \chi_{\mathsf{Sim},t}(s, e, \zeta)$ for $t \le N$ and define $\mathbf{x} := \mathsf{vec}(x)$. We have $\|x\|_\infty \le \|\mathbf{x}\| \le \|\sqrt{\mathbf{\Sigma}}\|\sqrt{n}$ with overwhelming probability by Lem. 2.21. Thus, the correctness holds by Lem. 5.14. Note that $\|\sqrt{\mathbf{\Sigma}}\| \le \|\sqrt{\mathbf{\Sigma}}\|_F = (n(Ns_{\mathsf{sm}}^2 + s_{\mathsf{enc}}^2) + s_{\mathsf{enc}}^2\|\boldsymbol{\beta}_{\mathsf{pub}}\|^2)^{1/2}$ holds by Fact 5.3; thus, we can select $q = \mathrm{poly}(\lambda)$. □

We prove the deferred Lem. 5.17: We analyze the distribution of $\chi_{\mathsf{Sim},t}$ (defined in (16)) when we instantiate $\chi_{\mathsf{sm}} := D_{\mathbb{Z}^n,s_{\mathsf{sm}}}$ and $\chi_{\mathsf{pk}} := D_{\mathbb{Z}^n,s_{\mathsf{pk}}}$:

Lemma 5.17. *Let $t \le N$ be arbitrary. Let $s_{\mathsf{pk}}, s_{\mathsf{sm}} \ge \tilde{\eta}^+_\epsilon(\mathbb{Z}^n)$, $s_{\mathsf{enc}} \ge 2ns^2_{\mathsf{pk}}\eta^+_\epsilon(\mathbb{Z}^n)$, and define $\overline{s} := \sqrt{ts^2_{\mathsf{sm}} + s^2_{\mathsf{enc}}}$. Let $\mathbf{\Sigma}_\zeta$, $\mathbf{\Sigma}_e$ and $\mathbf{\Sigma}_s$ be coefficient Gram matrices of (non-zero) $\zeta, e, s \in \mathcal{R}$. Let $\chi_{\mathsf{pk}} := D_{\mathbb{Z}^n,s_{\mathsf{pk}}}$, $\chi_{\mathsf{enc}} := D_{\mathbb{Z}^n,s_{\mathsf{enc}}}$, and $\chi_{\mathsf{sm}} := D_{\mathbb{Z}^n,s_{\mathsf{sm}}}$. Then, $\chi_{\mathsf{Sim},t}$ defined in (16) satisfies*

$$\chi_{\mathsf{Sim},t}(s,e,\zeta) \approx_{\mathsf{s}} D_{\mathbb{Z}^n,\sqrt{\overline{s}^2\mathbf{I}_n + s^2_{\mathsf{enc}}(\mathbf{\Sigma}_\zeta+\mathbf{\Sigma}_e+\mathbf{\Sigma}_s)}}.$$

Proof. By (16) and Fact 5.2, we have $\chi_{\mathsf{Sim},t}(s,e,\zeta) = \{\sum_{i=1}^t \mathbf{e}^{\mathsf{sm}}_i + \mathbf{Z}\mathbf{r}_{\mathsf{aux}} - \mathbf{E}\mathbf{r} - \mathbf{S}\mathbf{e}_1 - \mathbf{e}_2\}$, where $\mathbf{Z}, \mathbf{E}, \mathbf{S}$ are the coefficient matrices of ζ, e, s and $\mathbf{e}^{\mathsf{sm}}_i, \mathbf{r}_{\mathsf{aux}}, \mathbf{r}, \mathbf{e}_1, \mathbf{e}_2$ are the coefficient vectors of $e^{\mathsf{sm}}_i, r_{\mathsf{aux}}, r, e_1, e_2$ defined in (16). We have $\overline{\mathbf{e}} := \sum_{i=1}^t \mathbf{e}^{\mathsf{sm}}_i - \mathbf{e}_2 \approx_{\mathsf{s}} D_{\mathbb{Z}^n,\overline{s}}$ by Lem. 2.15. We obtain $\mathbf{Z}\mathbf{r}_{\mathsf{aux}} = D_{\mathbf{Z}\mathbb{Z}^n,s_{\mathsf{enc}}\mathbf{Z}}$, $\mathbf{E}\mathbf{r} = D_{\mathbf{E}\mathbb{Z}^n,s_{\mathsf{enc}}\mathbf{E}}$ and $\mathbf{S}\mathbf{e}_1 = D_{\mathbf{S}\mathbb{Z}^n,s_{\mathsf{enc}}\mathbf{S}}$ by Lem. 2.16 and Fact 5.4. Hence, by Cor. 2.20,

$$\mathbf{Z}\mathbf{r}_{\mathsf{aux}} + \overline{\mathbf{e}} \approx_{\mathsf{s}} D_{\mathbf{Z}\mathbb{Z}^n,s_{\mathsf{enc}}\mathbf{Z}} + D_{\mathbb{Z}^n,\overline{s}} \approx_{\mathsf{s}} D_{\mathbb{Z}^n,\sqrt{s^2_{\mathsf{enc}}\mathbf{\Sigma}_\zeta+\overline{s}^2\mathbf{I}}} \tag{21}$$

holds since $\overline{s} \ge \eta^+_\epsilon(\mathbb{Z}^n)$ and $\mathbf{\Sigma}_3 := (s^{-2}_{\mathsf{enc}}\mathbf{\Sigma}^{-1}_\zeta + \overline{s}^{-2}\mathbf{I})^{-1}$ satisfies $\sqrt{\mathbf{\Sigma}_3} \ge \eta_\epsilon(\mathbf{Z}\mathbb{Z}^n)$ as follows: By Fact 2.14 and subsequent Fact 5.18, $\eta_\epsilon(\sqrt{\mathbf{\Sigma}_3}^{-1}\mathbf{Z}\mathbb{Z}^n)/\eta^+_\epsilon(\mathbb{Z}^n) \le \|\mathbf{Z}\|_{\mathrm{len}}\|\sqrt{\mathbf{\Sigma}_3}^{-1}\| \le \|\boldsymbol{\zeta}\|(s^{-2}_{\mathsf{enc}}\|\mathbf{Z}^{-1}\|^2 + \overline{s}^{-2})^{1/2} \le s_{\mathsf{pk}}\sqrt{n}(ns^2_{\mathsf{pk}}s^{-2}_{\mathsf{enc}} + \overline{s}^{-2})^{1/2} < \sqrt{2}ns^2_{\mathsf{pk}}/s_{\mathsf{enc}} \le 1/\eta^+_\epsilon(\mathbb{Z}^n)$ holds since we choose $s_{\mathsf{enc}} \ge 2ns^2_{\mathsf{pk}}\eta^+_\epsilon(\mathbb{Z}^n)$. Again by Cor. 2.20 and (21), we have

$$-\mathbf{E}\mathbf{r} + \mathbf{Z}\mathbf{r}_{\mathsf{aux}} + \overline{\mathbf{e}} \approx_{\mathsf{s}} D_{\mathbf{E}\mathbb{Z}^n,s_{\mathsf{enc}}\mathbf{E}} + D_{\mathbb{Z}^n,\sqrt{s^2_{\mathsf{enc}}\mathbf{\Sigma}_\zeta+\overline{s}^2\mathbf{I}}} \approx_{\mathsf{s}} D_{\mathbb{Z}^n,\sqrt{s^2_{\mathsf{enc}}(\mathbf{\Sigma}_e+\mathbf{\Sigma}_\zeta)+\overline{s}^2\mathbf{I}}}$$

since $\sqrt{\mathbf{\Sigma}_3} \ge \eta_\epsilon(\mathbf{Z}\mathbb{Z}^n) \ge \eta_\epsilon(\mathbb{Z}^n)$ and $\mathbf{\Sigma}_4 := (s^{-2}_{\mathsf{enc}}(\mathbf{\Sigma}^{-1}_e + \mathbf{\Sigma}^{-1}_\zeta) + \overline{s}^{-2}\mathbf{I})^{-1}$ satisfies $\sqrt{\mathbf{\Sigma}_4} \ge \eta_\epsilon(\mathbf{E}\mathbb{Z}^n)$: We have $\eta_\epsilon(\sqrt{\mathbf{\Sigma}_4}^{-1}\mathbf{E}\mathbb{Z}^n)/\eta^+_\epsilon(\mathbb{Z}^n) \le \|\mathbf{e}\|(s^{-2}_{\mathsf{enc}}(\|\mathbf{E}^{-1}\|^2 + \|\mathbf{Z}^{-1}\|^2) + \overline{s}^{-2})^{1/2} \le s_{\mathsf{pk}}\sqrt{n}\sqrt{2ns^2_{\mathsf{pk}}s^{-2}_{\mathsf{enc}} + \overline{s}^{-2}} < \sqrt{3}ns^2_{\mathsf{pk}}/s_{\mathsf{enc}} \le 1/\eta^+_\epsilon(\mathbb{Z}^n)$. Similarly, $\mathbf{S}\mathbf{e}_1 - \mathbf{E}\mathbf{r} + \mathbf{Z}\mathbf{r}_{\mathsf{aux}} + \overline{\mathbf{e}} \approx_{\mathsf{s}} D_{\mathbb{Z}^n,\sqrt{s^2_{\mathsf{enc}}(\mathbf{\Sigma}_s+\mathbf{\Sigma}_e+\mathbf{\Sigma}_\zeta)+\overline{s}^2\mathbf{I}}}$ also holds. □

We prove deferred Fact 5.18 to complete the proof:

Fact 5.18. *Let $a \in \mathcal{R}$ and define $\mathbf{a} := \mathsf{vec}(a)$ and $\mathbf{A} := \mathsf{mat}(a)$. If $a \sim D_{\mathbb{Z}^n,s_{\mathsf{pk}}}$ for $s_{\mathsf{pk}} \ge \eta^+_\epsilon(\mathbb{Z}^n)$, then $\|\mathbf{A}^{-1}\| \le s_{\mathsf{pk}}\sqrt{n}$ holds with overwhelming probability.*

Proof. $\|\mathbf{A}^{-1}\| \le \|\mathbf{A}\|_{\mathrm{len}} = \|\mathbf{a}\| \le s_{\mathsf{pk}}\sqrt{n}$ by Fact 5.3 and Lem. 2.22. □

Note that the above bound $\|\mathbf{A}^{-1}\| \le s_{\mathsf{pk}}\sqrt{n}$ is far from tight. We believe sharper bounds would be obtained by adapting [39, Thm. 1.7] or [44, Thm. 2.7.7] to $\mathbf{A}$, which we leave as a future work.

6 Conclusion and Future Works

In this paper, we propose efficient ThPKE schemes whose simulation-security are (directly) reduced from LWE or Ring-LWE with a polynomial modulus q.

We introduce a core technique called "error sharing" to prevent leakage of the norm $\|\mathbf{e}\|$ or the covariance of the error $\mathbf{\Sigma}_e$ (and secret $\mathbf{\Sigma}_s$) in the public key: In our schemes, the shares of a small error $\mathsf{err} := \boldsymbol{\zeta}$ are distributed with secret sharing to mask the partial decryptions in addition to the conventional smudging noise. Using this technique, we improved the ThPKE schemes proposed in [37] by eliminating the need to use "known-norm LWE" or "known-covariance Ring-LWE", which are nonstandard problems.

We believe our scheme can be extended to ThFHE by replacing the underlying PKE of ThPKE with FHE, and an efficient SS-ThFHE can be constructed from (Ring-)LWE with a polynomial modulus q. This implies that the applications of ThFHE can also be improved. For example, the round optimal MPC [5,22,24] and the universal thresholdizer [11] with simulation-security can be constructed from (Ring-)LWE with a polynomial modulus q. Additionally, the universal thresholdizer can be used to construct many threshold cryptosystems such as CCA-secure ThPKE, threshold signature, threshold PRF and threshold functional encryption. It is a future work to construct ThFHE from our ThPKE.

References

[1] Agrawal, S., Gentry, C., Halevi, S., Sahai, A.: Discrete Gaussian leftover hash lemma over infinite domains. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013. pp. 97–116. Springer (2013). https://doi.org/10.1007/978-3-642-42033-7_6

[2] Agrawal, S., Libert, B., Stehlé, D.: Fully secure functional encryption for inner products, from standard assumptions. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. pp. 333–362. Springer (2016). https://doi.org/10.1007/978-3-662-53015-3_12

[3] Alperin-Sheriff, J., Peikert, C.: Circular and KDM security for identity-based encryption. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) PKC 2012. pp. 334–352. Springer (2012). https://doi.org/10.1007/978-3-642-30057-8_20

[4] Asharov, G., Jain, A., López-Alt, A., Tromer, E., Vaikuntanathan, V., Wichs, D.: Multiparty computation with low communication, computation and interaction via threshold FHE. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. pp. 483–501. Springer (2012). https://doi.org/10.1007/978-3-642-29011-4_29

[5] Badrinarayanan, S., Jain, A., Manohar, N., Sahai, A.: Secure MPC: Laziness leads to GOD. In: Moriai, S., Wang, H. (eds.) ASIACRYPT 2020. pp. 120–150. Springer (2020). https://doi.org/10.1007/978-3-030-64840-4_5

[6] Bai, S., Lepoint, T., Roux-Langlois, A., Sakzad, A., Stehlé, D., Steinfeld, R.: Improved security proofs in lattice-based cryptography: Using the Rényi divergence rather than the statistical distance. J. Cryptol. **31**(2), 610–640 (2018). https://doi.org/10.1007/s00145-017-9265-9

[7] Bendlin, R., Damgård, I.: Threshold decryption and zero-knowledge proofs for lattice-based cryptosystems. In: Micciancio, D. (ed.) TCC 2010. pp. 201–218. Springer (2010). https://doi.org/10.1007/978-3-642-11799-2_13

[8] Boneh, D., Freeman, D.M.: Linearly homomorphic signatures over binary fields and new tools for lattice-based signatures. Cryptology ePrint Archive, Paper 2010/453 (2010), https://eprint.iacr.org/2010/453, full version of [9].

[9] Boneh, D., Freeman, D.M.: Linearly homomorphic signatures over binary fields and new tools for lattice-based signatures. In: Catalano, D., Fazio, N., Gennaro,

R., Nicolosi, A. (eds.) PKC 2011. pp. 1–16. Springer (2011). https://doi.org/10.1007/978-3-642-19379-8_1

[10] Boneh, D., Gennaro, R., Goldfeder, S., Jain, A., Kim, S., Rasmussen, P.M.R., Sahai, A.: Threshold cryptosystems from threshold fully homomorphic encryption. Cryptology ePrint Archive, Paper 2017/956 (2017), https://eprint.iacr.org/2017/956, (full version of [11])

[11] Boneh, D., Gennaro, R., Goldfeder, S., Jain, A., Kim, S., Rasmussen, P.M.R., Sahai, A.: Threshold cryptosystems from threshold fully homomorphic encryption. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018. pp. 565–596. Springer (2018). https://doi.org/10.1007/978-3-319-96884-1_19

[12] Boudgoust, K., Scholl, P.: Simple threshold (fully homomorphic) encryption from LWE with polynomial modulus. In: Guo, J., Steinfeld, R. (eds.) ASIACRYPT 2023. pp. 371–404. Springer (2023). https://doi.org/10.1007/978-981-99-8721-4_12

[13] Brakerski, Z., Döttling, N.: Hardness of LWE on general entropic distributions. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020. pp. 551–575. Springer (2020). https://doi.org/10.1007/978-3-030-45724-2_19

[14] Brakerski, Z., Gentry, C., Vaikuntanathan, V.: (Leveled) fully homomorphic encryption without bootstrapping. In: ITCS 2012. pp. 309–325. ACM (2012). https://doi.org/10.1145/2090236.2090262

[15] Brakerski, Z., Langlois, A., Peikert, C., Regev, O., Stehlé, D.: Classical hardness of learning with errors. In: STOC '13. p. 575–584. ACM (2013). https://doi.org/10.1145/2488608.2488680

[16] Brandão, L.T., Peralta, R.: NIST IR 8214C ipd: NIST first call for multi-party threshold schemes (initial public draft) (2023), https://doi.org/10.6028/NIST.IR.8214C.ipd

[17] Canetti, R.: Universally composable security: A new paradigm for cryptographic protocols. In: FOCS' 01. pp. 136–145 (2001). https://doi.org/10.1109/SFCS.2001.959888

[18] Cheon, J.H., Kim, A., Kim, M., Song, Y.: Homomorphic encryption for arithmetic of approximate numbers. In: Takagi, T., Peyrin, T. (eds.) ASIACRYPT 2017. pp. 409–437. Springer (2017). https://doi.org/10.1007/978-3-319-70694-8_15

[19] Chillotti, I., Gama, N., Georgieva, M., Izabachène, M.: TFHE: Fast fully homomorphic encryption over the torus. J. Cryptol. **33**(1), 34–91 (2020). https://doi.org/10.1007/s00145-019-09319-x

[20] Chowdhury, S., Sinha, S., Singh, A., Mishra, S., Chaudhary, C., Patranabis, S., Mukherjee, P., Chatterjee, A., Mukhopadhyay, D.: Efficient threshold FHE with application to real-time systems. ePrint 2022/1625 (2022), https://eprint.iacr.org/2022/1625

[21] Dahl, M., Demmler, D., El Kazdadi, S., Meyre, A., Orfila, J.B., Rotaru, D., Smart, N.P., Tap, S., Walter, M.: Noah's ark: Efficient threshold-FHE using noise flooding. In: WAHC '23. p. 35–46. ACM (2023). https://doi.org/10.1145/3605759.3625259

[22] Dov Gordon, S., Liu, F.H., Shi, E.: Constant-round MPC with fairness and guarantee of output delivery. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. pp. 63–82. Springer (2015). https://doi.org/10.1007/978-3-662-48000-7_4

[23] Ducas, L., Galbraith, S., Prest, T., Yu, Y.: Integral matrix Gram root and lattice Gaussian sampling without floats. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020. pp. 608–637. Springer (2020). https://doi.org/10.1007/978-3-030-45724-2_21

[24] Garg, S., Gentry, C., Halevi, S., Raykova, M.: Two-round secure MPC from indistinguishability obfuscation. In: Lindell, Y. (ed.) TCC 2014. pp. 74–94. Springer (2014). https://doi.org/10.1007/978-3-642-54242-8_4
[25] Genise, N., Micciancio, D.: Faster Gaussian sampling for trapdoor lattices with arbitrary modulus. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018. pp. 174–203. Springer (2018). https://doi.org/10.1007/978-3-319-78381-9_7
[26] Genise, N., Micciancio, D., Peikert, C., Walter, M.: Improved discrete Gaussian and subGaussian analysis for lattice cryptography. In: Kiayias, A., Kohlweiss, M., Wallden, P., Zikas, V. (eds.) PKC 2020. pp. 623–651. Springer (2020). https://doi.org/10.1007/978-3-030-45374-9_21
[27] Gentry, C.: Fully homomorphic encryption using ideal lattices. In: STOC '09. pp. 169–178. ACM (2009). https://doi.org/10.1145/1536414.1536440
[28] Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: STOC '08. p. 197–206. ACM (2008). https://doi.org/10.1145/1374376.1374407
[29] Katsumata, S., Yamada, S.: Partitioning via non-linear polynomial functions: More compact IBEs from ideal lattices and bilinear maps. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016. pp. 682–712. Springer (2016). https://doi.org/10.1007/978-3-662-53890-6_23
[30] Kiltz, E., Lyubashevsky, V., Schaffner, C.: A concrete treatment of Fiat-Shamir signatures in the quantum random-oracle model. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018. pp. 552–586. Springer (2018). https://doi.org/10.1007/978-3-319-78372-7_18
[31] Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. In: Gilbert, H. (ed.) EUROCRYPT 2010. pp. 1–23. Springer (2010). https://doi.org/10.1007/978-3-642-13190-5_1
[32] Micciancio, D., Mol, P.: Pseudorandom knapsacks and the sample complexity of LWE search-to-decision reductions. In: Rogaway, P. (ed.) CRYPTO 2011. pp. 465–484. Springer (2011). https://doi.org/10.1007/978-3-642-22792-9_26
[33] Micciancio, D., Peikert, C.: Trapdoors for lattices: Simpler, tighter, faster, smaller. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. pp. 700–718. Springer (2012). https://doi.org/10.1007/978-3-642-29011-4_41
[34] Micciancio, D., Peikert, C.: Hardness of SIS and LWE with small parameters. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013. pp. 21–39. Springer (2013). https://doi.org/10.1007/978-3-642-40041-4_2
[35] Micciancio, D., Regev, O.: Worst-case to average-case reductions based on Gaussian measures. In: FOCS '04. pp. 372–381 (2004). https://doi.org/10.1109/FOCS.2004.72
[36] Micciancio, D., Regev, O.: Worst-case to average-case reductions based on Gaussian measures. SIAM J. Comput. **37**(1), 267–302 (2007). https://doi.org/10.1137/S0097539705447360, full version of [35]
[37] Micciancio, D., Suhl, A.: Simulation-secure threshold PKE from LWE with polynomial modulus. ePrint 2023/1728 (2023), https://eprint.iacr.org/2023/1728
[38] Micciancio, D., Walter, M.: Gaussian sampling over the integers: Efficient, generic, constant-time. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017. pp. 455–485. Springer (2017). https://doi.org/10.1007/978-3-319-63715-0_16
[39] Nguyen, H.H., Vu, V.H.: Normal vector of a random hyperplane. International Mathematics Research Notices **2018**(6), 1754–1778 (2016). https://doi.org/10.1093/imrn/rnw273

[40] O'Neill, A., Peikert, C., Waters, B.: Bi-deniable public-key encryption. In: Rogaway, P. (ed.) CRYPTO 2011. pp. 525–542. Springer (2011). https://doi.org/10.1007/978-3-642-22792-9_30

[41] Peikert, C.: An efficient and parallel Gaussian sampler for lattices. In: Rabin, T. (ed.) CRYPTO 2010. pp. 80–97. Springer (2010). https://doi.org/10.1007/978-3-642-14623-7_5

[42] Prest, T.: Sharper bounds in lattice-based cryptography using the Rényi divergence. In: Takagi, T., Peyrin, T. (eds.) ASIACRYPT 2017. pp. 347–374. Springer (2017). https://doi.org/10.1007/978-3-319-70694-8_13

[43] Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. J. ACM **56**(6) (2009). https://doi.org/10.1145/1568318.1568324

[44] Terence, T.: Topics in random matrix theory. Graduate Studies in Mathematics **132** (2012). https://doi.org/10.1090/gsm/132