Tighter Security for Efficient Lattice Cryptography via the Rényi Divergence of Optimized Orders*

Katsuyuki Takashima and Atsushi Takayasu**

Mitsubishi Electric, Japan
Takashima.Katsuyuki@aj.MitsubishiElectric.co.jp
The University of Tokyo, Japan
a-takayasu@it.k.u-tokyo.ac.jp

Abstract. In security proofs of lattice based cryptography, bounding the closeness of two probability distributions is an important procedure. To measure the closeness, the Rényi divergence has been used instead of the classical statistical distance. Recent results have shown that the Rényi divergence offers security reductions with better parameters, e.g. smaller deviations for discrete Gaussian distributions. However, since previous analyses used a fixed order Rényi divergence, i.e., order two, they lost tightness of reductions. To overcome the deficiency, we *adaptively* optimize the orders based on the advantages of the adversary for several lattice-based schemes. The optimizations enable us to prove the security with both improved efficiency and tighter reductions. Indeed, our analysis offers security reductions with smaller parameters than the statistical distance based analysis and the reductions are tighter than those of previous Rényi divergence based analyses. As applications, we show tighter security reductions for sampling discrete Gaussian distributions with smaller precomputed tables for Bimodal Lattice Signature Scheme (BLISS), and the variants of learning with errors (LWE) problem and the small integer solution (SIS) problem called k-LWE and k-SIS, respectively.

Keywords: lattice based cryptography, tight reduction, Rényi divergence, sampling discrete Gaussian, BLISS, LWE, SIS

1 Introduction

Background. The security of current cryptographic schemes relies on the hardness of the factorization/RSA problem and the (elliptic curve) discrete logarithm problem. Solving these problems becomes feasible when quantum computers are developed. Although quantum computers are not currently available, it is worthwhile to research next candidate cryptographic constructions. Lattice based cryptographic schemes have become central candidates for the post-quantum world. While some papers have focused on theoretical analyses, there are several papers that discuss practical implementations and the appropriate parameter selections [LP10, CN11, DDLL13, PDG14]. These works reveal some drawbacks in the efficiency of the lattice based schemes. For example, one of the deficiencies is the discrete Gaussian sampling with large deviations.

In security proofs of lattice based cryptography, bounding the closeness of two probability distributions (e.g., zero centered and non-zero centered discrete Gaussian distributions) is an important procedure. To measure the closeness, the classical statistical distance (SD) is naturally used. However, several papers [LPR13, LSS14, LPSS14, BLL+15] used the Rényi divergence (RD) [Ren61, EH12] instead of the SD. These works show that the RD offers better security reductions for

* Date: 24 November, 2015. This paper is the full version of [TT15].

** The second author is supported by a JSPS Research Fellowship for Young Scientists. This work was supported by Grant-in-Aid for JSPS Fellows Grant Number 26·8237.

lattice based cryptographic schemes. More concretely, the RD enables security reductions with better parameters (e.g. smaller deviations for discrete Gaussian distributions) that cannot be handled by the SD.

In short, the SD denotes differences of two probability distributions whereas the RD denotes the ratios of the distributions; hence, some properties of the SD expressed by additions are replaced by multiplications in the RD. For the SD based security proofs to be relevant, the quantity of the SD has to be smaller than a probability for an adversary to break the scheme. To satisfy the restriction, inefficient parameters (e.g. large deviations for discrete Gaussian distributions) have to be used. On the other hand, for the RD based security proofs to be relevant, the quantity of the RD can be permitted to larger bounds, e.g. the logarithm of the probability for an adversary to break the scheme. In some cases, the latter requirement (for the RD) is weaker than the former requirement (for the SD). Indeed, there are several reports confirming that the RD based analysis offers a significant parameter savings.

However, there is one disadvantage of the RD based analysis that cannot be disregarded; RD based security reductions lose the tightness. If the quantity of the SD is significantly small, the SD based security reduction becomes tight, and probabilities that an adversary will break the real and simulated schemes are almost identical. However, even if the value of the RD is significantly small, the probability that an adversary will break the real scheme is at least larger than the square root of the probability that an adversary will break the simulated scheme. Therefore, for the probability to break the real scheme to be sufficiently small, RD based analysis requires the probability to break the simulated scheme to be smaller than the SD based analysis. As a result, the RD based analysis sacrifices tightness to achieve the parameter saving compared with the SD based analysis.

Previous Results of RD Based Security Proofs. Suppose instances of a real cryptographic scheme are sampled from one distribution and instances of a simulated scheme are sampled from another distribution; the former (resp. latter) distribution is defined as the *real* (resp. *ideal*) distribution. If the two distributions are statistically close, then an adversary that breaks the real scheme is also an adversary that breaks the simulated scheme. Then, if the simulated scheme is assumed to be secure, the real scheme is also secure.

The Bimodal Lattice Signature Scheme (BLISS) was proposed by Ducas et al. [DDLL13] (Crypto 2013), and its efficiency is comparable to RSA and ECDSA. For signing a message, about several hundreds independent integers should be sampled from one-dimensional discrete Gaussian distributions. To implement BLISS signature scheme over constrained devices, Ducas et al. also proposed an efficient algorithm for the discrete Gaussian sampling. First, to sample an integer from a discrete Gaussian distribution, several integers are sampled independently from Bernoulli distributions. Using these Bernoulli random integers and a rejection sampling technique, a discrete Gaussian distribution is sampleable. Sampling from Bernoulli distributions is efficiently performed with a precomputed table that stores the probabilities. Since the probabilities are not rational, each stored value is truncated with some precisions. Required precisions to maintain the security of BLISS are analyzed by measuring the statistical closeness between truncated Bernoulli distributions (*real distributions*) and untruncated Bernoulli distributions (*ideal distributions*). Although two distributions become close when large precisions are used, the scheme is inefficient since the table storage becomes large. Ducas et al. analyzed the precisions using the SD, and Pöppelmann et al. [PDG14] (CHES 2014) gave an alternative analysis using the Kullback-Leibler divergence (KLD). The KLD based analysis reduces the required precisions that lead to reduced table storage.

Table 1. Comparison of required precisions p and success probabilities ε for adversaries to break BLISS signatures where each Bernoulli variable is sampled with truncated probabilities (*real distribution*). Each signature is generated by sampling $2n$ discrete Gaussian variables, and each discrete Gaussian variable is produced by sampling ℓ Bernoulli variables. Adversaries are allowed q_s signing queries and break BLISS signatures with probabilities ε' where each Bernoulli variable is sampled with untruncated probabilities (*ideal distribution*). In the last column for ε, $\approx$ is defined as the approximate equivalence when $-\ln(\varepsilon') \gg \ell \cdot n \cdot q_s \cdot 2^{-2p}$, which holds for practical numerical examples given in the right parameter of Table 4.

disc. Gauss. Sampling	stat. measure	precision p	ε
[DDLL13]	SD	$\log(\ell \cdot 2n \cdot q_s/\varepsilon)$	$\leq \varepsilon' + \ell \cdot 2n \cdot q_s \cdot 2^{-p-1} \approx \varepsilon'$
[PDG14]	KLD	$\log(\ell \cdot 2n \cdot q_s/\varepsilon^2)/2 + 1/2$	$\leq \varepsilon' + \sqrt{\ell \cdot 2n \cdot q_s \cdot 2^{-2p}} \approx \varepsilon'$
[BLL+15]	RD, $\alpha = +\infty$	$\log(\ell \cdot 2n \cdot q_s)$	$\leq \varepsilon' \cdot (1 + 2^{-p})^{\ell \cdot 2n \cdot q_s} \approx \varepsilon'$
[BLL+15]	RD, $\alpha = 2$	$\log(\ell \cdot 2n \cdot q_s)/2$	$\leq \varepsilon'^{1/2} \cdot (1 + 2^{-2p})^{\ell \cdot 2n \cdot q_s/2} \approx \varepsilon'^{1/2}$
Proposed	RD, $\alpha = \sqrt{\frac{-\ln(\varepsilon')}{\ell \cdot n \cdot q_s \cdot 2^{-2p}}}$	$\log(-\ln(\varepsilon') \cdot \ell \cdot n \cdot q_s)/2$	$\leq \exp\left(-\left(\sqrt{-\ln(\varepsilon')} - \sqrt{\ell \cdot n \cdot q_s \cdot 2^{-2p}}\right)^2\right) \approx \varepsilon'$

Recently, Bai et al. [BLL+15] (Asiacrypt 2015) further improved the analysis based on the RD, however the reduction was no longer tight.

Boneh and Freeman [BF11] (PKC 2011) introduced the k-small integer solution (k-SIS) problem that is a variant of the small integer solution (SIS) problem [MR07]. In short, the k-SIS problem is defined as follows: given k hint vectors that are solutions to the original SIS problem and the goal of the problem is to compute the other SIS solution that is orthogonal to the k hint vectors. Based on the hardness of the k-SIS problem, Boneh and Freeman constructed lattice based linearly homomorphic signatures, k-time signatures, and proved that the k time GPV signature scheme [GPV08] is secure in the standard model. However, for the k-SIS problem to be no easier than the SIS problem, the solution bound of the SIS problem becomes exponential of k; hence, the k-SIS problem is as hard as the worst case standard lattice problems only when $k = O(1)$. Ling et al. [LPSS14] (Crypto 2014) introduced the dual problem, k-learning with errors (k-LWE) problem that is a variant of the learning with errors (LWE) problem [Reg05]. Based on the hardness of the k-LWE problem, Ling et al. proposed the first algebraic construction of a traitor tracing scheme from lattices. Moreover, Ling et al. considered more efficient reductions than [BF11]. Their reduction enables the value of k to be a polynomial of the lattice dimension and the technique used in the reduction is applicable to the k-SIS problem. Specifically, Ling et al.'s reduction consists of two subreductions. In the first subreduction, LWE is reduced to k-LWE where k hint vectors are sampled from non-zero centered discrete Gaussian distributions (*real distributions*). In the second subreduction, the former k-LWE is reduced to k-LWE where k hint vectors are sampled from zero centered discrete Gaussian distributions (*ideal distributions*). To bound the closeness of two distributions, the RD is used. Although the analyses can handle smaller Gaussian deviations than the SD based analysis, the reduction is not tight.

Our Contributions. In this paper, we show improved security reductions for several lattice based cryptographic schemes. Our analysis offers security reductions with *smaller parameters* than the SD and KLD based analyses and the reductions are *tighter* than those of previous RD based analyses. In particular, when we analyze specific parameter selections, the tightness improves significantly. Our results are as follows:

Table 2. Comparison of Gaussian deviations of hint vectors $\sigma_{m+k}(S)$ and success probabilities ε for adversaries to solve LWE. The quantity of γ has a negative correlation with standard deviations of discrete Gaussian distributions. Adversaries $\mathcal{A}$ solve k-LWE with advantage ε'. λ denotes the security parameter and k denotes the number of hint vectors. In the last column for ε, $\approx$ is defined as the approximate equivalence when $-\ln(\varepsilon') \gg \kappa\gamma$.

LWE to k-LWE reduction	stat. measure	$\sigma_{m+k}(S)$	ε
	SD	2^λ	$\leq \varepsilon' + \mathrm{negl}(\lambda) \approx \varepsilon'$
[LPSS14]	RD, $\alpha = 2$	$poly(\lambda)$	$\leq \exp\left(\ln\left(\varepsilon'\right)/3 + 2k\gamma/3\right) \approx \varepsilon'^{1/3}$
Proposed	RD,$\alpha = \left(1 + \sqrt{-1 - \frac{2\ln(\varepsilon')}{k\gamma}}\right)/2$	$poly(\lambda)$	$\leq \exp\left(\ln\left(\varepsilon'\right)/2 + k\gamma\sqrt{-1 - \frac{2\ln(\varepsilon')}{k\gamma}}/2\right) \approx \varepsilon'^{1/2}$

Table 3. Comparison of Gaussian deviations of hint vectors $\sigma_{m+k}(S)$ and success probabilities ε for adversaries to solve SIS. The quantity of γ has a negative correlation with standard deviations of discrete Gaussian distributions. Adversaries solve k-SIS with advantage ε'. λ denotes the security parameter and k denotes the number of hint vectors. In the last column for ε, $\approx$ is defined as the approximate equivalence when $-\ln(\varepsilon') \gg \kappa\gamma$.

SIS to k-SIS reduction	stat. measure	$\sigma_{m+k}(S)$	ε
	SD	2^λ	$\leq \varepsilon' + \mathrm{negl}(n) \approx \varepsilon'$
[LPSS14]	RD, $\alpha = 2$	$poly(\lambda)$	$\leq \exp\left(\ln\left(\varepsilon'\right)/2 + k\gamma\right) \approx \varepsilon'^{1/2}$
Proposed	RD, $\alpha = \sqrt{-\ln(\varepsilon')/(k\gamma)}$	$poly(\lambda)$	$\leq \exp\left(-\left(\sqrt{-\ln(\varepsilon')} - \sqrt{k\gamma}\right)^2\right) \approx \varepsilon'$

- Sampling discrete Gaussian distributions for the BLISS signature scheme (Theorem 1 in Section 3) is achieved with *both* reduced table storages and tight reductions. In particular, our analysis shows that the sampling can be performed with a 1276 bits table for BLISS-I scheme with 128 bit security. Table 1 compares the required precisions p (affecting table storages), and the probabilities ε' (representing tightness) for an adversary to break the BLISS signature scheme with idealized distributions. Our reduction is as tight as the SD [DDLL13], KLD [PDG14], and RD of order $+\infty$ [BLL+15] based analyses with reduced table storages. Although our table requires slightly larger storage than that of RD of order 2 based analysis [BLL+15], the reduction is tighter. See Table 4 in Section 3 for detailed comparisons.
- LWE to k-LWE reduction (Theorem 2 in Section 4) is achieved with *both* small Gaussian deviations for sampling hint vectors and tighter reductions. Table 2 compares the Gaussian deviations $\sigma_{m+k}(S)$, and the probabilities ε' (that represent the tightness) for an adversary to solve k-LWE. Our reduction is as tight as the SD based analysis with smaller Gaussian deviations, and the deviations are as small as the previous RD based analysis [LPSS14] with tighter reductions.
- SIS to k-SIS reduction (Theorem 4 in Section 5) is achieved with *both* small Gaussian deviations for sampling hint vectors and tighter reductions. Table 3 compares the Gaussian deviations $\sigma_{m+k}(S)$, and the probabilities ε' (that represent the tightness) for an adversary to solve k-SIS. Our reduction is as tight as the SD based analysis with smaller Gaussian deviations, and the deviations are as small as the previous RD based analysis with tighter reductions.

Our improved results are obtained with the RD as previous works [BLL+15, LPSS14]. In previous RD based analyses, the order was fixed to $\alpha = 2$. However, we *adaptively* optimize the order based on the scheme parameters and probabilities for an adversary to break the simulated scheme. In Tables 1–3, ε (resp. ε') denotes the advantage for an adversary to break the real (resp. simulated)

scheme. As the tables show, the RD based analyses (including previous works) offer security reductions with smaller parameters (p for Table 1 and $\sigma_{m+k}(S)$ for Tables 2 and 3) than the SD based analyses. Furthermore, our optimizations of the order offer tighter reductions than previous RD based analyses with fixed orders. Briefly speaking, although upper bounds of ε for search problems (resp. distinguishing problems) are at least larger than $\varepsilon'^{1/2}$ (resp. $\varepsilon'^{1/3}$) when the order is fixed to $\alpha = 2$, our improvements offer tighter upper bounds that are almost ε' (resp. $\varepsilon'^{1/2}$). For appropriate choices of parameters, our results offer almost the same tightness as the SD based analyses. Therefore, efficient parameters and tight reductions are compatible in our improved analyses.

Adaptive Optimization of α. We briefly summarize the point of our improvements; the *adaptive* optimization of the order α. Let P and P' be two computing problems where the problem P (resp. P') is defined as follows: given $X = \{x_i : x_i \leftarrow \Phi\}_{i=1,\ldots,k}$ (resp. $X' = \{x'_i : x'_i \leftarrow \Phi'\}_{i=1,\ldots,k}$) and the goal of the problem is to compute $f(X)$ (resp. $f(X')$). In cryptographic security proofs, P (resp. P') can be viewed as the real (resp. simulated) cryptographic scheme, and Φ (resp. Φ') is the *real* (resp. *ideal*) distribution. Let γ be some quantity (that do not depend on α) that bounds the RD between the real distribution Φ and the ideal distribution Φ' such that $R_\alpha(\Phi\|\Phi') \leq \exp(\alpha \cdot \gamma)$. Although there are no assurance for the upper bound of $R_\alpha(\Phi\|\Phi')$ to be $O(\exp(\alpha))$ for arbitrary distributions Φ and Φ', it holds for the distributions that we study in this paper. By the definition and the properties of the RD, if there is an adversary $\mathcal{A}$ against the problem P with run-time T and advantage ε, then $\mathcal{A}$ is also an adversary against the problem P' with run-time $T' = T$ and advantage ε' where

$$\varepsilon \leq \left(\varepsilon' \cdot R_\alpha(\Phi\|\Phi')^k\right)^{\frac{\alpha-1}{\alpha}} \leq \exp\left(\frac{\alpha-1}{\alpha} \cdot \ln(\varepsilon') + (\alpha-1) \cdot k\gamma\right) \tag{1}$$

where the second inequality is obtained from the fact $R_\alpha(\Phi\|\Phi') \leq \exp(\alpha \cdot \gamma)$, and k is the number of samples. We say that the reduction is tight when the right hand side of the inequality (1) is approximately equivalent to ε', i.e., $\approx \varepsilon'$. Since the number of samples k (resp. the quantity γ) relate to cryptographic security or functionality, e.g., the number of signing queries in BLISS signatures, (resp. cryptographic efficiency, e.g., table storage size for sampling a discrete Gaussian distributions for BLISS signatures), we try to handle as large k and γ as possible. Then, the goal of our analysis is to prove the cryptographic security with both tight reductions and small parameters. When the order is fixed to $\alpha = 2$ as previous works, the inequality (1) becomes $\varepsilon \leq \exp(\ln(\varepsilon')/2 + k\gamma)$; hence, even if k and γ are small, the upper bound of ε becomes larger than $\varepsilon'^{1/2}$ and the reduction is not tight. This is the disadvantage of previous RD based analyses that always lose the tightness.

To overcome the issue, we *adaptively* optimize the order α to enable the reduction to be tighter. First, we analyze the inequality (1) with a general $\alpha \in (1, +\infty]$. For the fixed analysis with $\alpha = 2$, the tightness is lost by the existence of the exponent of ε', $\frac{\alpha-1}{\alpha}$. If a larger α is used, the exponent becomes close to 1; therefore, the reduction is expected to be tighter. However, an infinitely large α cannot be used since $R_\alpha(\Phi\|\Phi')$ becomes exponentially large, which results in a loss of the tightness. Hence, we optimize the order α to minimize the right hand side of the inequality (1). The right hand side is bounded below by $\exp\left(\ln(\varepsilon') - k\gamma + (-\ln(\varepsilon')/\alpha + \alpha \cdot k\gamma)\right) \geq \exp\left(\ln(\varepsilon') - k\gamma + 2\sqrt{-\ln(\varepsilon') \cdot k\gamma}\right)$ by the inequality of the arithmetic mean and geometric mean, where the equality holds if and only if $-\ln(\varepsilon')/\alpha = \alpha \cdot k\gamma$, i.e., $\alpha = \sqrt{-\ln(\varepsilon')/(k\gamma)}$. We then set

the order $\alpha = \sqrt{-\ln(\varepsilon')/(k\gamma)}$, and the inequality (1) becomes

$$\varepsilon \leq \exp\left(\ln(\varepsilon') - k\gamma + 2\sqrt{-\ln(\varepsilon') \cdot k\gamma}\right) = \exp\left(-\left(\sqrt{-\ln(\varepsilon')} - \sqrt{k\gamma}\right)^2\right). \tag{2}$$

The right hand side of the inequality (2) is always smaller than that of the inequality (1) with fixed $\alpha = 2$. Hence, our optimization always offers a tighter reduction than previous analyses [BLL+15, LPSS14]. Since we only consider the order $\alpha \in (1, +\infty]$, it leads to $\alpha = \sqrt{-\ln(\varepsilon')/(k\gamma)} > 1$, i.e., $-\ln(\varepsilon') > k\gamma$. Moreover, when $-\ln(\varepsilon') \gg k\gamma$, the right hand side of the inequality (2) is approximately equivalent to ε'; that is, the ideal P' to the real P reduction is almost tight.

The above analysis captures security reductions for computing problems, a security proof for discrete Gaussian sampling and SIS to k-SIS reduction in our results. Although the result of the LWE to k-LWE reduction, which are distinguishing problems, does not follow the inequality (1), the spirit of the improvement is the same.

2 Preliminaries

Notation. Let $\ln(x)$ (resp. $\log(x)$) denote the natural logarithm (resp. the base 2 logarithm) of x. Let $\mathbb{T}$ denote the additive group $\mathbb{R}/\mathbb{Z}$. For an integer q, we let $\mathbb{Z}_q$ denote the ring of integers modulo q. Vectors are denoted in bold and are column representations. For $\boldsymbol{b} \in \mathbb{R}^n$, we let $\|\boldsymbol{b}\|$ denote its Euclidean norm. We let $\langle \cdot, \cdot \rangle$ denote the canonical inner product. If A is a matrix, its entries are denote by a_{ij}. For two matrices A and B of compatible dimensions, we let $(A|B)$ (resp. $(A\|B)$) denote the horizontal (resp. vertical) concatenations of A and B. For $A \in \mathbb{Z}_q^{m \times n}$, we define $\mathrm{Im}(A) = \{A\boldsymbol{s} : \boldsymbol{s} \in \mathbb{Z}_q^n\} \subseteq \mathbb{Z}_q^m$. For $X \subseteq \mathbb{Z}_q^m$, we let $\mathrm{Span}(X)$ denote the set of all linear combinations of elements of X. We let $X^\perp$ denote the linear subspace $\{\boldsymbol{b} \in \mathbb{Z}_q^m : \forall \boldsymbol{c} \in X, \langle \boldsymbol{b}, \boldsymbol{c} \rangle = 0\}$. For a matrix $S \in \mathbb{Z}^{m \times n}$, we let $\|S\|$ denote the norm of its largest column. The smallest (resp. largest) singular value of S is denoted by $\sigma_n(S) = \inf(\|S\boldsymbol{u}\|)$ (resp. $\sigma_1(S) = \sup(\|S\boldsymbol{u}\|)$) where $\boldsymbol{u} \in \mathbb{R}^n$ and $\|\boldsymbol{u}\| = 1$.

If D is a probability distribution, we let $\mathrm{Supp}(D) = \{x : D(x) \neq 0\}$ denote its support. The uniform distribution on a finite set X is denoted by $U(X)$. The statistical distance (SD) between two distributions D_1 and D_2 over a countable support X is given by $\Delta(D_1, D_2) = \frac{1}{2}\sum_{x \in X} |D_1(x) - D_2(x)|$. For a function $f : X \to \mathbb{R}$ over a countable domain X, we let $f(X) = \sum_{x \in X} f(x)$. Let ν_β denote the one-dimensional Gaussian distribution on $\mathbb{T}$ with center 0 and standard deviation β.

Lattices and Discrete Gaussian Distributions. Lattice Λ is an additive discrete subgroup of $\mathbb{R}^n$. An n-dimensional lattice $\Lambda \subseteq \mathbb{R}^n$ is the set of all integer linear combinations $\sum_{j=1}^k c_j \boldsymbol{b}_j$ where $c_j \in \mathbb{Z}$ of some linearly independent vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k \in \mathbb{R}^n$ for some $k \leq n$. The rank of Λ is k. The determinant $\det(\Lambda)$ is defined by $\sqrt{\det(B^T B)}$, where $B = (\boldsymbol{b}_i)_i$ is any such basis of Λ. For a matrix $A \in \mathbb{Z}_q^{m \times n}$, define $\Lambda^\perp(A) = \{\boldsymbol{x} \in \mathbb{Z}^m : \boldsymbol{x}^T \cdot A = 0 \mod q\}$. The dual Λ^* of a lattice Λ is defined by $\Lambda^* = \{x \in \mathbb{R}^n : \forall y \in \Lambda, \langle x, y \rangle \in \mathbb{Z}\}$.

For a rank-n matrix $S \in \mathbb{R}^{m \times n}$ and a vector $\boldsymbol{c} \in \mathbb{R}^n$, the ellipsoid discrete Gaussian distribution with parameter S and center $\boldsymbol{c}$ is defined as follows: $\forall \boldsymbol{x} \in \mathbb{R}^n, \rho_{S,\boldsymbol{c}}(x) = \exp\left(-\pi(\boldsymbol{x} - \boldsymbol{c})^T \left(S^T S\right)^{-1} (\boldsymbol{x} - \boldsymbol{c})\right)$. Note that $\rho_{S,\boldsymbol{c}}(x) = \exp(-\pi\|(S^T)^\dagger(\boldsymbol{x} - \boldsymbol{c})\|^2)$, where $X^\dagger$ denotes the pseudo-inverse of X. The ellipsoid discrete Gaussian distribution over a coset $\Lambda + \boldsymbol{z}$ of a lattice Λ, with parameter S and center $\boldsymbol{c}$ is defined as follows: $\forall \boldsymbol{x} \in \Lambda + \boldsymbol{z}, D_{\Lambda+\boldsymbol{z},S,\boldsymbol{c}}(\boldsymbol{x}) = \rho_{S,\boldsymbol{c}}(\boldsymbol{x})/\rho_{S,\boldsymbol{c}}(\Lambda)$. For $S = sI_m$, we write $\rho_{s,\boldsymbol{c}}$ and $D_{\Lambda+\boldsymbol{z},s,\boldsymbol{c}}$. When $\boldsymbol{c} = 0$, the subscript $\boldsymbol{c}$ is omitted.

Smoothing Parameter. The smoothing parameter [MR07] $\eta_\varepsilon(\Lambda)$ of an n-dimensional lattice Λ for real $\varepsilon > 0$ is defined as the smallest s such that $\rho_{1/s}(\Lambda^* \setminus \{0\}) \leq \varepsilon$. When the deviation of the discrete Gaussian distribution is larger than the smoothing parameter, the following results are known.

Lemma 1 (Lemma 2.5 of [LSS14]) *Let Λ be an n-dimensional lattice and $\varepsilon \in (0,1)$. Then for any $\boldsymbol{c} \in \mathbb{R}^n$ and $s \geq \eta_\varepsilon(\Lambda)$ we have $\rho_{s,\boldsymbol{c}}(\Lambda) \in [1-\varepsilon, 1+\varepsilon] \cdot \det(\Lambda)^{-1}$.*

Lemma 2 (Lemma 3 of [AGHS13]) *For a rank-n lattice Λ, a constant $0 < \varepsilon < 1$, a vector $\boldsymbol{c}$ and a matrix S with $\sigma_n(S) \geq \eta_\varepsilon(\Lambda)$, if $\boldsymbol{x}$ is sampled from $D_{\Lambda,S,\boldsymbol{c}}$ then $\|\boldsymbol{x}\| \leq \sigma_1(S)\sqrt{n}$ with probability $\leq \frac{1+\varepsilon}{1-\varepsilon} \cdot 2^{-n}$.*

Lemma 3 (Lemma 1 of [LPSS14]) *Let q be a prime, m and n be integers with $m \geq 2n$ and $\varepsilon > 0$. Then $\eta_\varepsilon(\Lambda^\perp(A)) \leq 4q^{n/m}\sqrt{\log(2m(1+1/\varepsilon))/\pi}$, for all except a fraction $2^{-\Omega(n)}$ of $A \in \mathbb{Z}_q^{m \times n}$.*

Rényi Divergence. For any two discrete probability distributions P and Q such that $\mathrm{Supp}(P) \subseteq \mathrm{Supp}(Q)$ and $\alpha \in (1, \infty]$, we define the Rényi divergence (RD) of order α by

$$R_\alpha(P\|Q) = \left(\sum_{x \in \mathrm{Supp}(P)} \frac{P(x)^\alpha}{Q(x)^{\alpha-1}} \right)^{\frac{1}{\alpha-1}} \text{ for } \alpha \in (1,\infty), \quad R_\infty(P\|Q) = \max_{x \in \mathrm{Supp}(P)} \frac{P(x)}{Q(x)}.$$

We summarize the basic properties of the RD that we use in this paper.

Lemma 4 (Lemma 4.1 of [LSS14]) *Let P_1, P_2, P_3 and Q_1 and Q_2 denote discrete distributions on a domain X. Let $\alpha \in (1, +\infty]$. Then the following properties hold:*

- *Log. Positivity: $R_\alpha(P_1\|Q_1) \geq R_\alpha(P_1\|P_1) = 1$.*
- *Data Processing Inequality: $R_\alpha\left(P_1^f \| Q_1^f\right) \leq R_\alpha(P_1\|Q_1)$ for any function f, where P_1^f (resp. Q_1^f) denotes the distribution of $f(y)$ induced by sampling $y \leftarrow P_1$ (resp. $y \leftarrow Q_1$).*
- *Multiplicativity: Let P and Q denote any two distributions of a pair of random variables (Y_1, Y_2) on $X \times X$. For $i \in \{1,2\}$, let P_i (resp. Q_i) denote the marginal distribution of Y_i under P (resp. Q), and $P_{(2|1)}(\cdot|y_1)$ (resp. $Q_{(2|1)}(\cdot|y_1)$) denote the conditional distribution of Y_2 given that $Y_1 = y_1$. Then we have $R_\alpha(P\|Q) = R_\alpha(P_1\|Q_1) \cdot R_\alpha(P_2\|Q_2)$ if Y_1 and Y_2 are independent, and $R_\alpha(P\|Q) \leq R_\infty(P_1\|Q_1) \cdot \max_{y_1 \in X} R_\alpha(P_{2|1}(\cdot|y_1)\|Q_{2|1}(\cdot|y_1))$.*
- *Weak Triangle Inequality: We have $R_\alpha(P_1\|P_3) \leq R_\alpha(P_1\|P_2) \cdot R_\infty(P_2\|P_3)$, and $R_\alpha(P_1\|P_3) \leq R_\infty(P_1\|P_2)^{\alpha/(\alpha-1)} \cdot R_\alpha(P_2\|P_3)$.*
- *R_∞ Triangle Inequality: If $R_\infty(P_1\|P_2)$ and $R_\infty(P_2\|P_3)$ are defined, then $R_\infty(P_1\|P_3) \leq R_\infty(P_1\|P_2) \cdot R_\infty(P_2\|P_3)$.*
- *Probability Preservation: Let $E \subseteq X$ be an arbitrary event. Then $Q_1(E) \geq P_1(E)^{\alpha/(\alpha-1)} / R_\alpha(P_1\|Q_1)$.*

The divergence R_1 is the exponential of the KLD, $R_1(P\|Q) = \exp\left(\sum_{x \in \mathrm{Supp}(P)} P(x) \log \frac{P(x)}{Q(x)}\right)$. The probability preservation property of the KLD can be written as $Q(E) \geq P(E) - \sqrt{\ln R_1(P\|Q)/2}$.

In this paper, we use the following result[1] that is essential for our improvements in Sections 4 and 5.

[1] In the proceedings version of [BLL+15], Bai et al. showed a slightly better bound for our Lemma 5. However, we do not know the proof, so we prove the lemma in this paper. See Section A.

Lemma 5 *For any n-dimensional lattice $\Lambda \subseteq \mathbb{R}^n$ and inversible rank-n matrix $S \in \mathbb{R}^{m\times n}$ for $m \geq n$, set $P = D_{\Lambda,S,\boldsymbol{c}}$ and $Q = D_{\Lambda,S,\boldsymbol{c}'}$ for some fixed $\boldsymbol{c}, \boldsymbol{c}' \in \mathbb{R}^n$. If $\boldsymbol{c}, \boldsymbol{c}' \in \Lambda$, let $\varepsilon = 0$; otherwise, fix $\varepsilon \in (0,1)$ and assume that $\sigma_n(S) \geq \eta_\varepsilon(\Lambda)$. Then $R_\alpha(P\|Q) \leq \left(\frac{1+\varepsilon}{1-\varepsilon}\right)^{\frac{\alpha}{\alpha-1}} \cdot \exp\left(\alpha\pi\frac{\|\boldsymbol{c}-\boldsymbol{c}'\|^2}{\sigma_n(S)^2}\right)$.*

3 Tighter Analysis for Discrete Gaussian Sampling with Small Precomputed Tables

In this section, we study Ducas et al.'s discrete Gaussian sampling [DDLL13] with precomputed tables. By adaptively optimizing the order of the RD, we show that the sampling for BLISS signature scheme can be securely performed with less table storage.

Discrete Gaussian Sampling. In the BLISS signature scheme [DDLL13], signing a message requires sampling $2n$ independent integers from one-dimensional discrete Gaussian distributions $D_{\mathbb{Z},s}$, where s is the standard deviation parameter. See Appendix B for detailed algorithms. In [DDLL13], an efficient sampling algorithm for $D_{\mathbb{Z},s}$ is presented. Let B_c be the Bernoulli distribution that outputs 1 with probability c and 0 otherwise. First, the algorithm samples ℓ Bernoulli random variables of the form B_{c_i} for $i = 0, \ldots, \ell-1$ where $c_i = \exp(-\pi 2^i/s^2)$. By using a rejection sampling [GPV08], these ℓ Bernoulli samples produce a sample from $D_{\mathbb{Z},s}$. Hence, to sign a signature, $\ell \cdot 2n$ Bernoulli variables are sampled. For the detailed algorithm, see Table 3 in [DDLL13]. In this paper, we focus on sampling from Bernoulli distributions. To efficiently sample the Bernoulli random variables, a precomputed table that stores the probabilities c_i for $i = 0, \ldots, \ell-1$ is used. The algorithm samples x from a uniform distribution over $(0,1)$, and outputs 1 if $x < c_i$ and 0 otherwise. Since the exact quantities of c_i are real, the truncated values $\tilde{c}_i = c_i + \varepsilon_i$ are stored. Here, $|\varepsilon_i| \leq 2^{-p}c_i$ denotes the truncation error where p is the bit precision. When $c_i > 1/2$, truncated probabilities are stored for $1 - c_i$ with the bit precisions p. Hence, the table storage becomes $\ell \cdot p$ bits whose size affects the efficiency.

Previous Analyses. As in [BLL+15], we analyze the security of BLISS when an adversary is allowed up to q_s signing queries. In this case, $\ell \cdot 2n \cdot q_s$ Bernoulli random variables are sampled since we should sample $\ell \cdot 2n$ Bernoulli random variables to sign a signature. Let Φ (resp. Φ') be a distribution of signatures in the view of the adversary where all $\ell \cdot 2n \cdot q_s$ variables are sampled from the truncated (resp. untruncated) Bernoulli distribution $B_{\tilde{c}_i}$ (resp. B_{c_i}). The distribution Φ (resp. Φ') is regarded as the *real* (resp. *ideal*) distribution. We will show that the BLISS signature scheme by sampling from the real distribution Φ is secure with smaller parameters, i.e., more signing queries q_s and less bit precision p, and the reduction from the scheme by sampling from the ideal distribution Φ' is tight, i.e., ε becomes small with larger ε'.

To examine the security, Ducas et al. [DDLL13] and Pöppelmann et al. [PDG14] used the SD and KLD, respectively. Although we omit the details, the SD becomes $\Delta(\Phi, \Phi') = \ell \cdot 2n \cdot q_s \cdot 2^{-p-1}$, which leads to $\varepsilon \leq \varepsilon' + \ell \cdot 2n \cdot q_s \cdot 2^{-p-1}$; hence, when $p \geq \log(\ell \cdot 2n \cdot q_s/\varepsilon)$, the reduction becomes almost tight, i.e., $\varepsilon \leq 2 \cdot \varepsilon'$. The KLD becomes $\ln R_1(\Phi\|\Phi') \leq \ell \cdot 2n \cdot q_s \cdot 2^{-2p}$ that leads to $\varepsilon \leq \varepsilon' + \sqrt{\ell \cdot 2n \cdot q_s \cdot 2^{-2p}}$. Hence, when $p \geq \log(\ell \cdot 2n \cdot q_s/\varepsilon^2)/2 + 1/2$, the reduction becomes almost tight, i.e., $\varepsilon \leq 2 \cdot \varepsilon'$. See [BLL+15] for detailed analyses. Notice that the required precisions p depend on ε for both SD and KLD based analyses.

Bai et al. [BLL+15] used the RD of orders $\alpha = +\infty$ and 2, and showed that the sampling algorithm becomes secure with less table storage $\ell \cdot p$, which does not depend on ε. From the multiplicativity property over $i = 0, \ldots, \ell - 1$ and the data processing inequality of the RD, $R_\alpha(\Phi \| \Phi') \leq (\max_{i \in [1,\ell]} R_\alpha(B_{\tilde{c}_i} \| B_{c_i}))^{\ell \cdot 2n \cdot q_s}$. Let ε (resp. ε') be the advantage for an adversary to break BLISS whose instances are sampled from Φ (resp. Φ'). From the probability preservation property of the RD, $\varepsilon \leq (\varepsilon' \cdot R_\alpha(\Phi \| \Phi'))^{\frac{\alpha-1}{\alpha}}$.

Using symmetry, we assume that $c_i \leq 1/2$; otherwise, we exchange c_i and $1 - c_i$ in the following calculations. First, Bai et al. used the RD of order $\alpha = +\infty$. By definition,

$$R_\infty(B_{\tilde{c}_i} \| B_{c_i}) = \max \left\{ \frac{c_i + \varepsilon_i}{c_i}, \frac{1 - c_i - \varepsilon_i}{1 - c_i} \right\} = 1 + \frac{|\varepsilon_i|}{c_i} \leq 1 + 2^{-p}.$$

Then, $R_\infty(\Phi \| \Phi') \leq (1 + 2^{-p})^{\ell \cdot 2n \cdot q_s}$ from the multiplicativity property over $i = 0, \ldots, \ell - 1$ and the data processing inequality of the RD. The RD bound implies $\varepsilon \leq \varepsilon' \cdot (1 + 2^{-p})^{\ell \cdot 2n \cdot q_s}$ from the probability preservation property of the RD. Hence, when $p \geq \log(\ell \cdot 2n \cdot q_s)$, the reduction becomes almost tight, i.e., $\varepsilon \leq 2 \cdot \varepsilon'$. Since the probability preservation property of the RD is multiplicative, the required precisions do not depend on ε, which results in less table storage. The required precision is less than that of the previous SD and KLD based analyses [DDLL13, PDG14].

Next, the RD of order $\alpha \in (1, +\infty)$ was considered. By definition,

$$(R_\alpha(B_{\tilde{c}_i} \| B_{c_i}))^{\alpha - 1} = c_i \left(\frac{c_i + \varepsilon_i}{c_i} \right)^\alpha + (1 - c_i) \left(\frac{1 - c_i - \varepsilon_i}{1 - c_i} \right)^\alpha. \tag{3}$$

In particular, Bai et al. focused on the case $\alpha = 2$, which is, $R_2(B_{\tilde{c}_i} \| B_{c_i}) = 1 + \frac{\varepsilon_i^2}{c_i(1-c_i)} \leq 1 + 2^{-2p}$. The last inequality holds by using the fact that $|\varepsilon_i| \leq 2^{-p} c_i$ and the assumption $c_i \leq 1/2$. Then, $R_2(\Phi \| \Phi') \leq (1 + 2^{-2p})^{\ell \cdot 2n \cdot q_s}$ from the multiplicativity property over $i = 0, \ldots, \ell - 1$ and the data processing inequality of the RD. The RD bound leads to $\varepsilon \leq \varepsilon'^{1/2} \cdot (1 + 2^{-2p})^{\ell \cdot 2n \cdot q_s}$ from the probability preservation property of the RD. Hence, Bai et al. concluded the precision to be $p \geq \log(\ell \cdot 2n \cdot q_s)/2$. The required precision of the R_2 based analysis is half that of the R_∞ based analysis. The improvements are derived from the exponent of $R_2(B_{\tilde{c}_i} \| B_{c_i})$, which becomes $-2p$, although that of R_∞ is $-p$. Although the required precision is less than that of the R_∞ based analysis, R_2 based analysis offers a reduction that is no longer tight, i.e., $\varepsilon \leq 2 \cdot \varepsilon'^{1/2}$ from the probability preservation property of the RD. The deficiency comes from the preservation property of R_2, i.e., $\varepsilon \leq \varepsilon'^{1/2} \cdot R_2(\Phi \| \Phi')$. The exponent of ε' never allows tight reductions even if the precision become infinitely large.

Tighter RD Based Analysis with Smaller Table Storage. In the rest of this section, we show that the R_α based analysis offers both less required precision and tighter reductions when the order α is appropriately determined. First, the RD of the inequality (3) is bounded for general α as follows.

Lemma 6 *Let probability distributions $B_{\tilde{c}_i}$ and B_{c_i} be defined as above. If the order α is an integer with $\alpha < 2^p$, then $(R_\alpha(B_{\tilde{c}_i} \| B_{c_i}))^{\alpha - 1} = \exp\left(\frac{\alpha(\alpha-1)}{2} \cdot 2^{-2p} \right) + O((\alpha 2^{-p})^3)$.*

The proof of Lemma 6 is given in Appendix C. Then, we obtain the following Theorem 1.

For the condition in Theorem 1, we define the minimal key recovery advantage $\hat{\varepsilon}$. In Appendix A of [DDLL13], known attacks for BLISS are summarized including lattice reduction attacks for the underlying SIS, primal and dual lattice reduction key recoveries. The most primitive brute-force key recovery is also analyzed, where an adversary guesses a random secret vector g and checks whether $f = a_q^{-1}(2g+1) \mod q$ is a legitimate secret polynomial or not for the public polynomial a_q; otherwise, the adversary aborts. The advantage is estimated as[2] $\hat{\varepsilon} = 2^{-d_1-d_2} \cdot \binom{n}{d_1}^{-1} \cdot \binom{n-d_1}{d_2}^{-1}$ where d_1 and d_2 are defined in the key generation of BLISS. For example, $\hat{\varepsilon} \approx 2^{-600}$ for BLISS-I parameters $n = 512, d_1 \approx 153$, and $d_2 \approx 0$. In Theorem 1, we consider powerful adversaries with signing query number $q_s \approx 2^{64}$. For such a powerful adversary, it holds that $\ell \cdot n \cdot q_s \gg -\ln(\hat{\varepsilon})$. For example, for practical BLISS-I parameters ($n = 512, \ell = 29$), the left (resp. right) hand side $\approx 2^{78}$ (resp. ≈ 600), then the above inequality holds.

Theorem 1 *Let parameters p, ℓ, n, and q_s that satisfy $\ell \cdot n \cdot q_s \gg -\ln(\hat{\varepsilon})$, and probability distributions $B_{\tilde{c}_i}$ and B_{c_i} be defined as above. Then, if there is an adversary $\mathcal{A}$ against the BLISS signature scheme when Bernoulli random variables are sampled from $B_{\tilde{c}_i}$ with run-time T and advantage ε, then $\mathcal{A}$ is also an adversary against the BLISS signature scheme when Bernoulli random variables are sampled from B_{c_i} with run-time $T' = T$ and advantage ε' that satisfies $-\ln(\varepsilon') > \ell \cdot n \cdot q_s \cdot 2^{-2p}$ and*

$$\varepsilon \leq \exp\left(-\left(\sqrt{-\ln(\varepsilon')} - \sqrt{\ell \cdot n \cdot q_s \cdot 2^{-2p}}\right)^2\right). \tag{4}$$

Proof. To prove the theorem, we consider the RD of order α that is much smaller than 2^p. (The fact is justified by the inequality $\ell \cdot n \cdot q_s \gg -\ln(\hat{\varepsilon})$ later in this proof.) By Lemma 6, we ignore the small term and assume $(R_\alpha(B_{\tilde{c}_i} \| B_{c_i}))^{\alpha-1} = \exp\left(\frac{\alpha(\alpha-1)}{2} \cdot 2^{-2p}\right)$, which implies

$$(R_\alpha(\Phi \| \Phi'))^{\alpha-1} \leq (R_\alpha(B_{\tilde{c}_i} \| B_{c_i}))^{(\alpha-1)\cdot\ell\cdot 2n\cdot q_s} = \exp\left(\alpha(\alpha-1) \cdot \ell \cdot n \cdot q_s \cdot 2^{-2p}\right)$$

from the multiplicativity property over $i = 0, \ldots, \ell-1$ and the data processing inequality of the RD. Since the exponent is $-2p$, the analysis requires a small precision similar to the R_2 based analysis. Furthermore,

$$\varepsilon \leq \left(\varepsilon' \cdot R_\alpha(\Phi \| \Phi')\right)^{\frac{\alpha-1}{\alpha}} = \exp\left(\frac{\alpha-1}{\alpha}\ln(\varepsilon') + (\alpha-1) \cdot \ell \cdot n \cdot q_s \cdot 2^{-2p}\right)$$

holds from the probability preservation property of the RD. The inequality is equivalent to the inequality (1) in Section 1. The right hand side of the inequality is bounded below by

$$\begin{aligned} &\exp\left(\ln(\varepsilon') - \ell \cdot n \cdot q_s \cdot 2^{-2p} + \left(-\ln(\varepsilon')/\alpha + \alpha \cdot \ell \cdot n \cdot q_s \cdot 2^{-2p}\right)\right) \\ \geq &\exp\left(\ln(\varepsilon') - \ell \cdot n \cdot q_s \cdot 2^{-2p} + 2\sqrt{-\ln(\varepsilon') \cdot \ell \cdot n \cdot q_s \cdot 2^{-2p}}\right) \end{aligned}$$

by the inequality of the arithmetic mean and geometric mean; the equality holds if and only if $-\ln(\varepsilon')/\alpha = \alpha \cdot \ell \cdot n \cdot q_s \cdot 2^{-2p}$, i.e., $\alpha = \sqrt{\frac{-\ln(\varepsilon')}{\ell \cdot n \cdot q_s \cdot 2^{-2p}}}$.

[2] In [DDLL13], the *brute-force* adversary for all key candidates is considered; however, we consider the corresponding *one-time* guessing adversary. Hence, the advantage of the guessing adversary is the inverse of the computation time of the brute-force adversary.

Table 4. Comparison of required precisions p, table bit-size and upper bounds of $-\log \varepsilon'$. The left table is a summary of previous analyses that are the same as in Table 1 of [BLL+15]. The right table is based on our analysis.

statistical measure	p	Table bit-size	$-\log \varepsilon'$
SD [DDLL13]	207	6003	≤ 129
KLD [PDG14]	168	4872	≤ 129
RD, $\alpha = +\infty$ [BLL+15]	79	2291	≤ 129
RD, $\alpha = 2$ [BLL+15]	40	1160	256.45

α	p	Table bit-size	$-\log \varepsilon'$
2.48	36	1044	418.66
6.94	38	1102	184.97
24.76	40	1160	141.26
96.07	42	1218	131.25
381.30	44	1276	128.80

Notice that the order $\alpha = \sqrt{\frac{-\ln(\varepsilon')}{\ell \cdot n \cdot q_s \cdot 2^{-2p}}}$ satisfies our assumption $\alpha \ll 2^p$. By definition, the inequality $\hat{\varepsilon} \leq \varepsilon'$, which is equivalent to $-\ln \varepsilon' \leq -\ln(\hat{\varepsilon})$, holds. Since we only consider the case $-\ln(\hat{\epsilon}) \ll \ell \cdot n \cdot q_s$, $-\ln(\epsilon') \ll \ell \cdot n \cdot q_s$ also holds. That leads to $\alpha = \sqrt{\frac{-\ln(\varepsilon')}{\ell \cdot n \cdot q_s \cdot 2^{-2p}}} \ll 2^p$.

Next, we set the order $\alpha = \sqrt{\frac{-\ln(\varepsilon')}{\ell \cdot n \cdot q_s \cdot 2^{-2p}}}$. In this case, the above inequality becomes

$$\varepsilon \leq \exp\left(-\left(\sqrt{-\ln(\varepsilon')} - \sqrt{\ell \cdot n \cdot q_s \cdot 2^{-2p}}\right)^2\right).$$

The inequality is equivalent to the inequality (2) in Section 1 as required. The order $\alpha = \sqrt{\frac{-\ln(\varepsilon')}{\ell \cdot n \cdot q_s \cdot 2^{-2p}}}$ that is used satisfies $\alpha \in (1, +\infty]$ since $-\ln(\varepsilon') > \ell \cdot n \cdot q_s \cdot 2^{-2p}$. □

For the BLISS signature scheme to be secure, i.e., ε to be small, with *smaller* $-\ln(\varepsilon')$ (larger ε', i.e., tighter reductions), *more* signing queries q_s (i.e., for powerful adversaries), and *larger* 2^{-p} (less precision p, i.e., more efficiency), the inequality (4) shows an appropriate trade-off. The upper bound of ε based on our analysis is lower than that of Bai et al.'s R_2 based analysis for all $\varepsilon', \ell, n, q_s$, and p. In particular, from the inequality (4), if

$$\begin{aligned}\varepsilon &\leq \exp\left(-\left(\sqrt{-\ln(\varepsilon')} - \sqrt{\ell \cdot n \cdot q_s \cdot 2^{-2p}}\right)^2\right) \\ &= \varepsilon' \cdot \exp\left(2\sqrt{-\ln(\varepsilon') \cdot \ell \cdot n \cdot q_s \cdot 2^{-2p}} - \ell \cdot n \cdot q_s \cdot 2^{-2p}\right),\end{aligned}$$

when $-\ln(\varepsilon') \cdot \ell \cdot n \cdot q_s \cdot 2^{-2p} \leq 1$, then $\varepsilon \leq \varepsilon' \cdot O(1)$ holds and the upper bound cannot be obtained by the R_2 based analysis. The condition leads to the precision requirement $p \geq \log(-\ln(\varepsilon') \cdot \ell \cdot n \cdot q_s)/2$ that is less than that of the SD, KLD, and R_∞ based analyses for powerful adversaries, i.e., $\ell \cdot n \cdot q_s \gg -\ln(\hat{\varepsilon})$.

Numerical Examples. Table 4 shows the numerical examples that compare required precisions p, table bit-size $\ell \cdot p$, and upper bounds of $-\log(\varepsilon')$ of previous analyses [DDLL13, PDG14, BLL+15] and our analysis. According to Table 1 in [BLL+15], an adversary is allowed $q_s = 2^{64}$ sign queries and breaks BLISS-I with probability $\varepsilon = 2^{-128}$ with parameters $n = 512$, and $\ell = 29$. The values of $-\log(\varepsilon')$ are given by

$$-\log(\varepsilon') \leq \log(e) \cdot \left(\sqrt{-\ln(\varepsilon)} + \sqrt{\ell \cdot n \cdot q_s \cdot 2^{-2p}}\right)^2$$

which is equivalent to the inequality (4). The table clarifies our improvements that are briefly summarized in Table 1. Although Bai et al.'s R_2 based analysis [BLL+15] requires less precision p than SD, KLD, and R_∞ based analyses [DDLL13, PDG14, BLL+15], the reduction is no longer tight and $-\log(\varepsilon')$ becomes much larger than $-\log(\varepsilon) = 128$. Theorem 1 shows a better trade-off than previous analyses. As the right table indicates, as the bit precision p increases, $-\log(\varepsilon')$ becomes smaller, which makes the reduction tighter. In particular, based on our analysis, the upper bound of $-\log(\varepsilon')$ for $p = 40$ is smaller that of the R_2 based analysis by Bai et al. [BLL+15]. As a result[3] , when $p \geq 44$, the reduction becomes almost tight, i.e., $-\log(\varepsilon') \leq 129$. Notice that the orders α are always much smaller than 2^p, which we assume to bound the quantity of RD.

4 Tighter Analysis for LWE to k-LWE Reduction

In this section, we study LWE to k-LWE reduction [LPSS14]. By adaptively optimizing the order of the RD, the reduction becomes tighter.

First, we introduce a variant of the LWE problem, where the number of samples m produced by the oracle is a priori bounded.

Definition 1 ($\mathrm{LWE}_{\beta,m}$ Problem) *Given $A \leftarrow U\left(\mathbb{Z}_q^{m\times n}\right)$, the goal of the $\mathrm{LWE}_{\beta,m}$ problem is to distinguish between the distributions (over $\mathbb{T}^m$)*

$$\frac{1}{q}U\left(\mathrm{Im}(A)\right) + \nu_\beta^m \text{ and } \frac{1}{q}U\left(\mathbb{Z}_q^m\right) + \nu_\beta^m.$$

Next, we introduce the k-LWE problem defined in [LPSS14].

Definition 2 ((k,S,C)-$\mathrm{LWE}_{\beta,m}$ Problem, Definition 7 of [LPSS14]) *Let $k \leq m$, $S \in \mathbb{R}^{m\times m}$ be invertible and $C = (\boldsymbol{c}_1\| \cdots \|\boldsymbol{c}_k) \in \mathbb{R}^{k\times m}$. Given $A \leftarrow U\left(\mathbb{Z}_q^{m\times n}\right)$, and $\boldsymbol{x}_i \leftarrow D_{\Lambda^\perp(A),S,\boldsymbol{c}_i}$ for $i \leq k$, the goal of the (k,S,C)-$\mathrm{LWE}_{\beta,m}$ problem (the (k,S)-$\mathrm{LWE}_{\beta,m}$ problem when $C = 0$) is to distinguish between the distributions (over $\mathbb{T}^m$)*

$$\frac{1}{q}U\left(\mathrm{Im}\left(A\right)\right) + \nu_\beta^m \text{ and } \frac{1}{q}U\left(\mathrm{Span}_{i\leq k}\left(\boldsymbol{x}_i\right)^\perp\right) + \nu_\beta^m.$$

The k vectors $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k$ can be used to solve the original $\mathrm{LWE}_{\beta,m}$. When we obtain a vector $\boldsymbol{y}$ from the left distribution, $\langle \boldsymbol{x}_i, \boldsymbol{y}\rangle$ becomes much smaller than 1 for standard parameter settings since $\boldsymbol{x}_i \in \Lambda^\perp(A)$ and is orthogonal to $\mathrm{Im}(A)$. On the other hand, when we obtain a vector $\boldsymbol{y}$ from the right distribution, $\langle \boldsymbol{x}_i, \boldsymbol{y}\rangle$ is uniform. However, (k,S,C)-$\mathrm{LWE}_{\beta,m}$ becomes non-trivial and seems to be hard since the right distribution $\frac{1}{q}U\left(\mathbb{Z}_q^m\right)$ is replaced by $\frac{1}{q}U\left(\mathrm{Span}_{i\leq k}\left(\boldsymbol{x}_i\right)^\perp\right)$.

Ling et al. [LPSS14] proved the security reduction for the (k,S)-$\mathrm{LWE}_{\beta,m}$ problem. An adversary that solves the (k,S)-$\mathrm{LWE}_{\beta',m+k}$ problem in Definition 2 is also an adversary that solves the $\mathrm{LWE}_{\beta,m}$ problem in Definition 1. However, Ling et al.'s reduction is not tight since they fix the order of the RD to $\alpha = 2$. We show the tighter security reduction as follows by *adaptively* optimizing the order.

[3] In [BLL+15], Bai et al. analyzed the precisions by measuring the closeness between $B_{\tilde{c}_i}$ and B_{c_i} which depend on i. The analysis further reduces the required precisions for SD and KLD based analyses, i.e., 4598 and 3893-bit tables respectively. Although our analysis also offers lower precisions, we omit the analysis in this paper.

Theorem 2 *Let m, q, σ, σ', and k satisfy $\sigma \geq \Omega(\max(m\sqrt{\log m}, \sigma'^{k/(m+k)}))$, $\sigma' \geq \Omega\left(m^3\sigma^2 \log^{3/2}(m\sigma)\right)$, $q \geq \Omega\left(\sigma'\sqrt{\log m}\right)$ is prime, and $m \geq \Omega(n \log q)$. Then there exists a probabilistic polynomial-time reduction from $\mathcal{A}'$ for $\mathrm{LWE}_{\beta,m}$ in dimension n to (k,S)-$\mathrm{LWE}_{\beta',m+k}$ in dimension n, where $\beta' = \Omega\left(m^{3/2}\sigma'\beta\right)$, S is a diagonal matrix, $a_{ii} = \sigma$ for $1 \leq i \leq m$, and $a_{ii} = \sigma'$ for $m+1 \leq i \leq m+k$.*

More concretely, using a (k,S)-$\mathrm{LWE}_{\beta',m+k}$ algorithm with run-time T and advantage ε, the reduction gives an $\mathrm{LWE}_{\beta,m}$ algorithm with run-time $T' = O\left(T \cdot poly(m) \cdot (\varepsilon - 2^{-\Omega(n)})^{-2} \log((\varepsilon - 2^{-\Omega(n)})^{-1})\right)$ and advantage ε' where

$$\varepsilon \leq \exp\left(\frac{\ln\left(\varepsilon' + 2^{-\Omega(n)}\right)}{2} + \frac{\sqrt{-1 - 2n\ln(\varepsilon' + 2^{-\Omega(n)})}}{2n}\right) \cdot 2^{O(k \cdot 2^{-n})} + 2^{-\Omega(n)}.$$

In [LPSS15], Ling et al. suggested appropriate selections of parameters as $k = m/10, \sigma = \tilde{\Theta}(n), \sigma' = \tilde{\Theta}(n^5), q = \tilde{\Theta}(n^5)$ and $m = \Theta(n \log n)$.

Proof. The proof of Theorem 2 consists of Lemma 7 and Theorem 3; that is, the required reduction of Theorem 2 consists of two subreductions as in [LPSS14]. The first is the LWE to (k,S,C)-LWE reduction, and the second is the (k,S,C)-LWE to (k,S)-LWE reduction. We follow the first subreduction.

Lemma 7 ([LPSS15]) *Let parameters $k, n, m, q, \sigma, \sigma', \beta'$, and matrix S be defined as in Theorem 2. Let $C \in \mathbb{R}^{k \times (m+k)}$ be the matrix whose i-th row is the unit vector $\mathbf{c}_i = (0^m | \delta_i)$ where δ_i denotes the i-th canonical unit vector in $\mathbb{Z}^k$ for $k = 1, \ldots, k$. If there exists a distinguisher $\mathcal{A}$ against (k,S,C)-$\mathrm{LWE}_{\beta',m+k}$ in dimension n with run-time T and advantage ε, then $\mathcal{A}$ is also a distinguisher against $\mathrm{LWE}_{\beta,m}$ in dimension n with run-time $T' = T + poly(m)$ and advantage $\varepsilon' = \varepsilon - 2^{-\Omega(n)}$.*

Next, we analyze the second subreduction. Although our analysis is similar to that in [LPSS14], the following Theorem 3 is obtained as an application of our optimized selection of the order α.

Theorem 3 *Let $m' = m + k$ and assume that $\sigma_{m'}(S) \geq \omega(\sqrt{n})$. Let γ be a constant that satisfies $\sigma_{m'}(S) \geq \sqrt{\pi/\gamma} \cdot \|C\|$. If there exists a distinguisher $\mathcal{A}$ against (k,S)-$\mathrm{LWE}_{\beta',m'}$ in dimension n' with run-time T and advantage ε, then there exists a distinguisher $\mathcal{A}'$ against (k,S,C)-$\mathrm{LWE}_{\beta',m'}$ with run-time $T' = O\left(poly(m') \cdot \left(\varepsilon - 2^{-\Omega(n)}\right)^{-2} \cdot T \cdot \log\left((\varepsilon - 2^{-\Omega(n)})^{-1}\right)\right)$ and advantage ε' that satisfies $-\ln\left(\varepsilon' + 2^{-\Omega(n)}\right) \geq k\gamma$, and*

$$\varepsilon \leq \exp\left(\frac{\ln\left(\varepsilon' + 2^{-\Omega(n)}\right)}{2} + \frac{k\gamma\sqrt{-1 - 2\ln(\varepsilon' + 2^{-\Omega(n)})/(k\gamma)}}{2}\right) \cdot 2^{O(k \cdot 2^{-n})} + 2^{-\Omega(n)}.$$

The proof of Theorem 3 is given in Appendix D. Based on the SD, the deviations to sample k hint vectors become exponentials of the security parameter. Since Ling et al. used the RD, the deviations become smaller. Moreover, we optimize the order α and obtain a tighter reduction.

Note that in the above reduction from $\mathrm{LWE}_{\beta,m}$ to (k,S,C)-$\mathrm{LWE}_{\beta',m+k}$, $\|C\| = 1$ and $\sigma_{m'}(S) = \sigma = \Omega(n)$; hence, we set $\gamma = O(1/n^2)$. Using the fact that $k < n$ and we can obtain the required inequality in Theorem 2. □

Analogous to Theorem 3, the inequality in [LPSS14] can be written as

$$\varepsilon \leq \exp\left(\frac{\ln\left(\varepsilon' + 2^{-\Omega(n)}\right)}{3} + \frac{2k\gamma}{3}\right) \cdot 2^{O(k \cdot 2^{-n})} + 2^{-\Omega(n)}.$$

The inequality can be obtained by R_2. The right hand side of the inequality becomes the same as ours only when $\alpha = 2$; otherwise, our analysis always offers a tighter reduction since the right hand side of the inequality in Theorem 3 is always smaller than that of Ling et al.

5 Tighter Analysis for SIS to *k*-SIS Reduction

In this section, we study SIS to k-SIS reduction [BF11, LPSS14]. By adaptively optimizing the order of the RD, the reduction becomes tighter.

First, we introduce the SIS problem.

Definition 3 ($\mathrm{SIS}_{\beta,m}$ Problem) *Given $A \leftarrow U\left(\mathbb{Z}_q^{m \times n}\right)$, the goal of the $\mathrm{SIS}_{\beta,m}$ problem is to find a nonzero vector $\boldsymbol{b} \in \mathbb{Z}^m$ such that*

- $\|\boldsymbol{b}\| \leq \beta$,
- $\boldsymbol{b}^T \cdot A = \boldsymbol{0} \mod q$.

Next, we introduce the k-SIS problem. The definition follows from Definition 2 rather than the original definition from [BF11].

Definition 4 ((k,S,C)-$\mathrm{SIS}_{\beta,m}$ Problem, Adapted from Definition 4.1 of [BF11]) *Let $k \leq m$, $S \in \mathbb{R}^{m \times m}$ be invertible, and $C = (\boldsymbol{c}_1 \| \cdots \| \boldsymbol{c}_k) \in \mathbb{R}^{k \times m}$. Given $A \leftarrow U\left(\mathbb{Z}_q^{m \times n}\right)$ and $x_i \leftarrow D_{\Lambda^\perp(A),S,\boldsymbol{c}_i}$ for $i \leq k$, the goal of the (k,S,C)-$\mathrm{SIS}_{\beta,m}$ problem (the (k,S)-$\mathrm{SIS}_{\beta,m}$ problem when $C = 0$) is to find a nonzero vector $\boldsymbol{b} \in \mathbb{Z}^m$ such that*

- $\|\boldsymbol{b}\| \leq \beta$,
- $\boldsymbol{b}^T \cdot A = \boldsymbol{0} \mod q$,
- $\boldsymbol{b} \in \mathrm{Span}_{i \leq k}\left(\boldsymbol{x}_i\right)^\perp$.

The k vectors $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k$ for (k,S)-$\mathrm{SIS}_{\beta,m}$ can be used to solve the original $\mathrm{SIS}_{\beta,m}$. By definition, the vectors satisfy the second condition of $\mathrm{SIS}_{\beta,m}$. Since the vectors are sampled from Gaussian distributions, their norms are small and the vectors are expected to satisfy the first condition of $\mathrm{SIS}_{\beta,m}$. However, (k,S,C)-$\mathrm{SIS}_{\beta,m}$ is non-trivial and seems to be hard since the additional condition $\boldsymbol{b} \in \mathrm{Span}_{i \leq k}\left(\boldsymbol{x}_i\right)^\perp$ have to be satisfied. The integer linear combinations of the k hint vectors cannot be solutions to the (k,S,C)-$\mathrm{SIS}_{\beta,m}$.

Ling et al. [LPSS14] briefly summarized the SIS to k-SIS reduction. As the $\mathrm{LWE}_{\beta,m}$ to the (k,S)-$\mathrm{LWE}_{\beta,m+k}$ reduction, they showed that an adversary that solves the (k,S)-$\mathrm{SIS}_{\beta',m+k}$ problem in Definition 4 is also an adversary that solves the $\mathrm{SIS}_{\beta,m}$ problem in Definition 3. However, Ling et al.'s reduction is not tight since they fix the order of the RD to $\alpha = 2$. We show the tighter security reduction as follows by *adaptively* optimizing the order.

Theorem 4 *Let parameters $k, n, m, q, \sigma, \sigma', \beta'$, and a matrix S be defined as in Theorem 2. If there exists an adversary $\mathcal{A}$ against (k,S)-$\mathrm{SIS}_{\beta',m+k}$ in dimension n, with run-time T and advantage ε,*

then $\mathcal{A}'$ is also an adversary against $\mathrm{SIS}_{\beta,m}$ *in dimension n and $\beta = \Omega(\sqrt{km}\sigma'\beta')$ with run-time $T' = T + poly(m)$ and advantage ε' where*

$$\varepsilon \leq \exp\left(-\left(\sqrt{-\ln\left(\varepsilon' + 2^{-\Omega(n)}\right)} - \sqrt{k\gamma}\right)^2\right) \cdot 2^{O\left(k \cdot 2^{-n}\right)} + 2^{-\Omega(n)}.$$

Proof. As LWE to (k, S)-LWE reduction, the reduction consists of two subreductions. The first is the SIS to (k, S, C)-SIS reduction, and the second is the (k, S, C)-SIS to (k, S)-SIS reduction. The first subreduction is almost identical to that of the LWE to (k, S, C)-LWE reduction as suggested in [LPSS14].

Lemma 8 (Adapted from [LPSS14]) *Let k, n, m, q, σ, and σ' be the same as those in Theorem 2. Let matrices C and S be the same as Lemma 7. If there exists an adversary against (k, S, C)-$\mathrm{SIS}_{\beta',m+k}$ in dimension n, with S as in Theorem 2, run-time T, and advantage ε, then there exists an adversary against* $\mathrm{SIS}_{\beta,m}$ *in dimension n with $\beta = \Omega(\sqrt{km}\sigma'\beta')$, run-time $T' = T + poly(m)$, and advantage $\varepsilon' = \varepsilon - 2^{-\Omega(n)}$.*

The proof of Lemma 8 is given in Appendix E.

Next, we analyze the second subreduction. The following Theorem 5 is obtained as an application of our optimized selection of the order α. We cannot obtain the same tightness when we fix the order $\alpha = 2$ as in [LPSS14].

Theorem 5 *Assume that $\sigma_{m'}(S) \geq \omega(\sqrt{n})$. Let γ be a constant that satisfies $\sigma_{m'}(S) \geq \sqrt{\pi/\gamma} \cdot \|C\|$. If there exists an adversary $\mathcal{A}$ against (k, S)-$\mathrm{SIS}_{\beta,m'}$ in dimension n with run-time T and advantage ε, then $\mathcal{A}$ is also an adversary against (k, S, C)-$\mathrm{SIS}_{\beta,m'}$ with run-time $T' = T$ and advantage ε' that satisfies $-\ln\left(\varepsilon' + 2^{-\Omega(n)}\right) \geq k\gamma$, and*

$$\varepsilon \leq \exp\left(-\left(\sqrt{-\ln\left(\varepsilon' + 2^{-\Omega(n)}\right)} - \sqrt{k\gamma}\right)^2\right) \cdot 2^{O\left(k \cdot 2^{-n}\right)} + 2^{-\Omega(n)}.$$

The proof of Theorem 5 is given in Appendix E. Based on the SD, the deviations to sample k hint vectors become exponentials of the security parameter. Since Ling et al. used the RD, the deviations become smaller. Moreover, we optimize the order α and obtain a tighter reduction.

Note that in the above reduction from $\mathrm{SIS}_{\beta,m}$ to (k, S, C)-$\mathrm{SIS}_{\beta',m+2n}$, $\|C\| = 1$, and $\sigma_{m'}(S) = \sigma = \Omega(n)$. Hence, we set $\gamma = O(1/n^2)$ and using the fact that $k < n$, we can obtain the required inequality in Theorem 4. □

Analogous to Theorem 5, the inequality can be written as

$$\varepsilon \leq \exp\left(\frac{\ln\left(\varepsilon' + 2^{-\Omega(n)}\right)}{2} + k\gamma\right) \cdot 2^{O\left(k \cdot 2^{-n}\right)} + 2^{-\Omega(n)}.$$

when the order is fixed to $\alpha = 2$. The right hand side of the inequality becomes the same as ours only when $\alpha = 2$. Otherwise, our analysis always offers a tighter reduction since the right hand side of the inequality in Theorem 5 is always smaller than that of the R_2 based analysis.

References

[AGHS13] S. Agrawal, C. Gentry, S. Halevi and A. Sahai, "Discrete gaussian leftover hash lemma over infinite domains," Proc. Asiacrypt 2013, LNCS 8629, pp. 97–116, Springer, Heidelberg, 2013.

[AD97] M. Ajtai and C. Dwork, "A public-key cryptosystem with worst-case/average-case equivalence," Proc. STOC 1997, pp. 284–293, ACM, 1997.

[BLL+15] S. Bai, A. Langlois, T. Lepoint, D. Stehlé and R. Steinfeld, "Improved security proofs in lattice-based cryptography: using the Rényi divergence rather than the statistical distance," IACR Cryptology ePrint Archive: Report 2015/483, to appear at Asiacrypt 2015, 2015.

[BF11] D. Boneh and D. M. Freeman, "Linearly homomorphic signatures over binary fields and new tools for lattice-based signatures," Proc. PKC 2011, LNCS 6571, pp. 1–16, Springer, Heidelberg, 2011.

[CN11] Y. Chen and P. Q. Nguyen, "BKZ 2.0: Better lattice security estimates," D. H. Lee and X. Wang (Eds.) Proc. Asiacrypt 2011, LNCS 7073, pp. 1–20, Springer-Verlag, 2011.

[DDLL13] L. Ducas, A. Durmus, T. Lepoint and V. Lyubashevsky, "Lattice signatures and bimodal gaussians," Proc. Crypto 2013, LNCS 8042, pp. 40–56, Springer, Heidelberg, 2013.

[EH12] T. van Erven and P. Harremoës, "Rényi divergence and Kullback-Leibler divergence," CoRR, abs/1206.2459, 2012.

[GPV08] C. Gentry, C. Peikert and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," Proc. STOC 2008, pp. 197–206, ACM, 2008.

[LSS14] A. Langlois, D. Stehlé and R. Steinfeld, "GGHLite: More efficient multilinear maps from ideal lattices," Proc. Eurocrypt 2014, LNCS 8441, pp. 239–256, Springer, Heidelberg, 2014.

[LP10] R. Lindner and C. Peikert, "Better key sizes (and attacks) for LWE-based encryption," Proc. CT-RSA 2011, LNCS 6558, pp. 319–339, Springer, Heidelberg, 2011.

[LPSS14] S. Ling, D. H. Phan, D. Stehlé and R. Steinfeld, "Hardness of k-LWE and applications in traitor tracing," Proc. Crypto 2014, LNCS 8616, pp. 315–334, Springer, Heidelberg, 2014.

[LPSS15] S. Ling, D. H. Phan, D. Stehlé and R. Steinfeld, "Hardness of k-LWE and applications in traitor tracing," IACR Cryptology ePrint Archive: Report 2014/494 version 5 August 2015, 2015.

[LPR13] V. Lyubashevsky, C. Peikert and O. Regev, "On ideal lattices and learning with errors over rings," J. ACM, 60(6):43, 2013.

[MR07] D. Micciancio and O. Regev, "Worst-case to average-case reductions based on gaussian measures," SIAM J. Comput. 37(1): 267–302, 2007.

[PDG14] T. Pöppelmann, L. Ducas and T. Güneysu, "Enhanced lattice-based signatures on reconfigurable hardware," Proc. CHES 2014, LNCS 8731, pp. 353–370, Springer, Heidelberg, 2014.

[Reg05] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," Journal of ACM, volume 56, number 6, 2009.

[Ren61] A. Rényi, "On measures of entropy and information," Proc. The Fourth Berkeley Symposium on Math. Statistics and Probability, volume 1, pp. 547–561, 1961.

[TT15] K. Takashima and A. Takayasu, "Tighter security for efficient lattice cryptography via the Rényi divergence of optimized orders" Proc. ProvSec 2015, 2015.

A Proof of Lemma 5 in Section 2

By the definition of a discrete Gaussian distribution,

$$P(\boldsymbol{x}) = \frac{\exp(-\pi\|(S^T)^\dagger(\boldsymbol{x}-\boldsymbol{c})\|^2)}{\sum_{\boldsymbol{y}\in\Lambda}\exp(-\pi\|(S^T)^\dagger(\boldsymbol{y}-\boldsymbol{c})\|^2)} \text{ and } Q(\boldsymbol{x}) = \frac{\exp(-\pi\|(S^T)^\dagger(\boldsymbol{x}-\boldsymbol{c}')\|^2)}{\sum_{\boldsymbol{y}\in\Lambda}\exp(-\pi\|(S^T)^\dagger(\boldsymbol{y}-\boldsymbol{c}')\|^2)}.$$

By the definition of the RD, if follows that

$$R_\alpha(P\|Q)^{\alpha-1} = \sum_{\boldsymbol{x}\in\Lambda}\frac{P(\boldsymbol{x})^\alpha}{Q(\boldsymbol{x})^{\alpha-1}}$$

$$= \sum_{\boldsymbol{x}\in\Lambda}\left(\frac{\exp(-\pi\|(S^T)^\dagger(\boldsymbol{x}-\boldsymbol{c})\|^2)}{\sum_{\boldsymbol{y}\in\Lambda}\exp(-\pi\|(S^T)^\dagger(\boldsymbol{y}-\boldsymbol{c})\|^2)}\right)^\alpha \cdot \left(\frac{\sum_{\boldsymbol{y}\in\Lambda}\exp(-\pi\|(S^T)^\dagger(\boldsymbol{y}-\boldsymbol{c}')\|^2)}{\exp(-\pi\|(S^T)^\dagger(\boldsymbol{x}-\boldsymbol{c}')\|^2)}\right)^{\alpha-1}$$

$$= \frac{(\sum_{\boldsymbol{y}\in\Lambda}\exp(-\pi\|(S^T)^\dagger(\boldsymbol{y}-\boldsymbol{c}')\|^2))^{\alpha-1}}{(\sum_{\boldsymbol{y}\in\Lambda}\exp(-\pi\|(S^T)^\dagger(\boldsymbol{y}-\boldsymbol{c})\|^2))^{\alpha}} \cdot \sum_{\boldsymbol{x}\in\Lambda}\exp(-\alpha\pi\|(S^T)^\dagger(\boldsymbol{x}-\boldsymbol{c})\|^2 + (\alpha-1)\pi\|(S^T)^\dagger(\boldsymbol{x}-\boldsymbol{c}')\|^2).$$

Define $\tilde{\boldsymbol{c}} = \alpha\boldsymbol{c} - (\alpha-1)\boldsymbol{c}'$; then,

$$-\alpha\pi\|(S^T)^\dagger(\boldsymbol{x}-\boldsymbol{c})\|^2 + (\alpha-1)\pi\|(S^T)^\dagger(\boldsymbol{x}-\boldsymbol{c}')\|^2 = -\pi\|(S^T)^\dagger(\boldsymbol{x}-\tilde{\boldsymbol{c}})\|^2 + \alpha(\alpha-1)\pi\|(S^T)^\dagger(\boldsymbol{c}-\boldsymbol{c}')\|^2.$$

Therefore,

$$\begin{aligned} &R_\alpha(P\|Q)^{\alpha-1} \\ &= \frac{(\sum_{\boldsymbol{y}\in\Lambda}\exp(-\pi\|(S^T)^\dagger(\boldsymbol{y}-\boldsymbol{c}')\|^2))^{\alpha-1}\cdot\sum_{\boldsymbol{x}\in\Lambda}\exp(-\pi\|(S^T)^\dagger(\boldsymbol{x}-\tilde{\boldsymbol{c}})\|^2)}{(\sum_{\boldsymbol{y}\in\Lambda}\exp(-\pi\|(S^T)^\dagger(\boldsymbol{y}-\boldsymbol{c})\|^2))^{\alpha}} \cdot \exp(\alpha(\alpha-1)\pi\|(S^T)^\dagger(\boldsymbol{c}-\boldsymbol{c}')\|^2). \end{aligned}$$

The remaining analysis is the same as the proof of Lemma 4.2 in [LSS14]. For any $\boldsymbol{c}\in\Lambda$, if follows that $\sum_{\boldsymbol{x}\in\Lambda}\exp(-\pi\|(S^T)^\dagger(\boldsymbol{x}-\boldsymbol{c})\|^2) = \sum_{\boldsymbol{x}\in\Lambda}\exp(-\pi\|(S^T)^\dagger\boldsymbol{x}\|^2)$. Therefore, if $\boldsymbol{c},\boldsymbol{c}'\in\Lambda$, then $\tilde{\boldsymbol{c}}\in\Lambda$; hence, we have $R_\alpha(P\|Q) = \exp(\alpha\pi\|(S^T)^\dagger(\boldsymbol{c}-\boldsymbol{c}')\|^2)$.

In general $\boldsymbol{c},\boldsymbol{c}'\in\mathbb{R}^n$, we have $\rho_{\sigma_n(S),\boldsymbol{c}}(\Lambda) \le \sum_{\boldsymbol{x}\in\Lambda}\exp(-\pi\|(S^T)^\dagger(\boldsymbol{x}-\boldsymbol{c})\|^2) \le \rho_{\sigma_1(S),\boldsymbol{c}}(\Lambda)$, using the fact that $\sigma_n((S^T)^\dagger)\|\boldsymbol{x}-\boldsymbol{c}\| \le \|(S^T)^\dagger(\boldsymbol{x}-\boldsymbol{c})\| \le \sigma_1((S^T)^\dagger)\|\boldsymbol{x}-\boldsymbol{c}\|$, and

$$\begin{aligned} \sum_{\boldsymbol{x}\in\Lambda}\exp(-\pi\sigma_1((S^T)^\dagger)^2\|\boldsymbol{x}-\boldsymbol{c}\|^2) &= \rho_{1/\sigma_1((S^T)^\dagger),\boldsymbol{c}}(\Lambda) = \rho_{\sigma_n(S),\boldsymbol{c}}(\Lambda) \\ \sum_{\boldsymbol{x}\in\Lambda}\exp(-\pi\sigma_n((S^T)^\dagger)^2\|\boldsymbol{x}-\boldsymbol{c}\|^2) &= \rho_{1/\sigma_n((S^T)^\dagger),\boldsymbol{c}}(\Lambda) = \rho_{\sigma_1(S),\boldsymbol{c}}(\Lambda). \end{aligned}$$

Using the assumption that $\sigma_1(S) \ge \sigma_n(S) \ge \eta_\varepsilon(\Lambda)$ and Lemma 1, both $\rho_{\sigma_1(S),\boldsymbol{c}}(\Lambda)$ and $\rho_{\sigma_n(S),\boldsymbol{c}}(\Lambda)$ are in the interval $[1-\varepsilon, 1+\varepsilon]\cdot(\det(\Lambda))^{-1}$. From the above inequality, $\sum_{\boldsymbol{x}\in\Lambda}\exp(-\pi\|(S^T)^\dagger(\boldsymbol{x}-\boldsymbol{c})\|^2)$ are also in the interval. Hence, we have $R_\alpha(P\|Q) \le \left(\frac{1+\varepsilon}{1-\varepsilon}\right)^{\frac{\alpha}{\alpha-1}} \cdot \exp(\alpha\pi\|(S^T)^\dagger(\boldsymbol{c}-\boldsymbol{c}')\|^2)$.

Using the fact that $\|(S^T)^\dagger\boldsymbol{c}\|^2 \le \sigma_1((S^T)^\dagger)^2 \cdot \|\boldsymbol{c}\|^2$ and $\sigma_1((S^T)^\dagger) = 1/\sigma_n(S)$, the claimed inequality is satisfied.

B BLISS Signature Scheme

The BLISS signature algorithm is as follows:

- Key generation algorithm, $\mathsf{KeyGen}()$:
  - Choose f and g as uniform polynomials with exactly $d_1 = \lceil\delta_1 n\rceil$ entries in $\{\pm1\}$ and $d_2 = \lceil\delta_2 n\rceil$ entries in $\{\pm2\}$
  - $S = (s_1, s_2)^T \leftarrow (f, 2g+1)^T$
  - If $N_\kappa(S) \ge C^2\cdot 5\cdot(\lceil\delta_1 n\rceil + 4\lceil\delta_2 n\rceil)\cdot\kappa$ then restart
  - $a_q = (2g+1)/f \mod q$ (restart if f is not invertible)
  - Return $(pk = A, sk = S)$ where $A = (2a_q, q-2) \mod 2q$
- Signature Algorithm, $\mathsf{Sign}(\mu, pk = A, sk = S)$:
  - $\boldsymbol{y}_1, \boldsymbol{y}_2 \leftarrow D_{\mathbb{Z}^n,s}$
  - $\boldsymbol{u} = \zeta\cdot\boldsymbol{a}_1\cdot\boldsymbol{y}_1 + \boldsymbol{y}_2 \mod 2q$
  - $\boldsymbol{c} \leftarrow H(\lfloor\boldsymbol{u}\rceil_d \mod p, \mu)$

  - Choose a random bit b
  - $\boldsymbol{z}_1 \leftarrow \boldsymbol{y}_1 + (-1)^b \boldsymbol{s}_1 \boldsymbol{c}$
  - $\boldsymbol{z}_2 \leftarrow \boldsymbol{y}_2 + (-1)^b \boldsymbol{s}_2 \boldsymbol{c}$
  - Continue with probability $1/\left(M \exp\left(-\frac{\|S\boldsymbol{c}\|^2}{s^2/\pi}\right) \cosh\left(\frac{\langle \boldsymbol{z}, S\boldsymbol{c}\rangle}{s^2/\pi}\right)\right)$; otherwise, restart
  - $\boldsymbol{z}_2^\dagger \leftarrow (\lfloor \boldsymbol{u} \rceil_d - \lfloor \boldsymbol{u} - \boldsymbol{z}_2 \rceil_d) \mod p$
  - Return $(\boldsymbol{z}_1, \boldsymbol{z}_2^\dagger, \boldsymbol{c})$
- Verification Algorithm, $\mathsf{Verify}(\mu, pk = A, (\boldsymbol{z}_1, \boldsymbol{z}_2^\dagger, \boldsymbol{c}))$:
  - If $\|(\boldsymbol{z}_1 | 2^d \cdot \boldsymbol{z}_2^\dagger)\|_2 \geq B_2$, then reject
  - If $\|(\boldsymbol{z}_1 | 2^d \cdot \boldsymbol{z}_2^\dagger)\|_\infty \geq B_\infty$, then reject
  - Accept if and only if $\boldsymbol{c} = H(\lfloor \zeta \cdot \boldsymbol{a}_1 \cdot \boldsymbol{z}_1 + \zeta \cdot q \cdot \boldsymbol{c} \rceil_d + \boldsymbol{z}_2^\dagger \mod p, \mu)$

For the detailed definitions of parameters, see Table 3 in [DDLL13].

C Proof of Lemma 6 in Section 3

From the equality (3), it follows that

$$\begin{aligned}
(R_\alpha(B_{\tilde{c}_i} \| B_{c_i}))^{\alpha-1} &= c_i \sum_{j=0}^{\alpha} \binom{\alpha}{j} \left(\frac{\varepsilon_i}{c_i}\right)^j + (1-c_i) \sum_{j=0}^{\alpha} \binom{\alpha}{j} \left(-\frac{\varepsilon_i}{1-c_i}\right)^j \\
&= \sum_{j=0}^{\alpha} \binom{\alpha}{j} \left(\frac{\varepsilon_i^j}{c_i^{j-1}} + \frac{(-\varepsilon_i)^j}{(1-c_i)^{j-1}}\right) \\
&= 1 + \frac{\alpha(\alpha-1)}{2} \cdot \frac{\varepsilon_i^2}{c_i(1-c_i)} + \sum_{j=3}^{\alpha} \binom{\alpha}{j} \left(\frac{\varepsilon_i^j}{c_i^{j-1}} + \frac{(-\varepsilon_i)^j}{(1-c_i)^{j-1}}\right).
\end{aligned}$$

The first two terms satisfy

$$1 + \frac{\alpha(\alpha-1)}{2} \cdot \frac{\varepsilon_i^2}{c_i(1-c_i)} \leq \left(1 + \frac{|\varepsilon_i|^2}{c_i(1-c_i)}\right)^{\frac{\alpha(\alpha-1)}{2}} \leq \left(1 + 2^{-2p} \cdot \frac{c_i}{1-c_i}\right)^{\frac{\alpha(\alpha-1)}{2}} \leq \left(1 + 2^{-2p}\right)^{\frac{\alpha(\alpha-1)}{2}}$$

by using the fact that $c_i \leq 1/2$ and $|\varepsilon_i| \leq c_i 2^{-p}$. Since $\ln(1 + 2^{-2p}) \leq 2^{-2p}$,

$$\left(1 + 2^{-2p}\right)^{\frac{\alpha(\alpha-1)}{2}} \leq \exp\left(\frac{\alpha(\alpha-1)}{2} \cdot 2^{-2p}\right).$$

To complete the proof, it suffices to show that the remaining terms are of $O((\alpha 2^{-p})^3)$. The terms are bounded above by

$$\sum_{j=3}^{\alpha} \binom{\alpha}{j} \left(\frac{(-\varepsilon_i)^j}{(1-c_i)^{j-1}} + \frac{\varepsilon_i^j}{c_i^{j-1}}\right) \leq \sum_{j=3}^{\alpha} \frac{\alpha^j}{j!} \left(\frac{(-\varepsilon_i)^j}{(1-c_i)^{j-1}} + \frac{\varepsilon_i^j}{c_i^{j-1}}\right) \leq \sum_{j=3}^{\alpha} \frac{\alpha^j}{j!} \cdot 2 \cdot \frac{|\varepsilon_i|^j}{c_i^j} \cdot c_i \leq \sum_{j=3}^{\alpha} \frac{(\alpha 2^{-p})^j}{j!}$$

by using the fact that $c_i \leq 1/2$ and $|\varepsilon_i| \leq c_i 2^{-p}$. Then, the terms are bounded above by

$$\leq (\alpha 2^{-p})^3 \cdot \sum_{j=0}^{\alpha-3} \frac{(\alpha 2^{-p})^j}{j!} \leq (\alpha 2^{-p})^3 \cdot \sum_{j=0}^{\infty} \frac{(\alpha 2^{-p})^j}{j!} = (\alpha 2^{-p})^3 \cdot \exp(\alpha 2^{-p}) = O((\alpha 2^{-p})^3)$$

by using the fact that $\alpha 2^{-p} \leq 1$.

D Proof of Theorem 3 in Section 4

As in the proof of Lemma 15 in [LPSS14], we consider the following sequence of games $\mathsf{Game}_0, \ldots, \mathsf{Game}_3$, where the distributions from the view of the distinguisher $\mathcal{A}$ differ among the games as follows:

- Game_0: The original (k, S)-LWE experiment. The distinguisher $\mathcal{A}$ receives an instance of the form $(r, \boldsymbol{y})$, where $r = (A, \{\boldsymbol{x}_i\}_{i \le k})$ with $A \leftarrow U\left(\mathbb{Z}_q^{m' \times n}\right)$, and $\boldsymbol{x}_i \leftarrow D_{\Lambda^\perp(A),S,\boldsymbol{0}}$ for $i = 1, \ldots, k$, and $\boldsymbol{y} \in \mathbb{T}^{m'}$ is a sample from either the distribution
$$\frac{1}{q} U\left(\mathrm{Im}\left(A\right)\right) + \nu_\beta^{m'} \text{ or } \frac{1}{q} U\left(\mathrm{Span}_{i \le k}\left(\boldsymbol{x}_i\right)^\perp\right) + \nu_\beta^{m'}.$$
- Game_1: Modification of Game_0 in that the distribution of A is the following rejection sampling: A is sampled uniformly from $\mathbb{Z}_q^{m' \times n'}$; however, reject and resample A if $\eta_{2^{-n}}(A) > 4q^{n/m'}\sqrt{\log\left(2m'\left(1+2^n\right)\right)/\pi} = O(\sqrt{n})$.
- Game_2: Modification of Game_0 in that the distribution of the hint $\boldsymbol{x}_i'$s in $\boldsymbol{r}$ is from the non-zero centered distribution $D_{\Lambda^\perp(A),S,\boldsymbol{c}_i}$ (instead of the zero centered distribution $D_{\Lambda^\perp(A),S,\boldsymbol{0}}$).
- Game_3: Modification of Game_0 in that the distribution of A is $A \leftarrow U\left(\mathbb{Z}_q^{m' \times n}\right)$. The instance distribution is identical to that of the (k, S, C)-LWE experiment.

Let $\varepsilon_i(\mathcal{A})$ for $i = 0, \ldots, 3$ denote the advantage of $\mathcal{A}$ in distinguishing between the distributions in Game_i. By definition, $\varepsilon_0(\mathcal{A}) = \varepsilon$. As in [LPSS14], $\varepsilon_1(\mathcal{A}) \ge \varepsilon_0(\mathcal{A}) - 2^{-\Omega(n)}$ by Lemma 3.

As claimed in [LPSS14], the (k, S, C)-LWE problem has the *public samplability* property required to apply the following Lemma 9.

Lemma 9 (Theorem 4.1 of [BLL+15]) *Let Φ and Φ' denote two distributions with $\mathrm{Supp}\left(\Phi\right) \subseteq \mathrm{Supp}\left(\Phi'\right)$, and let $D_0(r)$ and $D_1(r)$ denote two distributions determined by some parameter $r \in \mathrm{Supp}\left(\Phi'\right)$. Let P and P' be two decision problems defined as follows:*

- *Problem P: Distinguish whether input x is sampled from X_0 or X_1, where*
$$X_0 = \left\{x : r \leftarrow \Phi, x \leftarrow D_0(r)\right\}, X_1 = \left\{x : r \leftarrow \Phi, x \leftarrow D_1(r)\right\}.$$
- *Problem P': Distinguish whether input x is sampled from X_0' or X_1', where*
$$X_0' = \left\{x : r \leftarrow \Phi', x \leftarrow D_0(r)\right\}, X_1' = \left\{x : r \leftarrow \Phi', x \leftarrow D_1(r)\right\}.$$

Assum that $D_0(\cdot)$ and $D_1(\cdot)$ satisfy the following public sampleablity property: there exists a sampling algorithm S with run-time T_{S} such that for all (r, b), given any sample x from $D_b(r)$:

- *$\mathsf{S}(0, x)$ outputs a fresh sample distributed as $D_0(r)$ over the randomness of S,*
- *$\mathsf{S}(1, x)$ outputs a fresh sample distributed as $D_1(r)$ over the randomness of S.*

Then, given a distinguisher $\mathcal{A}$ for problem P with run-time T and advantage ε, a distinguisher $\mathcal{A}'$ can be constructed for problem P' with run-time T' and advantage ε' where
$$T' = O\left(\frac{1}{\varepsilon^2}\log\left(\frac{R_\alpha\left(\Phi \| \Phi'\right)}{\varepsilon^{\alpha/(\alpha-1)}}\right) \cdot \left(T_{\mathsf{S}} + T\right)\right), \varepsilon' = \frac{\varepsilon}{4 \cdot R_\alpha\left(\Phi \| \Phi'\right)} \cdot \left(\frac{\varepsilon}{2}\right)^{\frac{\alpha}{\alpha-1}},$$
for any $\alpha \in (1, \infty]$.

Thus, there exists a distinguisher $\mathcal{A}'$ in Game_2 with run-time $T' = O\left(poly(m') \cdot \varepsilon_1(\mathcal{A})^{-2} \cdot T\right)$ and advantage $\varepsilon_2(\mathcal{A}') \geq \frac{\varepsilon_1(\mathcal{A})}{4R_\alpha(\Phi\|\Phi')} \cdot \left(\frac{\varepsilon_1(\mathcal{A})}{2}\right)^{\frac{\alpha}{\alpha-1}}$, where Φ and Φ' are the distribution of $\boldsymbol{r}$ in Game_1 and Game_2, respectively. The difference between the previous analysis [LPSS14] and our analysis is the value of α. Although Ling et al. fixed the value $\alpha = 2$, we *adaptively* optimize the order α. Since the $\boldsymbol{x}_i$'s are independent, and conditioning A, we have, from the multiplicativity property of the RD, $R_\alpha(\Phi\|\Phi') \leq \prod_{i\leq k} R_\alpha\left(D_{\Lambda^\perp(A),S,\boldsymbol{0}}\|D_{\Lambda^\perp(A),S,\boldsymbol{c}_i}\right)$. The latter can be bounded from above by applying Lemma 5. The condition of Lemma 5 holds since $\sigma_{m'}(S) \geq \omega\left(\sqrt{n}\right)$ holds; thus, if follows from the rejection step of the previous game that $\sigma_{m'}(S) \geq \eta_{2^{-n}}(A)$. This leads to $R_\alpha(\Phi\|\Phi') \leq \prod_{i\leq k} \exp\left(\frac{\alpha}{\alpha-1}2^{-n+2} + \alpha\pi\frac{\|\boldsymbol{c}_i\|^2}{\sigma_{m'}(S)^2}\right) \leq \prod_{i\leq k} \exp\left(\frac{\alpha}{\alpha-1}2^{-n+2} + \alpha\gamma\right) \leq \exp\left(k \cdot \left(\frac{\alpha}{\alpha-1}2^{-n+2} + \alpha\gamma\right)\right)$ from the condition $\sigma_{m'}(S) \geq \sqrt{\pi/\gamma} \cdot \|C\|$. Therefore, the advantage can be bounded from below by

$$\varepsilon_2(\mathcal{A}') \geq \frac{\varepsilon_1(\mathcal{A})}{4R_\alpha(\Phi\|\Phi')} \cdot \left(\frac{\varepsilon_1(\mathcal{A})}{2}\right)^{\frac{\alpha}{\alpha-1}} \geq \frac{(\varepsilon_1(\mathcal{A})/2)^{\frac{2\alpha-1}{\alpha-1}}}{4\exp\left(k \cdot \left(\frac{\alpha}{\alpha-1}2^{-n+2} + \alpha\pi\frac{\|C\|^2}{\sigma_{m'}(S)^2}\right)\right)}.$$

We optimize the value of α later.

Finally, as in [LPSS14], $\varepsilon_3(\mathcal{A}') \geq \varepsilon_2(\mathcal{A}') - 2^{-\Omega(n)}$ by Lemma 3. By definition, $\mathcal{A}'$ has advantage $\varepsilon_3(\mathcal{A}')$ against the (k, S, C)-LWE.

The above discussions lead to

$$\varepsilon \leq \exp\left(\frac{\alpha-1}{2\alpha-1}\ln\left(\varepsilon' + 2^{-\Omega(n)}\right) + k \cdot \frac{\alpha(\alpha-1)}{2\alpha-1}\gamma\right) \cdot 2^{O(k\cdot 2^{-n})} + 2^{-\Omega(n)}.$$

The right hand side of the inequality is bounded below by $\geq \exp\left(\frac{\ln\left(\varepsilon'+2^{-\Omega(n)}\right)}{2} + \frac{k\gamma\sqrt{-1-2\ln(\varepsilon'+2^{-\Omega(n)})/(k\gamma)}}{2}\right) \cdot 2^{O(k\cdot 2^{-n})} + 2^{-\Omega(n)}$, where the equality holds if and only if $\alpha = \left(1 + \sqrt{-1 - 2\ln\left(\varepsilon' + 2^{-\Omega(n)}\right)/(k\gamma)}\right)/2$. Then, we set the order and the above inequality becomes

$$\varepsilon \leq \exp\left(\frac{\ln\left(\varepsilon' + 2^{-\Omega(n)}\right)}{2} + \frac{k\gamma\sqrt{-1 - 2\ln(\varepsilon' + 2^{-\Omega(n)})/(k\gamma)}}{2}\right) \cdot 2^{O(k\cdot 2^{-n})} + 2^{-\Omega(n)}$$

as required. The order $\alpha = \left(1 + \sqrt{-1 - 2\ln\left(\varepsilon' + 2^{-\Omega(n)}\right)/(k\gamma)}\right)/2$ that we use satisfies $\alpha \in (1, +\infty]$ since $-\ln\left(\varepsilon' + 2^{-\Omega(n)}\right) \geq k\gamma$.

E Proofs of Lemma 8 and Theorem 5 in Section 5

Proof of Lemma 8. First, we show that given a matrix A for $\mathrm{SIS}_{\beta,m}$ in dimension n, then we can produce a matrix A' for (k, S, C)-$\mathrm{SIS}_{\beta',m+k}$ in dimension n with k hint vectors $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k$. The reduction is briefly written in [LPSS14].

Sample matrices $(X_1, X_2, U) \in \mathbb{Z}^{m\times k} \times \mathbb{Z}^{k\times k} \times \mathbb{Z}^{(m+k)\times(m+k)}$ using the following Lemma 10.

Lemma 10 (Theorem 17 of [LPSS15]) *Let $k \geq 100$ and $\sigma, \sigma' > 0$ satisfying $\sigma \geq \Omega(\sqrt{(m+k)k\log(m+k)}), m+k \geq \Omega(k\log(\sigma k))$ and $\sigma' \geq \Omega(k^{5/2}\sqrt{m+k}\sigma^2\log^{3/2}((m+k)\sigma))$. Let $k \geq n$ be bounded by $n^{O(1)}$ and $k < m$. There exists a ppt algorithm that given k and m (in unary), and σ and σ' as inputs, returns $(X_1, X_2, U) \in \mathbb{Z}^{m\times k} \times \mathbb{Z}^{k\times k} \times \mathbb{Z}^{(m+k)\times(m+k)}$ such that:*

- *the distribution of* (X_1, X_2) *is within the SD* $2^{-\Omega(k)}$ *of the distribution* $D_{\mathbb{Z},\sigma}^{m\times k} \times (D_{\mathbb{Z}^k,\sigma',\boldsymbol{\delta}_1} \times \cdots \times D_{\mathbb{Z}^k,\sigma',\boldsymbol{\delta}_k})^T$ *where* $\boldsymbol{\delta}_i$ *denotes the i-th canonical unit vector in* $\mathbb{Z}^k$ *whose i-th coordinate is* 1 *and whose remaining coordinates are* 0,
- *we have* $|\det U| = 1$ *and* $U \cdot (X_1 \| X_2) = (I_k \| 0)$,
- *every row of* U *has norm* $\leq O(\sqrt{km}\sigma')$, *with probability* $1 - 2^{\Omega(k)}$.

Define $\boldsymbol{x}_i$ as the i-th column of $(X_1\|X_2)$ for $i \leq k$. Let $V \in \mathbb{Z}^{m\times(m+k)}$ be the matrix consisting of the bottom m rows of U. Let $X \in \mathbb{Z}^{k\times(m+k)}$ be the matrix whose i-th row is $\boldsymbol{x}_i$ for all $i \leq k$. Compute $A' = V^T A$, and return (A', X). All steps of the reduction can be implemented in polynomial time. The following lemma shows that the output (A', X) can be used as (k, S, C)-SIS instances: A' is the (k, S, C)-SIS matrix and the rows of X are k hint vectors.

Lemma 11 (Lemma 19 of [LPSS15]) *The tuple* (A', X) *is within statistical distance* $2^{-\Omega(k)}$ *of the distribution in which* $A' \in \mathbb{Z}_q^{(m+k)\times n}$ *are uniform, and the rows of* $X \in \mathbb{Z}^{k\times(m+k)}$ *are from* $D_{\Lambda^\perp(A'),S,\boldsymbol{c}_i}$, *where* $\boldsymbol{c}_i = (\mathbf{0}^m|\boldsymbol{\delta}_i) \in \mathbb{R}^{m+k}$ *and* $\boldsymbol{\delta}_i$ *denotes the i-th canonical unit vector in* $\mathbb{Z}^k$ *for* $i = 1, \ldots, k$.

Let $\boldsymbol{b}' \in \mathbb{Z}^{m+k}$ be the solution to the (k, S, C)-$\mathrm{SIS}_{\beta',m+k}$ problem. Then, a vector $\boldsymbol{b} = V\boldsymbol{b}'$ can be used as a solution to the $\mathrm{SIS}_{\beta,m}$ problem, since $\boldsymbol{b}'^T \cdot A' = \boldsymbol{b}'^T \cdot V^T A = \boldsymbol{b}^T A = 0 \mod q$. Notice that $V\boldsymbol{b}' \neq 0$ since $\boldsymbol{b}'$ is linearly independent from the rows of X, and V is a basis of the lattice kerX. Furthermore, the following lemma bounds a norm of the solution $\|\boldsymbol{b}\|$.

Lemma 12 *Given the solution of the* (k, S, C)-$\mathrm{SIS}_{\beta',m+k}$ *problem for* (A', X) *defined above, the solution to the* $\mathrm{SIS}_{\beta,m}$ *problem can be computed for* A, *where* $\beta = \Omega(\sqrt{km}\sigma'\beta')$ *with probability* $\geq 1 - 2^{-\Omega(k)}$.

Proof. By Lemma 10, $\|V\| \leq O(\sqrt{km}\sigma')$ holds with probability $\geq 1 - 2^{-\Omega(k)}$. Therefore, $\|\boldsymbol{b}\| = \|V\boldsymbol{b}'\| \leq \Omega(\sqrt{km}\sigma'\beta')$. □

Hence, Lemma 8 is proved. □

Proof of Theorem 5. We consider the following sequence of games $\mathsf{Game}_0, \ldots, \mathsf{Game}_3$ as (k, S, C)-LWE to (k, S)-LWE reduction, where the distributions from the view of $\mathcal{A}$ differ among the games as follows:

- Game_0: The original (k, S)-SIS experiment. The adversary $\mathcal{A}$ receives an instance of the form $(A, \{\boldsymbol{x}_i\}_{i\leq k})$ with $A \leftarrow U\left(\mathbb{Z}_q^{m'\times n'}\right)$, and $\boldsymbol{x}_i \leftarrow D_{\Lambda^\perp(A),S,\boldsymbol{0}}$ for $i = 1, \ldots, k$.
- Game_1: Modification of Game_0 in that the distribution of A is the following rejection sampling: A is sampled uniformly from $\mathbb{Z}_q^{m'\times n'}$; however, reject and resample A if $\eta_{2^{-n}}(A) > 4q^{n'/m'}\sqrt{\log\left(2m'\left(1+2^n\right)\right)/\pi} = O(\sqrt{n})$.
- Game_2: Modification of Game_1 in that the distribution of the hint $\boldsymbol{x}_i$'s are from the non-zero centered distribution $D_{\Lambda^\perp(A),S,\boldsymbol{c}_i}$ (instead of the zero centered distribution $D_{\Lambda^\perp(A),S,\boldsymbol{0}}$).
- Game_3: Modification of Game_2 in that the distribution of A is $A \leftarrow U\left(\mathbb{Z}_q^{m'\times n'}\right)$. The instance distribution is identical to that of the (k, S, C)-LWE experiment.

Let $\varepsilon_i(\mathcal{A})$ for $i = 0, \ldots, 3$ denote the advantage of $\mathcal{A}$ fo find the correct k-SIS solution in Game_i. By definition, $\varepsilon_0(\mathcal{A}) = \varepsilon$. As in [LPSS14], $\varepsilon_1(\mathcal{A}) \geq \varepsilon_0(\mathcal{A}) - 2^{-\Omega(n)}$ by Lemma 3.

Let Φ and Φ' be the distributions of $\{\boldsymbol{x}_i\}_{i \leq k}$ in Game_1 and Game_2, respectively. $R_\alpha(\Phi \| \Phi') \leq \prod_{i \leq k} R_\alpha \left(D_{\Lambda^\perp(A), S, \boldsymbol{0}} \| D_{\Lambda^\perp(A), S, \boldsymbol{c}_i} \right)$. The latter can be bounded from above by applying Lemma 5. The condition of Lemma 5 holds since $\sigma_{m'}(S) \geq \omega(\sqrt{n})$; thus, by the rejection step of the previous game, it follows that $\sigma_{m'}(S) \geq \eta_{2^{-n}}(A)$. This leads to $R_\alpha(\Phi \| \Phi') \leq \prod_{i \leq k} \exp\left(\frac{\alpha}{\alpha - 1} 2^{-n+2} + \alpha\pi \frac{\|\boldsymbol{c}_i\|^2}{\sigma_{m'}(S)^2} \right) \leq \prod_{i \leq k} \exp\left(\frac{\alpha}{\alpha-1} 2^{-n+2} + \alpha\gamma \right) \leq \exp\left(k \cdot \left(\frac{\alpha}{\alpha-1} 2^{-n+2} + \alpha\gamma \right) \right)$ from the condition $\sigma_{m'}(S) \geq \sqrt{\pi/\gamma} \cdot \|C\|$. Therefore, the advantage can be bounded from below by $\varepsilon_2(\mathcal{A}') \geq \frac{\varepsilon_1(\mathcal{A})^{\frac{\alpha}{\alpha-1}}}{R_\alpha(\Phi \| \Phi')} \geq \frac{\varepsilon_1(\mathcal{A})^{\frac{\alpha}{\alpha-1}}}{\exp\left(k \cdot \left(\frac{\alpha}{\alpha-1} 2^{-n+2} + \alpha\gamma \right) \right)}$. We optimize the value of α at the end of the proof.

Finally, as in [LPSS14], $\varepsilon_3(\mathcal{A}') \geq \varepsilon_2(\mathcal{A}') - 2^{-\Omega(n)}$ by Lemma 3. By definition, $\varepsilon_3(\mathcal{A}') = \varepsilon'$.

The above discussion leads to

$$\varepsilon \leq \exp\left(\frac{\alpha - 1}{\alpha} \cdot \ln\left(\varepsilon' + 2^{-\Omega(n)} \right) + (\alpha - 1) \cdot k\gamma \right) \cdot 2^{O(k \cdot 2^{-n})} + 2^{-\Omega(n)}.$$

The inequality is equivalent to the inequality (1) in Section 1. The term $\exp(\cdot)$ on the RHS of the inequality is bounded below by $\exp\left(\ln\left(\varepsilon' + 2^{-\Omega(n)} \right) - k\gamma + \left(-\ln\left(\varepsilon' + 2^{-\Omega(n)} \right) / \alpha + \alpha \cdot k\gamma \right) \right) \geq \exp\left(\ln\left(\varepsilon' + 2^{-\Omega(n)} \right) - k\gamma + \sqrt{-\ln\left(\varepsilon' + 2^{-\Omega(n)} \right) \cdot k\gamma} \right)$ by the inequality of arithmetic mean and geometric mean, where the equality holds if and only if $-\ln\left(\varepsilon' + 2^{-\Omega(n)} \right) / \alpha = \alpha \cdot k\gamma$, i.e., $\alpha = \sqrt{\frac{-\ln\left(\varepsilon' + 2^{-\Omega(n)} \right)}{k\gamma}}$. Then, we set the order $\alpha = \sqrt{\frac{-\ln\left(\varepsilon' + 2^{-\Omega(n)} \right)}{k\gamma}}$ and the above inequality becomes

$$\varepsilon \leq \exp\left(-\left(\sqrt{-\ln\left(\varepsilon' + 2^{-\Omega(n)} \right)} - \sqrt{k\gamma} \right)^2 \right) \cdot 2^{O(k \cdot 2^{-n})} + 2^{-\Omega(n)}.$$

The inequality is equivalent to the inequality (2) in Section 1 as required. The order $\alpha = \sqrt{\frac{-\ln\left(\varepsilon' + 2^{-\Omega(n)} \right)}{k\gamma}}$ that we use satisfies $\alpha \in (1, +\infty]$ since $-\ln\left(\varepsilon' + 2^{-\Omega(n)} \right) \geq k\gamma$. □