Reducing an LWE Instance by Modular Hints and its Applications to Primal Attack, Dual Attack and BKW Attack

Han Wu[1,2], Xiaoyun Wang[1,2,3], and Guangwu Xu[1,2(✉)]

[1] School of Cyber Science and Technology, Shandong University, Qingdao 266237, Shandong, China
hanwu97@mail.sdu.edu.cn

[2] Key Laboratory of Cryptologic Technology and Information Security of Ministry of Education, Shandong University, Qingdao 266237, Shandong, China
gxu4sdq@sdu.edu.cn

[3] Institute for Advanced Study, Tsinghua University, Beijing 100084, China
xiaoyunwang@mail.tsinghua.edu.cn

Abstract. An emerging direction of investigating the resilience of post-quantum cryptosystems under side-channel attacks is to consider the situations where leaked information is combined with traditional attack methods in various forms. In CRYPTO 2020, Dachman-Soled et al. integrated hints from side-channel information to the primal attack against LWE schemes. This idea is further developed in this paper. An accurate characterization of the information from perfect hints and modular hints is obtained through the establishment of an interesting decomposition of $\mathbb{Z}^n$. It is observed that modular hints with modulus p produce some orthogonal projection of the secret in $\mathbb{Z}_p$, which is exactly an extension of the case of perfect hints in $\mathbb{R}$. Based on these, a new attack framework is described when some modular hints with modulus q are available. In this framework, an adversary first reduces the LWE instance using such hints, and then performs various attacks on the new instance. One of the key characters of our framework is that the dimension of the secret in the new instance always decreases under some moderate conditions. A comparison with the previous work shows that our approach is in some sense more essential and applicable to various kinds of attacks. The new way of integrating modular hints to primal attack improves the existing work. The first attempt of using modular hints in dual attack and BKW attack is also discussed in the paper and better analysis results are produced. Experiments have been carried out and shown that multiple modular hints with modulus q can indeed significantly reduce their attack costs. For examples, with just 100 hints, the blocksize can be reduced by 101 and the time complexity can be reduced by a factor of 2^{30} in both primal attack and dual attack against a Newhope1024 instance. As for the BKW attack, if 90 hints are available, the number of queries to the LWE oracle can be decreased by a factor of 2^{60}, as do the time complexity and memory complexity when attacking an instance of Regev cryptosystem $(384, 147457, 39.19)$.

1 Introduction

The establishment of secure and reliable post-quantum cryptosystems becomes an important and urgent task with the rapid advance of computing technology. If large-scale quantum computers are ever built, they will compromise the security of many commonly used cryptographic algorithms. At present, there are several post-quantum cryptosystems that have been proposed, including lattice-based cryptosystems, code-based cryptosystems, multivariate cryptosystems, and others. For them, further research is needed in order to gain more confidence in their security.

As we know, lattice-based cryptography has been widely received because of its post-quantum feature as well as superior performance. The underlying mathematical hard problem to support most lattice-based schemes is the so-called learning with error (LWE) problem (as well as its variants). In particular, in July 2022, the US National Institute of Standards and Technology (NIST) has identified four candidate algorithms for Post-Quantum Cryptography (PQC) standardization. The only public-key encryption/key-establishment algorithm that was selected – Kyber – is based on Module-LWE (MLWE).

So far, several strategies to analyze the concrete hardness of LWE have been suggested. Two major lattice attack algorithms – dual attack and primal attack – both transform the problem into searching short vectors in some lattice, and then solve it by lattice reduction algorithms. The fact that the number of available samples is restricted in practice makes them effective choices. An algebraic attack was proposed by Arora and Ge [10] in 2011, and further analyzed by [2] in 2015. Its essential idea is, solving LWE can be reduced to solving a system of (error-free) high-degree non-linear equations. As we know, in the lattice-based schemes, sometimes ciphertexts generated honestly using a valid public key may result in decryption failures under the corresponding private key. This property leads to the so-called decryption failure attack [16–18]. Furthermore, much work has been done on the combinatorial attack based on BKW (Blum, Kalai, Wasserman) algorithm. One of its advantages is that the complexity can be analyzed in a standard way. BKW strategy tends to give algorithms with the best performance for some important parameter choices. However, the need for large amounts of memory and LWE samples are possible drawbacks of it.

In addition to the above traditional attack methods, there is also a concern about whether physical effects caused by the operations of a cryptosystem (on the side) can provide useful extra information about the secret/error, see, for example, [1,8,12,21,31]. In 2020, Dachman-Soled et.al [15] initiated a study of using pieces of side-channel information about secret/error as "hints", and integrating them into the primal attack. This opens a new direction of mixing the theoretical-based lattice attack method and practical-based side-channel attack method to advance the cryptanalysis of LWE schemes. Moreover, in 2021, the idea of "hints" was brought to the coded-based schemes by Horlemann et al. [23].

The two main kinds of hints in [15] – perfect hints and modular hints – are both discussed in this paper, with the latter being our main focus. As we shall see later, perfect hints and modular hints with modulus p give information over different rings $\mathbb{R}$ and $\mathbb{Z}_p$ respectively. To further explore the information from modular hints, some mathematical concepts, such as the projection matrix and pseudo-inversion, are generalized from

$\mathbb{R}$ to $\mathbb{Z}_p$. An interesting decomposition of $\mathbb{Z}^n$ is formulated and proved under certain conditions that are satisfied with a probability no less than $\frac{\Phi(p)}{p}$, where $\Phi(\cdot)$ is the Euler's totient function. Based on these analytical tools, we find that modular hints with modulus p produce an orthogonal projection of the secret in $\mathbb{Z}_p$, which is an extension of the case of perfect hints in $\mathbb{R}$. This discovery indicates a greater potential of modular hints, especially for those with modulus q (the modulus parameter for LWE schemes).

It is mentioned in [15] that, in a primal attack, only perfect hints can be used to decrease the dimension of the lattice for searching short vectors. Modular hints just serve the purpose of changing its volume (provided that the hints are primitive). Instead of adding hints directly to the attack, in this paper, we take an approach to find a more essential way for the integration of hints. To be more precise, hints are firstly used to reduce the underlying LWE instance to a new one whose secret is of a lower dimension, and then various attacks can be performed against the new instance. What is noteworthy is that, in this way, not only perfect hints, but even modular hints with modulus q can always be used to reduce the dimension of the secret when certain conditions are satisfied. The changes in our approach are reflected by two aspects: (1) from the reduction of attacks to that of LWE instances, (2) from the improvement in parameters of the lattice to those of the secret. We believe that these changes make things more fundamental and information more fully utilized. As the distribution of the secret is critical in primal attack and dual attack, we use the Gaussian elimination method in [9] to transform the secret of the new instance into one that follows the error distribution. Even though some more (about n) samples are necessary for this case, these additional samples are always available in several schemes, such as Newhope1024 and LAC.

Various types of attacks can be executed directly against this new instance. The cases of dual attack, primal attack, and BKW attack are all analysed in this paper. For the primal attack, we make a comparison between the two methods of adding modular hints with modulus q in this paper and that in [15], some similarities as well as additional benefits are found. With some moderate conditions, the new primal attack we designed performs better than that in [15] except for the case when their attack attains the optimality. Even in that case, our approach is still at the same cost as their primal attack (with the best performance). To make this more clear, some situations where our attack method is more applicable are presented. We also provide a direction for adding modular hints with modulus q to dual attack and BKW attack. To the best of our knowledge, this is the first time that hints are integrated into these two types of attacks. It is worth mentioning that, the BKW attack seems to be particularly compatible with our framework due to its construction. To show this clearly and intuitively, the two methods of integrating hints to the BKW attack (use hints to directly optimize the BKW attack or reduce the instance first and then perform the BKW attack) are both described in detail.

For these three types of attacks, extensive experiments have been carried out. It is shown that multiple modular hints with modulus q can indeed significantly reduce their attack costs. For examples, with just 100 hints, the BKZ blocksize can be reduced by 101 and the time complexity can be reduced by a factor of 2^{30} in both primal attack and dual attack against a Newhope1024 instance. As for the BKW attack, if 90 hints are available, the number of queries required to the LWE oracle can be decreased by

a factor of 2^{60}, as do the time complexity and memory complexity when attacking a Regev cryptosystem $(384, 147457, 39.19)$ instance.

The paper is organized into 6 sections. Necessary mathematical background and useful algorithms are given in Section 2. In Section 3, we give an interesting decomposition of $\mathbb{Z}^n$. Based on this, an accurate characterization of the information about the secret leaked from perfect hints and modular hints is presented and we show how to directly reduce the LWE instance by modular hints with modulus q. This implies a new attack framework in which the LWE instance is first reduced by hints and then attacked. The specific description of lattice attacks (including primal attack and dual attack) in this framework is provided in Section 4, while BKW attack is analysed in Section 5. For comparison, the BKW attack with or without our framework are both discussed. Experiments with these three attacks are conducted and the corresponding experimental results are shown in Section 6.

2 Preliminaries

In this section, we provide necessary preparations for the discussion of integration of hints to the LWE instance. For a distribution D, let $x \leftarrow D$ represent x is sampled according to D. We use $U(X)$ to denote the uniform distribution over X for any set X. f_x denotes the pdf (or pmf) of x, where x is an arbitrary random variable or random vector. Moreover, we write $L(B)$ as the lattice generated by matrix B. For any matrix A, we denote the submatrix formed by its i-th to j-th rows by $A_{[i:j]}$. And $v_{[i:j]}$ represents the subvector that contains the i-th to the j-th entries of some vector v. For a vector $x \in \mathbb{R}^m$ and a subspace $V \subseteq \mathbb{R}^m$, x_V is the orthogonal projection of x onto V.

2.1 Statistics

The normal (or Gaussian) distribution is one of the most famous distributions in statistics. Its finite discrete version is especially important in cryptography, as in actual LWE schemes, the entries of the secret and error are usually selected from $\mathbb{Z}_q$ according to the discrete Gaussian distribution. The following is the definition of Gaussian distribution.

Definition 1. *Let d be a positive integer. For $\mu \in \mathbb{R}^d$ and a symmetric matrix $\Sigma \in \mathbb{R}^{d\times d}$, we denote $G_{d,q}(\mu, \Sigma)$ to be the (discrete) multivariate normal distribution derived from the (continuous) multivariate normal distribution $N_d(\mu, \Sigma)$ with the probability mass function (pmf) being*

$$g^{d,q}_{\mu,\Sigma}(x) = \frac{\sum_{t\in\mathbb{Z}^d} f^d_{\mu,\Sigma}(x + tq)}{f^d_{\mu,\Sigma}(\mathbb{Z}^d)}, \quad x \in \mathbb{Z}^d_q,$$

where $f^d_{\mu,\Sigma}$ is the probability density function (pdf) of $N_d(\mu, \Sigma)$, i.e.

$$f^d_{\mu,\Sigma}(x) = \begin{cases} \frac{1}{(2\pi)^{\frac{r}{2}}\cdot\sqrt{rdet(\Sigma)}} \cdot e^{-\frac{1}{2}(x-\mu)^T\Sigma^{\sim}(x-\mu)}, & x \in \mu + Span(\Sigma) \\ 0, & else \end{cases}.$$

Some properties of the normal distribution will be used in our subsequent analysis.

Lemma 1. *Let k, d be two positive integers. Let $x \sim N_d(\mu_x, \Sigma_x)$ be a random vector. Given $A \in \mathbb{R}^{k\times d}$. Then $Ax \sim N_k(A\mu_x, A\Sigma_x A^T)$.*

Lemma 2. *Let $k < d$ be two positive integers. Let $x \sim N_d(\mu_x, \Sigma_x)$ be a random vector. For a matrix $M \in \mathbb{R}^{k\times d}$ of rank k and a random vector $g \sim N_k(0, \Sigma_g)$, we denote $y = Mx + g$. Then the conditional multivariate normal distribution $(x|y)$ also follows a multivariate normal distribution $N_d(\mu_{x|y}, \Sigma_{x|y})$, where*

$$\begin{cases} \mu_{x|y} = \mu_x + \Sigma_x M^T (M\Sigma_x M^T + \Sigma_g)^{-1}(y - M\mu_x) \\ \Sigma_{x|y} = \Sigma_x - \Sigma_x M^T (M\Sigma_x M^T + \Sigma_g)^{-1} M\Sigma_x \end{cases}.$$

Recall that the *discrete Fourier transform* of a function $f : \mathbb{Z}_q \to \mathbb{C}$ is given by $\widehat{f}(y) = \sum_{x\in\mathbb{Z}_q} e^{\frac{-2\pi i x\cdot y}{q}} \cdot f(x), \ \ \forall y \in \mathbb{Z}_q$. The following lemma on discrete Fourier transform will be useful in our later discussion.

Lemma 3. *([34]) Given two positive integers d, q. Let $x \sim G_{d,q}\left(0, \sigma^2 I_d\right)$ be a random vector. For any $v \in \mathbb{Z}_q^d$, we denote the pmf of (the random variable over $\mathbb{Z}_q$) $\langle v, x\rangle \pmod q$ by $f_{\langle v,x\rangle}$, then $\widehat{f_{\langle v,x\rangle}}(1) \geq e^{-\frac{2\pi^2\sigma^2\|v\|^2}{q^2}}$.*

The Chernoff-Hoeffding inequality is a powerful tool for distinguish attacks.

Lemma 4. *Let $\xi_1, \cdots, \xi_M$ be real-valued independent bounded random variables with $\xi_j \in [c, d]$ and $E[\xi_j] = \mu_j,\ j = 1, 2, \cdots, M$. Then for any $\epsilon \geq 0$,*

$$Pr\left[\left|\frac{1}{M}\sum_{j=1}^{M}(\xi_j - \mu_j)\right| \geq \epsilon\right] \leq 2\cdot e^{-\frac{2M\epsilon^2}{(d-c)^2}}.$$

In cryptanalysis, the so-called *bias* is often used in conjunction with it. The definition is as follows. Let ϕ be a pmf over $\mathbb{Z}_q$, then its *bias* is defined as $\mathbf{B}(\phi) = \mathbb{E}_{x\sim\phi}\left[e^{-\frac{2\pi i x}{q}}\right]$, i.e. $\mathbf{B}(\phi) = \widehat{\phi}(1)$. Hence, for two pmfs ϕ_{j1}, ϕ_{j2} and a given $x_j \in \mathbb{Z}_q$, the fact that the value of $e^{-\frac{2\pi i x_j}{q}}$ is closer to $\widehat{\phi_{j1}}(1)$ or $\widehat{\phi_{j2}}(1)$ is useful to the adversary for distinguishing between $f_{x_j} = \phi_{j1}$ and $f_{x_j} = \phi_{j2}$. As the number of j increases, so does the attacker's success rate. The *distinguish advantage* is relevant to the difference between $\widehat{\phi_{j1}}(1)$ and $\widehat{\phi_{j2}}(1)$, and the number of samples required can be estimated by the Chernoff-Hoeffding inequality.

2.2 Algebra

One should notice that, we can regard perfect hints and modular hints with modulus p as giving information about the secret and/or error over different rings $\mathbb{R}$ and $\mathbb{Z}_p$ respectively. So the analysis tools should be adapted accordingly to fit these two scenarios.

The *inverse* of a matrix is important in our analysis. As we know, the *adjoint matrix* is often used to describe the inverse in $\mathbb{R}$. This provides a natural way to extend the concepts to an arbitrary commutative ring $\mathscr{R}$. In fact, any $d \times d$ matrix A over $\mathscr{R}$ satisfies

$$A^* \cdot A = \det(A) I_d,$$

where A^* is the adjoint matrix of A in $\mathscr{R}$. Hence, for a positive integer p, a matrix $A \in \mathbb{Z}_p^{d\times d}$ is invertible in $\mathbb{Z}_p$ if and only if $\det(A)$ is invertible in $\mathbb{Z}_p$. If we treat $\det(A)$ as an integer, this means that $\gcd(\det(A), p) = 1$ and the inverse of A is $A_p^{-1} = (\det(A))_p^{-1} \cdot A^* \pmod p$, where $(\det(A))_p^{-1}$ is the modular inverse of $\det(A) \pmod p$.

Integrating hints always results in a situation that leads to the substitution of pseudo-inverse for inverse. As we know, the definition of *pseudo-inverse* comes from the *orthogonal projection matrix*. Let $\Psi \in \mathbb{R}^{d\times k}$ $(k \le d)$ be a matrix of rank k and $F = \text{Span}(\Psi)$. We denote the *orthogonal projection matrix* onto F by $\Pi_\Psi (= \Pi_F) = \Psi \cdot (\Psi^T\Psi)^{-1} \cdot \Psi^T$, and its complement by $\Pi_\Psi^\perp (= \Pi_F^\perp) = I - \Pi_F$. Then the *pseudo-inverse* of Ψ is defined as $\Psi^\sim = (\Psi^T\Psi)^{-1}\Psi^T$. It is easy to see that $\Psi^\sim \cdot \Psi = I_k$ and $\Psi \cdot \Psi^\sim = \Pi_\Psi$. These analysis tools are also generalized to $\mathbb{Z}_p$.

Definition 2. *Let p and $k \le d$ be positive integers. For any matrix $A \in \mathbb{Z}_p^{k\times d}$, we define*

$$\begin{cases} \Lambda_p^\perp(A) = \{x \in \mathbb{Z}^d : Ax = 0 \pmod p\} \\ \Lambda_p(A) = \{x \in \mathbb{Z}^d : x = A^T\xi \pmod p \text{ for some } \xi \in \mathbb{Z}_p^k\} \end{cases}$$

Definition 3. *Let p and $k \le d$ be positive integers. For any matrix $A \in \mathbb{Z}_p^{d\times k}$ that satisfies $\gcd(\det(A^TA), p) = 1$, we define the orthogonal projection matrix onto $\Lambda_p(A^T)$ with respect to $\mathbb{Z}_p$ as*

$$(\Pi_A)_p = A(A^TA)_p^{-1}A^T \pmod p,$$

and its pseudo-inverse as

$$A_p^\sim = (A^TA)_p^{-1}A^T \pmod p.$$

It can be proven that the projection matrix and pseudo-inverse with respect to $\mathbb{Z}_p$ satisfy some properties similar to those in $\mathbb{R}$. For example, $A_p^\sim \cdot A = I_k \pmod p$ and $A \cdot A_p^\sim = (\Pi_A)_p \pmod p$. Moreover, we have the following proposition whose proof is given in appendix A.

Proposition 1. *Let p and $k \le d$ be positive integers. For a matrix $A \in \mathbb{Z}_p^{d\times k}$ that satisfies $\gcd\left(\det(A^TA), p\right) = 1$, we have*

$$\begin{cases} (\Pi_A)_p \cdot z \equiv z \pmod p & \text{for any } z \in \Lambda_p(A^T) \\ (\Pi_A)_p \cdot y \equiv 0 \pmod p & \text{for any } y \in \Lambda_p^\perp(A^T) \end{cases}.$$

In some sense, $\Lambda_p(A^T)$ and $\Lambda_p^\perp(A^T)$ can be viewed as projection spaces with respect to $\mathbb{Z}_p$ that are orthogonal to each other. Their volume can be predicted as follows.

Lemma 5. *Let p and $k \le d$ be positive integers. If $A \in \mathbb{Z}_p^{k\times d}$ is chosen uniformly at random, i.e. $A \leftarrow U\left(\mathbb{Z}_p^{k\times d}\right)$, then*

$$Pr\left[vol\left(\Lambda_p^\perp(A)\right) = p^k\right] = Pr\left[vol(\Lambda_p(A)) = p^{d-k}\right] \ge 1 - \frac{1}{p^{d-k}}.$$

2.3 Lattices

The learning with error (LWE) problem has been the most popular choice for constructing cryptographic schemes. In the original definition of LWE [33], the secret is uniformly and randomly selected. In 2009, Applebaum et.al [9] showed that sampling the secret by the error distribution does not lose security. Besides, they proposed a way of transforming the distribution of the secret to be that of the error through Gaussian elimination. Hence, in practice, several schemes use this strategy to improve efficiency, such as NIST PQC algorithms Kyber [11], Newhope [6] and LAC [27]. In this paper, we also focus on this case, which is referred to as LWE in Hermite Normal Form (HNF).

Definition 4. *For positive integers n, m, q, let χ be a distribution over $\mathbb{Z}_q$ with a mean of 0 and a small standard deviation of σ_χ, then the Search-LWE (in HNF) with parameters (m, n, q, χ) is to find the secret $s \in \mathbb{Z}_q^n$, when given the pair*

$$(A, b = As + e \,(\mathrm{mod} q)) \in \mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m, \text{ where } A \leftarrow U(\mathbb{Z}_q^{m\times n}),\ s \leftarrow \chi^n,\ e \leftarrow \chi^m.$$

And the Decision-LWE (in HNF) with parameters (m, n, q, χ) is to distinguish pair

$$(A, b \leftarrow U\left(\mathbb{Z}_q^m\right)) \text{ and } (A, b = As + e \,(\mathrm{mod}\ q)), \text{ where } A \leftarrow U(\mathbb{Z}_q^{m\times n}), s \leftarrow \chi^n,\ e \leftarrow \chi^m.$$

The secret-noise transformation For any LWE instance $(A, b = As + e \pmod q) \in \mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m$, where $s \in \mathbb{Z}_q^n$ and $e \leftarrow \chi^m$, it can be transformed into another instance in HNF by using some additional samples. Suppose that other n samples $\overline{b} = \overline{A}s + \overline{e} \pmod q$ are available, where $\overline{e} \leftarrow \chi^n, \overline{A} \leftarrow \mathbb{Z}_q^{n\times n}$ and $\overline{A}$ is invertible in $\mathbb{Z}_q$[4]. We denote $A' = -A \cdot (\overline{A})_q^{-1} \pmod q$, $s' = \overline{e}$ and $b' = b + A'\overline{b} \pmod q$, then $(A', b' = A's' + e \pmod q) \in \mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m$ is an LWE instance in HNF.

As we know, the *volume* of a lattice Λ with a basis B is defined as $\mathrm{vol}(\Lambda) = \sqrt{\det(B^T B)}$ and its *dual lattice* is $\Lambda^* = \left\{y \in \mathrm{Span}(B) \middle| \forall x \in \Lambda, \langle x, y\rangle \in \mathbb{Z}\right\}$. There are some interesting properties between Λ and Λ^*. For example, if B is a basis of Λ, then its *dual matrix* $B^{\sim T}$ is a basis of Λ^*. Thus, $vol(\Lambda) = \frac{1}{vol(\Lambda^*)}$. Moreover, when considering projecting a lattice onto some subspace, we have the following lemma.

Lemma 6. *[29, Proposition 1.3.4] Let $\Lambda \subseteq \mathbb{R}^d$ be a lattice and F be a subspace of $\mathbb{R}^d$, then $(\Lambda \cap F)^* = \Pi_F \cdot \Lambda$.*

Recall that the column vectors of $\Psi = (\psi_1\ \cdots\ \psi_t)$ are said a set of *primitive vectors* with respect to Λ if they can be extended to a basis of Λ, i.e. $\Lambda \cap \mathrm{Span}(\Psi) = L(\Psi)$. The volume of the above intersection lattice is predictable when certain primitiveness conditions are satisfied. The following is a natural extension of the Lemma 12 in [15] and its proof is given in appendix B.

Lemma 7. *Given a lattice Λ. Suppose that $\Psi = (\psi_1\ \cdots\ \psi_t)$ contains linearly independent vectors of Λ^*. If $\{\psi_j\}_{j=1}^t$ is a set of primitive vectors of Λ^*, then $\Lambda \cap Span(\Psi)^\perp$ is a lattice of volume $\sqrt{\det(\Psi^T\Psi)} \cdot vol(\Lambda)$.*

[4] As done in [9], we can use $\frac{\Phi(q)}{q}$ to estimate the probability that $\overline{A}$ is invertible in $\mathbb{Z}_q$. More than n additional samples allow such $\overline{A}$ to be constructed with a high probability.

Shortest vector problem (SVP) is a fundamental problem surrounding lattice-based cryptography. The instances of other lattice hard problems can usually be transformed to those of it and solved by lattice reduction algorithms. We introduce two lattice reduction algorithms here. The first one is the LLL algorithm, which was proposed by Lenstra et al. [25] in 1982, is the first polynomial-time reduction algorithm. When given a lattice basis as input, the algorithm outputs another basis with better orthogonality. The first vector of the LLL output is a relatively short lattice vector. It is worth noting that, in the original LLL, the input must consist of linearly independent vectors. This limitation was overcome by Pohst [32] in 1987. A modification of the LLL algorithm named the MLLL algorithm was presented, whose input range was extended to a set of spanning vectors. The second lattice reduction algorithm we need is the BKZ algorithm with sieving as the SVP oracle. This algorithm is generally regarded as the most common and efficient choice. There is a blocksize parameter β in it, which determines both the quality of the output vectors and the complexity of the algorithm. The following heuristic assumptions are often used for the analysis of BKZ.

Assumption 1 *For a d-dimensional lattice Λ, given any of its basis as input, BKZ algorithm with blocksize β provides $2^{0.2075\beta}$ short vectors in one run when using sieving as the SVP oracle, whose norms are all close to $\delta_0(\beta)^d \cdot vol(\Lambda)^{\frac{1}{d}}$.*

The above $\delta_0(\beta)$ is referred to as the *Hermite factor*. For a β that is not too small (for example, $\beta \geq 50$), $\delta_0(\beta)$ is predictable by the following heuristic.

Heuristic 1 *([14]) BKZ with blocksize $\beta(\beta \geq 50)$ achieves Hermite factor*

$$\delta_0(\beta) \approx \left(\frac{\beta}{2\pi e}(\pi\beta)^{\frac{1}{\beta}}\right)^{\frac{1}{2(\beta-1)}}.$$

The cost of BKZ also depends on β. In particular, an acceleration in the search process of BKZ could be achieved in the quantum case.

Assumption 2 *When using sieving as the SVP oracle, the runtime of BKZ-β is*

$$T_{BKZ}(\beta) = \begin{cases} 2^{0.292\beta} & \textit{classical case} \\ 2^{0.265\beta} & \textit{quantum case} \end{cases}.$$

As we shall see, for a given lattice Λ, using a larger β in BKZ could lead to finding shorter lattice vectors, but also with a greater cost. Therefore, provided that the shortest non-zero vector in Λ can be found, the strategy for selecting β is to choose β as small as possible, i.e., the smallest β satisfies equation (1) or (2) in the following assumption.

Assumption 3 *([5, 7]) Given a lattice Λ, the shortest non-zero vector ξ in it can be found by BKZ-β, if*

$$\sqrt{\frac{\beta}{dim(\Lambda)}} \cdot \|\xi\| \leq (\delta_0(\beta))^{2\beta - dim(\Lambda) - 1} \cdot vol(\Lambda)^{\frac{1}{dim(\Lambda)}}. \tag{1}$$

In particular, if we approximate $\|\xi\|$ to be $\sigma_\xi \cdot \sqrt{dim(\Lambda)}$, where σ_ξ is the standard deviation of the distribution that ξ follows, then equation (1) can be simplified to

$$\sqrt{\beta} \cdot \sigma_\xi \leq (\delta_0(\beta))^{2\beta - dim(\Lambda) - 1} \cdot vol(\Lambda)^{\frac{1}{dim(\Lambda)}}. \tag{2}$$

3 Reducing the LWE Instance by Hints

The purpose of this section is to build necessary mathematical tools for characterizing the integration of hints. A useful decomposition of $\mathbb{Z}^n$ is given in Section 3.1. Based on that, we accurately characterize the information about the secret brought by perfect hints as well as modular hints in Section 3.2. It is interesting to note that modular hints with modulus p imply an orthogonal projection of the secret in $\mathbb{Z}_p$, which is exactly an extension of the case of perfect hints in $\mathbb{R}$. As the original LWE samples are all based on $\mathbb{Z}_q$, it is of special interest to work with modular hints for modulus q to be better compatible and to gain more useful information. We find that such hints play an important role in reducing the LWE instance to another one whose secret is of a lower dimension when certain conditions are met. A detailed process is given in Section 3.3.

3.1 A useful decomposition of $\mathbb{Z}^n$

For an LWE instance $(A, b = As + e \pmod q) \in \mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m$, suppose that $t(t < n)$ linearly independent perfect (modular) hints of s are available and they are expressed in a matrix form as

$$Y^T s = R \quad \left(\text{ or } \quad Y^T s = R \pmod p\right),$$

where $Y \in \mathbb{Z}^{n\times t}, R \in \mathbb{Z}^t$ (or $Y \in \mathbb{Z}_p^{n\times t}, R \in \mathbb{Z}_p^t, p \in \mathbb{N}^+$). We call Y a *hint description matrix* and p the *modulus* of hints.

Let $\mathscr{V} = \text{Span}(Y)$. We define the lattice $\mathscr{L} = \mathbb{Z}^n \cap \mathscr{V}$. It is a t-dimensional integer lattice and from lemma 6, $\Pi_{\mathscr{V}} \cdot \mathbb{Z}^n$ is its dual lattice. According to [15], a basis $\mathtt{B}$ of $\mathscr{L}$ can be calculated as follows:

1. Take the column vectors of $\Pi_{\mathscr{V}} \cdot I_n$ as input to the MLLL algorithm and get a basis $\mathtt{B}^{\sim T}$ of $\Pi_{\mathscr{V}} \cdot \mathbb{Z}^n$.
2. Compute the dual matrix of $\mathtt{B}^{\sim T}$ and obtain a basis $\mathtt{B}$ of $\mathscr{L}$.

Similarly, we define the $(n-t)$-dimensional integer lattice $\mathscr{G} = \mathbb{Z}^n \cap \mathscr{V}^\perp$ and use the MLLL algorithm to obtain a basis $\mathtt{D}$ of it. It is easy to see that $\mathtt{B}^T\mathtt{D} = O_{t\times(n-t)}$ and $\mathtt{D}^T\mathtt{B} = O_{(n-t)\times t}$. Some other properties of $\mathtt{B}$ and $\mathtt{D}$ can also be given.

Proposition 2. $\mathtt{B}$, $\mathtt{D}$ *are both primitive vector sets of* $\mathbb{Z}^n$.

Proof. Since $L(\mathtt{B}) = \mathscr{L} = \mathbb{Z}^n \cap V = \mathbb{Z}^n \cap \text{Span}(\mathtt{B})$, we know that $\mathtt{B}$ is a set of primitive vectors of $\mathbb{Z}^n$. The proof for $\mathtt{D}$ is similar. □

Proposition 3. $\det(\mathtt{B}^T\mathtt{B}) = \det(\mathtt{D}^T\mathtt{D})$, *i.e.* $vol(\mathscr{L}) = vol(\mathscr{G})$.

Proof. Because $\mathtt{B}$ is a set of primitive vectors of $\mathbb{Z}^n$ and $\mathscr{G} = \mathbb{Z}^n \cap \text{Span}(\mathtt{B})^\perp$, from proposition 7, we have

$$\sqrt{\det(\mathtt{D}^T\mathtt{D})} = \text{vol}(\mathscr{G}) = \sqrt{\det(\mathtt{B}^T\mathtt{B})} \cdot \text{vol}(\mathbb{Z}^n) = \sqrt{\det(\mathtt{B}^T\mathtt{B})}. \qquad \square$$

Almost all of our subsequent analysis is based on the following theorem.

Theorem 1. *For a positive integer p, the decomposition of $\mathbb{Z}^n$:*

$$\mathbb{Z}^n = \mathscr{L} + \mathscr{G} + p\mathbb{Z}^n \tag{3}$$

holds if $\gcd(\det(\mathtt{B}^T\mathtt{B}), p) = 1$. *In particular, if we regard* $\det(\mathtt{B}^T\mathtt{B})$ *as a uniformly random positive integer, i.e.* $\det(\mathtt{B}^T\mathtt{B}) \leftarrow U(\mathbb{N}^+)$, *then equation (3) is true with a probability no less than* $\frac{\Phi(p)}{p}$, *where* $\Phi(\cdot)$ *is the Euler's totient function.*

Proof. As $(\mathtt{B}\ \mathtt{D})$ is a basis of $\mathscr{L} + \mathscr{G}$ and $\mathrm{Span}(\mathtt{B}\ \mathtt{D}) = \mathbb{R}^n$, $\mathscr{L} + \mathscr{G}$ is a sublattice of $\mathbb{Z}^n$ of full dimension. It should be noted that, there must be some positive integer c such that $c\mathbb{Z}^n \subseteq \mathscr{L} + \mathscr{G}$. In fact, for any $c \in \mathbb{N}^+$, this is true if and only if cI_n can be linearly represented by $(\mathtt{B}\ \mathtt{D})$ with integer coefficients [5], i.e.

$$c\mathbb{Z}^n \subseteq \mathscr{L} + \mathscr{G} \iff c \cdot (\mathtt{B}\ \mathtt{D})^{-1} \in \mathbb{Z}^{n\times n},$$

and it is easy to verify that the inverse of $(\mathtt{B}\ \mathtt{D})$ is:

$$(\mathtt{B}\ \mathtt{D})^{-1} = \begin{pmatrix} \mathtt{B}^{\sim} \\ \mathtt{D}^{\sim} \end{pmatrix} = \begin{pmatrix} (\mathtt{B}^T\mathtt{B})^{-1}\mathtt{B}^T \\ (\mathtt{D}^T\mathtt{D})^{-1}\mathtt{D}^T \end{pmatrix}.$$

Since $\mathtt{B}$ and $\mathtt{D}$ are both integer matrices, it is easy to see that if $c(\mathtt{B}^T\mathtt{B})^{-1} \in \mathbb{Z}^{t\times t}$ and $c(\mathtt{D}^T\mathtt{D})^{-1} \in \mathbb{Z}^{(n-t)\times(n-t)}$, then $c\mathbb{Z}^n \subseteq \mathscr{L} + \mathscr{G}$. Actually, we can take $c = \det(\mathtt{B}^T\mathtt{B})$. On the one hand, $\det(\mathtt{B}^T\mathtt{B}) \cdot (\mathtt{B}^T\mathtt{B})^{-1} = (\mathtt{B}^T\mathtt{B})^* \in \mathbb{Z}^{t\times t}$, where $(\mathtt{B}^T\mathtt{B})^*$ is the adjoint matrix of $\mathtt{B}^T\mathtt{B}$. On the other hand, according to proposition 3, $\det(\mathtt{B}^T\mathtt{B}) \cdot (\mathtt{D}^T\mathtt{D})^{-1} = \det(\mathtt{D}^T\mathtt{D}) \cdot (\mathtt{D}^T\mathtt{D})^{-1} = (\mathtt{D}^T\mathtt{D})^*$ is also an integer matrix. To sum up, we have

$$\det(\mathtt{B}^T\mathtt{B}) \cdot \mathbb{Z}^n \subseteq \mathscr{L} + \mathscr{G}.$$

The point here is that, if $\gcd(\det(\mathtt{B}^T\mathtt{B}), p) = 1$, then there are integers u, v, such that $u\det(\mathtt{B}^T\mathtt{B}) + vp = 1$. Hence,

$$\mathbb{Z}^n = \big(u\det(\mathtt{B}^T\mathtt{B}) + vp\big)\mathbb{Z}^n \subseteq \det(\mathtt{B}^T\mathtt{B})\mathbb{Z}^n + p\mathbb{Z}^n \subseteq \mathscr{L} + \mathscr{G} + p\mathbb{Z}^n.$$

Because $\mathscr{L}, \mathscr{G}, p\mathbb{Z}^n$ are all integer lattice, $\mathscr{L}+\mathscr{G}+p\mathbb{Z}^n \subseteq \mathbb{Z}^n$, then $\mathbb{Z}^n = \mathscr{L}+\mathscr{G}+p\mathbb{Z}^n$. In particular, if we think that $\det(\mathtt{B}^T\mathtt{B}) \leftarrow U(\mathbb{N}^+)$, then equation (3) holds with a probability no less than

$$\Pr\big[a \leftarrow U(\mathbb{Z}^d); \gcd(a, p) = 1\big] = \Pr\big[a \leftarrow U(\mathbb{Z}_q^d); \gcd(a, p) = 1\big] = \frac{\Phi(p)}{p}. \quad \square$$

To further figure out the magnitude of $\frac{\Phi(p)}{p}$, suppose that the prime factorization of p is $p = \prod_{j=1}^{k} p_j^{l_j}$, where $p_1 < p_2 < \cdots < p_k$ are primes and $l_j \in \mathbb{N}^+, j = 1, 2, \cdots, k$. Then from Euler's product formula, we have $\frac{\Phi(p)}{p} = \prod_{j=1}^{k}\left(1 - \frac{1}{p_j}\right)$. In the following, we mainly consider the case where p is a large prime or p is a power of 2, so the probability of equation (3) being true is always big enough.

[5] See also in [28, Theorem 2.1].

Remark 1. It is easy to see that $(\mathtt{B}\ \mathtt{D})$ is a basis of $\mathbb{R}^n$. However, it may not be a basis of $\mathbb{Z}^n$ due to the lack of primitiveness. Theorem 1 implies that, with a certain probability, all vectors in $\mathbb{Z}^n$ can be expressed by $(\mathtt{B}\ \mathtt{D})$ in the sense of "$\bmod p$".

There are some other representations of the decomposition in equation (3). In fact, since $\mathscr{L} + p\mathbb{Z}^n = \Lambda_p(\mathtt{B}^T) \subseteq \Lambda_p^{\perp}(\mathtt{D}^T)$ and $\mathscr{G} + p\mathbb{Z}^n = \Lambda_p(\mathtt{D}^T) \subseteq \Lambda_p^{\perp}(\mathtt{B}^T)$, two other decompositions of $\mathbb{Z}^n$ can also be obtained.

Corollary 1. *For a positive integer p, if* $\gcd\left(\det(\mathtt{B}^T\mathtt{B}), p\right) = 1$*, then*

$$\begin{cases} \mathbb{Z}^n = \Lambda_p(\mathtt{B}^T) + \Lambda_p(\mathtt{D}^T) + p\mathbb{Z}^n \\ \mathbb{Z}^n = \Lambda_p^{\perp}(\mathtt{B}^T) + \Lambda_p^{\perp}(\mathtt{D}^T) + p\mathbb{Z}^n \end{cases}.$$

The following propositions also hold when $\gcd\left(\det(\mathtt{B}^T\mathtt{B}), p\right) = 1$, their proofs can be seen in appendix C and appendix D respectively.

Proposition 4. *For a positive integer p, if* $\gcd\left(\det(\mathtt{B}^T\mathtt{B}), p\right) = 1$*, then*

$$\Lambda_p(\mathtt{D}^T) = \Lambda_p^{\perp}(\mathtt{B}^T) \ \textit{and}\ \ \Lambda_p(\mathtt{B}^T) = \Lambda_p^{\perp}(\mathtt{D}^T).$$

Proposition 5. *For a positive integer p, if* $\gcd\left(\det(\mathtt{B}^T\mathtt{B}), p\right) = 1$*, then*

$$(\Pi_{\mathtt{B}})_p + (\Pi_{\mathtt{D}})_p = I_n \pmod p.$$

3.2 The information from hints

In this subsection, we describe an accurate characterization of the information brought by perfect hints and modular hints. The case of perfect hints is relatively easy. In fact, hints $Y^T s = R$ give $s_{\mathscr{V}}$, i.e. the orthogonal projection of s onto the subspace $\mathscr{V}$. According to lemma 2, with hints $Y^T s = R$, the distribution $s \sim G_{n,q}\left(0, \sigma_\chi^2 I_n\right)$ becomes $\left(s \middle| Y^T s = R\right) \sim G_{n,q}\left(s_{\mathscr{V}}, \sigma_\chi^2 \Pi_{\mathscr{V}}^{\perp}\right)$ [6]. One can directly calculate

$$s_{\mathscr{V}} = \Pi_{\mathscr{V}} \cdot s = Y(Y^TY)^{-1}Y^Ts = Y(Y^TY)^{-1}R.$$

Next, we discuss what the modular hints $Y^T s = R \pmod p$ can tell us about s. It should be noted that, our analysis is based on the assumption that $\gcd(\det(\mathtt{B}^T\mathtt{B}), p) = 1$, i.e. the decomposition of $\mathbb{Z}^n$ in equation (3) is true. Then s can be decomposed into

$$s = x_s + y_s + pu_s = \mathtt{B}w_s + \mathtt{D}v_s + pu_s,$$

where $x_s \in \mathscr{L}, y_s \in \mathscr{G}, u_s \in \mathbb{Z}^n$. It is easy to see that this decomposition is not unique and we can always require $w_s \in \mathbb{Z}_p^t, v_s \in \mathbb{Z}_p^{n-t}$.

[6] It is a widely used analytical means to inherit the properties of the continuous case to the discrete case. From lemma 2, the conditional distribution of a (continuous) multivariate normal distribution is still a (continuous) multivariate normal distribution. So here we assume that the conditional distribution of the secret after adding hints is still a discrete normal distribution. We still use lemma 2 to calculate the mean and covariance matrix.

In the following, we shall show that, x_s (or $x_s \pmod p$) is exactly the information given by modular hints with modulus p. Firstly, we transform the hint description matrix from Y to $\mathtt{B}$, as the latter is a set of primitive vectors of $\mathbb{Z}^n$. To be specific, as $Y \subseteq \mathscr{L}$, it can be expressed as $Y = \mathtt{B}F$, where $F \in \mathbb{Z}^{t\times t}$. Then,

$$R = Y^T s = F^T \mathtt{B}^T s \pmod p.$$

If $\gcd(\det(F), p) = 1$, the inverse of F in $\mathbb{Z}_p$ exists, and the hints can be rewritten as

$$F_p^{-T} \cdot R = \mathtt{B}^T s = \mathtt{B}^T \mathtt{B} w_s \pmod p.$$

As $\det(\mathtt{B}^T\mathtt{B}, p) = 1$, $(\mathtt{B}^T\mathtt{B})_p^{-1}$ exists, and

$$w_s = (\mathtt{B}^T\mathtt{B})_p^{-1} \cdot F_p^{-T} R \pmod p.$$

Since $w_s \in \mathbb{Z}_p^t$, we get w_s and then $x_s = \mathtt{B}w_s$. This is exactly the information about s given by modular hints $Y^T s = R \pmod p$. The above is true when

$$\gcd\left(\det(\mathtt{B}^T\mathtt{B}), p\right) = 1 \text{ and } \gcd(\det(F), p) = 1, \tag{4}$$

i.e., with a probability no less than $\left(\frac{\Phi(p)}{p}\right)^2$.

Remark 2. In fact, it is easy to verify that $x_s = (\Pi_{\mathtt{B}})_p \cdot s \pmod p$. This can be seen as a natural extension of the case of perfect hints, since we obtain $s_{\mathscr{V}} = \Pi_{\mathscr{V}} \cdot s$ from perfect hints $Y^T s = R$. It should be noted that $s_{\mathscr{V}}$ and $x_s \pmod p$ are similar results (i.e. some orthogonal projections of s) based on different rings $\mathbb{R}$ and $\mathbb{Z}_p$.

Remark 3. Actually, only the value of $F \pmod p$ is needed, and we could get it by

$$F = (\mathtt{B}^T\mathtt{B})_p^{-1} \cdot \mathtt{B}^T Y = \mathtt{B}_p^{\sim} \cdot Y \pmod p.$$

Remark 4. The Chinese remainder theorem may be useful for merging different modular hints. For example, suppose that the adversary gets $x_s = z_j \pmod{p_j}, j = 1, 2, \cdots, k$, where $p_1, \cdots, p_k$ is pairwise relatively prime. Let $P = \prod_{j=1}^k p_j$. We denote $P_j = \frac{P}{p_j}$ and the modular inverse of $P_j \pmod{p_j}$ by $(P_j)_{p_j}^{-1}, j = 1, 2, \cdots, k$. Then a modular hint with modulus P is derived, as $x_s \pmod P$ is given by

$$x_s = \sum_{j=1}^{k} z_j \cdot (P_j)_{p_j}^{-1} \cdot P_j \pmod P.$$

3.3 Reducing the LWE instance by modular hints with modulus q

Since the original LWE samples are based on $\mathbb{Z}_q$, modular hints with modulus q could be better compatible and provide more useful information. They are also the focus of this subsection. As summarized in [15], there are several scenarios to obtain such hints in practice, for example, by the leakage of the values of intermediate registers or NTT coefficients.

It can be seen in [15] that perfect hints can reduce the dimension of the lattice used by the adversary in the primal attack. However, modular hints are just used for possible change of its volume but without decreasing the dimension. In this subsection, the greater potential of modular hints with modulus q is explored. It is shown that such hints could also be used to reduce the dimension when certain conditions are met. Furthermore, we would like to emphasize two differences compared with [15]. The first one is that we shall directly use modular hints to reduce the LWE instance rather than optimizing the attack; the second one is a consequence of the first one, an improvement in parameter of the secret (i.e. its dimension) is obtained, not that of the lattice (i.e. its volume). We believe that these may be the changes that make things more fundamental and information more fully utilized.

The process of converting the original LWE instance (A, b) to another LWE instance whose secret is of a lower dimension using modular hints with modulus q (Of course, this process also applies to perfect hints) is as follows.

We assume $\gcd(\det(\mathtt{B}^T\mathtt{B}), q) = 1$. According to theorem 1, now $\mathbb{Z}^n = \mathscr{L} + \mathscr{G} + q\mathbb{Z}^n$ holds and the adversary obtains $x_s \pmod q$ by hints $Y^T s = R \pmod q$. We denote the j-th column of A^T by a_j, and it could be decomposed into

$$a_j = x_j + y_j + qu_j = \mathtt{B}w_j + \mathtt{D}v_j + qu_j,$$

where $w_j \in \mathbb{Z}_q^t, v_j \in \mathbb{Z}_q^{n-t}$ and $u_j \in \mathbb{Z}^n, j = 1, 2, \cdots, m$. It is easy to extract v_j since $v_j = \mathtt{D}_q^{\sim} \cdot a_j \pmod q, j = 1, 2, \cdots, m$. Let $V = \begin{pmatrix} v_1^T \\ \vdots \\ v_m^T \end{pmatrix} \in \mathbb{Z}_q^{m\times(n-t)}$, then we have

$$As = Ax_s + Ay_s = Ax_s + V\mathtt{D}^T y_s \pmod q.$$

Let $c = b - Ax_s \pmod q$ and $z = \mathtt{D}^T y_s \pmod q$, a new LWE instance is obtained:

$$c = Vz + e \pmod q.$$

As we shall see, the dimension of the new secret does decrease since $z \in \mathbb{Z}_q^{n-t}$. Various attacks can be applied directly to this new instance. However, one point to note is that, unlike s, z is not particularly short. This has no effect on the BKW algorithm without a partial guessing step, but a further secret-noise transformation may be necessary when considering primal attack and dual attack. This is because the distribution of the secret is critical in these two attacks. The details will be given in the next section.

4 Primal Attack and Dual Attack

Given an LWE instance $(A, b = As + e \pmod q) \in \mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m$ $(m > n)$[7]. We denote $S = \begin{pmatrix} s \\ e \end{pmatrix}$ and $d = m + n$. In practice, the adversary may gets hints of s

[7] In the primal attack and dual attack, m is usually very close to n, and the case where $m < n$ may occurs in several schemes. However, as mentioned in Section 3.3, after adding hints, a secret-noise transformation as well as some additional samples are needed. Hence, we suppose that $m > n$ here. As we shall see, this will not make the dimension of the lattice used by the attacker larger.

[1, 12, 31], of e [21], or even of S [15]. So here, we represent the hints in a general form, that is, $X^T S = J \pmod q$, where $X \in \mathbb{Z}_q^{d\times t}$ and $J \in \mathbb{Z}_q^t$.

To add these hints to a primal attack or a dual attack, the adversary first transforms them to some hints of s, and then get a new LWE instance whose secret is of a lower dimension. To be specific, he/she decomposes X into $X = \begin{pmatrix} X_1 \\ X_2 \end{pmatrix}$, where $X_1 \in \mathbb{Z}_q^{n\times t}$ and $X_2 \in \mathbb{Z}_q^{m\times t}$. Then $J = X_1^T s + X_2^T e = X_1^T s + X_2^T (b - As) \pmod q$ and then the hints of s are gotten:

$$J - X_2^T b = \left(X_1^T - X_2^T A\right) s \pmod q.$$

We denote the hint description matrix of s by $Y = \left(X_1 - A^T X_2\right) \bmod q \in \mathbb{Z}_q^{n\times t}$ and $R = J - X_2^T b \pmod q$. In the following, we only consider the case of $t < n$, i.e. the number of hints does not exceed the number of the entries of the secret. This seems to be reasonable as when too many hints are given, it may not make sense to analyze security in terms of the primal attack or dual attack. In this situation, the probability that Y contains t linearly independent column vectors is very high.

We denote $\mathscr{V} = \text{Span}(Y)$ and define the lattices $\mathscr{L} = \mathbb{Z}^n \cap \mathscr{V}, \mathscr{G} = \mathbb{Z}^n \cap \mathscr{V}^\perp$. As described in Section 3.1, a basis $\mathtt{B}$ of $\mathscr{L}$ and a basis $\mathtt{D}$ of $\mathscr{G}$ could be found by MLLL.

We focus on the case where conditions in equation (4) are met. From theorem 1, then $\mathbb{Z}^n$ can be decomposed into $\mathbb{Z}^n = \mathscr{L} + \mathscr{G} + q\mathbb{Z}^n$ and s can be decomposed into $s = x_s + y_s + qu_s$, where $x_s \in \mathscr{L}, y_s \in \mathscr{G}, u_s \in \mathbb{Z}^n$. According to Section 3.2, hints $Y^T s = R \pmod q$ give $x_s = \mathtt{B} \cdot (\mathtt{B}^T Y)_q^{-1} R \pmod q$ [8]. Then, using the method in Section 3.3, let $c = b - Ax_s \pmod q, V = A \cdot \mathtt{D}_q^{\sim T} \pmod q$ and $z = \mathtt{D}^T y_s \pmod q$, a new LWE instance $(V, c = Vz + e \pmod q) \in \mathbb{Z}_q^{m\times(n-t)} \times \mathbb{Z}_q^m$ is obtained.

Now, let us perform the secret-noise transformation. Without loss of generality, suppose that the first $n-t$ rows of V are linearly independent and form the matrix $V_{[1:n-t]}$. Further, we assume that $\gcd\left(\det\left(V_{[1:n-t]}\right), q\right) = 1$, i.e. $V_{[1:n-t]}$ is invertible in $\mathbb{Z}_q$. It should be pointed out that, since $m > n-t$, it is quite possible because we can swap the order of the rows of V. We define $V' = -V \cdot \left(V_{[1:n-t]}\right)_q^{-1} \pmod q, x = e_{[1:n-t]}$ and $c' = c + V' \cdot c_{[1:n-t]} \pmod q$, then $c' = V'x + e \pmod q$ and $c'_{[1:n-t]} = 0$. We only consider the non-zero part. Let $g = c'_{[n-t+1:m]}, W = V'_{[n-t+1:m]}$ and $f = e_{[n-t+1:m]}$, then a new LWE instance in HNF is obtained:

$$(W, g = W \cdot x + f \pmod q) \in \mathbb{Z}_q^{(m-n+t)\times(n-t)} \times \mathbb{Z}_q^{m-n+t}.$$

To sum up, using t modular hints with modulus q, the original instance (A, b) can be converted to another LWE instance (V, c) whose secret $z \in \mathbb{Z}_q^{n-t}$. A further secret-noise transformation could be performed to get the instance (W, g) in HNF at the cost of $n - t$ additional samples.

Remark 5. In fact, the original hints $X^T S = J \pmod q$ could be extended to the new instance (W, g). This is because now the new secret and error form $S' = \begin{pmatrix} x \\ f \end{pmatrix}$, which is

[8] When $\gcd\left(\det\left(\mathtt{B}^T\mathtt{B}\right), q\right) = 1$, $(\mathtt{B}^T Y)_q^{-1}$ exists if and only if $\gcd(\det(F), q) = 1$.

exactly e! As $m > n$, we know that when $\gcd\left(\det\left(A^T A\right), q\right) = 1$, s can be expressed as $s = A_q^{\sim}(b-e) \pmod q$, then $J = X_1^T s + X_2^T e = X_1^T A_q^{\sim}(b-e) + X_2^T e \pmod q$. These could be rewritten as hints of e:

$$J - X_1^T A_q^{\sim} b = \left(X_2^T - X_1^T A_q^{\sim}\right) e \pmod q.$$

We denote $K = J - X_1^T A_q^{\sim} b \pmod q, P = X_2 - (A_q^{\sim})^T X_1 \pmod q$. In the following, we will use the primal attack as an example to show that these inherited hints do not lead to any improvement. In other words, hints cannot be used twice.

4.1 Primal attack

In this subsection, we discuss the details of adding modular hints with modulus q to the primal attack. As previously mentioned, with t hints $X^T S = J \pmod q$, the original LWE instance (A, b) is transformed into a new instance (W, g) in HNF with a secret x whose dimension drops by t. The hints are also inherited as $P^T S' = K \pmod q$.

The primal attack is associated with the so-called Kannan's embedding, both before and after adding hints. To perform a primal attack, the adversary constructs the lattice

$$L_{\mathbf{pri}}(W, g) = \left\{ \begin{pmatrix} u \\ v \\ w \end{pmatrix} \in \mathbb{Z}^{m+1} \middle| Wu + v - g \cdot w = 0 \pmod q \right\}.$$

It is an $(m+1)$-dimensional lattice of volume q^{m-n+t}, and a basis of it is given by

$$B_{\mathbf{pri}}(W, g) = \begin{pmatrix} -I_{n-t} & 0 & 0 \\ W & qI_{m-n+t} & g \\ 0 & 0 & 1 \end{pmatrix}.$$

We define $\overline{S'} = \begin{pmatrix} S' \\ 1 \end{pmatrix} \in \mathbb{Z}_q^{m+1}$ and $\overline{P} = \begin{pmatrix} P \\ -K^T \end{pmatrix} \in \mathbb{Z}_q^{(m+1)\times t}$, then $\overline{S'}$ is a short vector in $L_{\mathbf{pri}}(W, g)$ and the hints could also be expressed as $\overline{P}^T \overline{S'} = 0 \pmod q$.

The essence of the above steps is to reduce the LWE instance by modular hints with modulus q. Further, we consider whether we could continue to use the rewritten hints to reduce the primal attack against the new instance. From some ideas of [15], after the integration of $\overline{P}^T \overline{S'} = 0 \pmod q$, $\overline{S'}$ can be searched in [9] $L'_{\mathbf{pri}}(W, g) = L_{\mathbf{pri}}(W, g) \cap \Lambda_q^{\perp}\left(\overline{P}^T\right)$. It has been proven in [15] that the dimension of the intersection lattice remains unchanged, but its volume could be larger, which is advantageous to the primal attack. However, a fact is discovered is that $L'_{\mathbf{pri}}(W, g) = L_{\mathbf{pri}}(W, g)$ always holds. This means that once some hints have been used to reduce the dimension of the LWE instance, they can no longer be expected to have a positive effect on the volume of the lattice again. Some explanations can be seen in appendix E.

[9] For the sake of simplification, we omit the steps of homogenization and isotropization, which is similar to a lightweight implementation in [15]. We use the two core parameters of the lattice (dimension, volume) as well as assumption 3 to predict the attack cost.

The new algorithm for the primal attack using modular hints with modulus q is summarized in algorithm 1. It works if the following conditions are met:

$$\gcd\left(\det(\mathtt{B}^T\mathtt{B}), q\right) = \gcd\left(\det(F), q\right) = \gcd\left(\det\left(V_{[1:n-t]}\right), q\right) = 1. \tag{5}$$

Hence, its success rate could be estimated as $\left(\frac{\Phi(q)}{q}\right)^3$. We notice that, in the actual schemes, q is either chosen to be a large prime number (such as Kyber and Newhope) or to be a power of 2 (for example, Saber and FrodoKEM). Hence, this probability is actually

$$\left(\frac{\Phi(q)}{q}\right)^3 = \begin{cases} \left(1-\frac{1}{q}\right)^3 & q \text{ is a odd prime} \\ \frac{1}{8} & q \text{ is a power of 2} \end{cases}.$$

Algorithm 1: Primal attack using modular hints with modulus q (main steps)

Input: The original instance $(A, b = As + e \pmod q) \in \mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m$ and $X \in \mathbb{Z}_q^{d\times t}, J \in \mathbb{Z}_q^t$, such that $X^T S = J \pmod q$.
Output: The secret s.
Step 1: Transform $X^T S = J \pmod q$ into hints of $s : Y^T s = R \pmod q$;
Step 2: Add hints of s and obtain a new instance $(V, c) \in \mathbb{Z}_q^{m\times(n-t)} \times \mathbb{Z}_q^m$;
Step 3: Perform the secret-noise transformation and obtain the instance $(W, g) \in \mathbb{Z}_q^{(m-n+t)\times(n-t)} \times \mathbb{Z}_q^{m-n+t}$;
Step 4: Construct the lattice $L_{\mathbf{pri}}(W, g)$ and search $\overline{S'}$ in it by the BKZ algorithm;
Step 5: Recover the secret s by $s = A_q^{\sim}(b - S') \pmod q$.

The complexity model of our new algorithm is quite easy, because the cost is mainly due to solving the uSVP instance on $L_{\mathbf{pri}}(W, g)$ rather than transforming the LWE instance. Since the volume and dimension of $L_{\mathbf{pri}}(W, g)$ are obvious, we only need to figure out the optimal BKZ blocksize β_0 and number of samples m_0' by assumption 3. As $n-t$ samples of these m_0' samples are for the secret-noise transformation, the actual number of samples used for searching short vectors in $L_{\mathbf{pri}}(W, g)$ is $m_0 = m_0' - n + t$.

Now let us make a comparison between the method of adding modular hints with modulus q to the primal attack in this paper and that in [15]. Suppose that an LWE instance (A, b) with t hints $X^T S = J \pmod q$ is given. In [15], hints $X^T S = J \pmod q$ are directly added to the primal attack against (A, b). While in our framework, we use these hints to transform (A, b) into another LWE instance (W, g) in HNF whose secret is of a lower dimension and then perform the primal attack against (W, g). In a sense, it may be more straightforward to directly reduce the instance itself rather than the attacks on it, and it may be more fundamental to optimize the parameter of the secret rather than the lattice.

One may notice that our method causes a decrease in dimension, but adding the rewritten hints of e to $L_{\mathbf{pri}}(W, g)$ can not bring any increase about volume. On the contrary, by using the method in [15], the volume may be enlarged, but the dimension remains the same. To give a further mathematical comparison between the effects of the

decrease in dimension and the increase in volume, we naturally extend the Lemma 13 of [15] as follows, and the proof is given in appendix F.

Proposition 6. *Given positive integers p and $n \leq m$. Let $\Lambda \subseteq \mathbb{R}^m$ be an n-dimensional lattice and $\Psi = (\psi_1 \ \psi_2 \ \cdots \ \psi_t)$ contains linearly independent vectors of $\mathbb{R}^m$. If $\left\{\frac{\psi_j}{l_j}\right\}_{j=1}^{t}$ is a set of primitive vectors with respect to Λ^*, where $l_j \in \mathbb{N}^+, j = 1, 2, \cdots, t$, then $\Lambda \cap \Lambda_p^{\perp}(\Psi^T)$ is an n-dimensional lattice of volume $\frac{p^t}{\prod_{j=1}^{t} \gcd(l_j,p)} \cdot vol(\Lambda)$.*

It should be noted that proposition 6 is not only an extension to the case with multiple hints, but also shows an interesting fact. In proposition 6, vol $\left(\Lambda \cap \Lambda_q^{\perp}(\Psi^T)\right) \leq p^t \text{vol}(\Lambda)$ and the equality holds if and only if $\gcd(l_j, p) = 1, 1 \leq j \leq t$. It is a relatively loose condition, as the primitiveness of Ψ (i.e. $l_j = 1, 1 \leq j \leq t$) is no longer required.

The key indicator of performance is the BKZ blocksize used. When the conditions in equation (5) are met, we see that our approach reduces the dimension of the secret by t. Recall that the optimal blocksize choice for our case is β_0. Now let us see the effect of having t modular hints with modulus q in the primal attack in [15]. From proposition 6, vol $\left(L'_{\mathbf{pri}}(A, b)\right) \leq q^t \cdot \text{vol}\left(L_{\mathbf{pri}}(A, b)\right) = q^{m+t}$. When the equality holds, the primal attack of [15] reaches its best performance and β_0 is also its optimal selection. However, when vol $\left(L'_{\mathbf{pri}}(A, b)\right) < q^{m+t}$, a larger optimal blocksize as well as a higher cost are needed in [15]. Please see appendix G for a more detailed analysis and some example for situations that vol $\left(L'_{\mathbf{pri}}(A, b)\right) < q^{m+t}$. We should remark that these depend on the conditions in equation (5) and come at the cost of more (about n) samples.

In conclusion, our new algorithm could be divided into two parts, the reduction of the LWE instance and the execution of the BKZ algorithm on $L_{\mathbf{pri}}(W, g)$. It should be pointed out that, although m is larger in our approach, this does not make the dimension of $L_{\mathbf{pri}}(W, g)$ go higher, since the secret-noise transformation is performed before the BKZ algorithm. Furthermore, the additional samples needed are available in several actual schemes. For example, there are 2048 samples can be used in a Newhope1024 instance [6, Section 4.2.3], however, even without hints, just 999 samples are enough for the primal attack. This number will decrease when more hints are given. The remaining samples are sufficient for the secret-noise transformation.

4.2 Dual attack

In this subsection, we shall report the first dual attack by using modular hints.

For a given instance $(A, b) \in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$, the goal of the dual attack is to distinguish whether it is an LWE instance or a uniform one. Once t hints $X^T S = J \pmod q$ are obtained, by a similar process as above, the adversary can transform it to another instance $(W, g) \in \mathbb{Z}_q^{(m-n+t)\times(n-t)} \times \mathbb{Z}_q^{m-n+t}$. As mentioned earlier, if (A, b) is an LWE instance, then (W, g) is also an LWE instance in HNF, i.e. both the secret and error vectors of (W, g) follow the error distribution. On the other hand, if b is uniform, then so is g.

The adversary now only has to make a distinction between the distribution of g in the two cases. The following lattice is considered:

$$L_{\mathbf{du}}(W) = \left\{ \begin{pmatrix} v \\ u \end{pmatrix} \in \mathbb{Z}^m \middle| W^T u = v \pmod q \right\}.$$

It is an m-dimensional lattice of volume q^{n-t}, and has a basis

$$B_{\mathbf{du}}(W) = \begin{pmatrix} I_{m-n+t} & O \\ W^T & qI_{n-t} \end{pmatrix}.$$

Short vectors will be searched in $L_{\mathbf{du}}(W)$ by BKZ. Suppose that M short vectors $w_j = \begin{pmatrix} v_j \\ u_j \end{pmatrix}, j = 1, 2, \cdots, M$ of length at most l are found and used in the dual attack. Then, for any j, if $g \leftarrow U(\mathbb{Z}_q^{m-n+t})$, $\langle u_j, g \rangle$ could also be viewed as uniform. Otherwise,

$$\langle u_j, g \rangle = u_j^T(Wx + f) = v_j^T x + u_j^T f = \left\langle \begin{pmatrix} v_j \\ u_j \end{pmatrix}, \begin{pmatrix} x \\ f \end{pmatrix} \right\rangle = \langle w_j, e \rangle \pmod q$$

is relatively small since w_j, e are both short vectors. From lemma 3, as M increases,

$$\frac{\sum_{j=1}^M e^{-\frac{2\pi i \langle u_j, g \rangle}{q}}}{M} \to \frac{\sum_{j=1}^M \mathbf{B}\left(f_{\langle u_j, g \rangle}\right)}{M} = \frac{\sum_{j=1}^M \widehat{f_{\langle u_j, g \rangle}}(1)}{M}$$

$$= \begin{cases} \frac{\sum_{j=1}^M 0}{M} = 0 & g \leftarrow U(\mathbb{Z}_q^{m-n+t}) \\ \frac{\sum_{j=1}^M \widehat{f_{\langle e, w_j \rangle}}(1)}{M} \geq \frac{\sum_{j=1}^M e^{-\frac{2\pi^2 \sigma_\chi^2 \|w_j\|^2}{q^2}}}{M} \geq e^{-\frac{2\pi^2 \sigma_\chi^2 l^2}{q^2}} := \epsilon & g = Wx + f \pmod q \end{cases}.$$

When constructing a distinguisher, only the real part is considered. That is, the adversary calculates $\frac{\sum_{j=1}^M \cos\left(\frac{2\pi \langle u_j, g \rangle}{q}\right)}{M}$ and checks whether it is greater than $\frac{\epsilon}{2}$. To achieve a constant success rate of the distinction, according to lemma 4, $M = O\left(\frac{1}{\epsilon^2}\right)$ vectors are needed. The new algorithm for the dual attack using modular hints with modulus q is summarized in algorithm 2.

Now we shall give the cost model of our new algorithm and the selection method of each parameter. According to assumption 1, the length of each short vector found in $L_{\mathbf{du}}(W)$ by BKZ-β is $l(m, \beta) = (\delta_0(\beta))^m \cdot q^{\frac{n-t}{m}}$, thereby bringing an advantage $\epsilon(m, \beta) = e^{-\frac{2\pi^2 \sigma_\chi^2 l(m,\beta)^2}{q^2}}$.

From Chernoff-Hoeffding inequality, $O\left(\frac{1}{\epsilon^2(m,\beta)}\right)$ short vectors are needed to reach a constant success rate. The process of BKZ must be repeated at least $R(d, \beta)$ times, where $R(m, \beta) = \max\left\{1, \frac{1}{\epsilon^2(m,\beta) \cdot 2^{0.2075\beta}}\right\}$. Then the cost of the search phase is

$$T(m, \beta) = TBKZ(\beta) \cdot R(m, \beta).$$

Hence, one should choose the optimal blocksize β_0 and the total number of samples m_0' that minimize $T(m_0', \beta_0)$. Actually, m_0' could be regarded as a function of β. From some ideas of [30] and [26], we have

$$m_0'(\beta) = \left\lceil \sqrt{\frac{\ln q}{\ln\left(\delta_0(\beta)\right)} \cdot (n - t)} \right\rfloor, \tag{6}$$

Algorithm 2: Dual attack using modular hints with modulus q (main steps)

Input: The original instance $(A, b = As + e \pmod q) \in \mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m$ and $X \in \mathbb{Z}_q^{d\times t}, J \in \mathbb{Z}_q^t$, such that $X^T S = J \pmod q$.
Output: 0 for $b \leftarrow U(\mathbb{Z}_q^m)$ and 1 for $b \leftarrow$ LWE.
Step 1: Transform $X^T S = J \pmod q$ into hints of $s : Y^T s = R \pmod q$;
Step 2: Add hints of s and obtain a new instance $(V, c) \in \mathbb{Z}_q^{m\times(n-t)} \times \mathbb{Z}_q^m$;
Step 3: Perform the secret-noise transformation and obtain the instance $(W, g) \in \mathbb{Z}_q^{(m-n+t)\times(n-t)} \times \mathbb{Z}_q^{m-n+t}$;
Step 4: Construct $L_{\mathbf{du}}(W)$ and find M short vectors $\{w_j\}_{j=1}^M$ in it by BKZ;
Step 5: Calculate $\frac{\sum_{j=1}^M \cos\left(\frac{2\pi\langle u_j, g\rangle}{q}\right)}{M}$ and output 0 if it is smaller than $\frac{\epsilon}{2}$, otherwise, output 1.

where $\lceil\cdot\rfloor$ means to round to the nearest whole number. This is because before rounding, it is the only zero of the derivative of $l(m, \beta)$ with respect to m:

$$\frac{\partial l(m,\beta)}{\partial m} = \frac{\partial\left((\delta_0(\beta))^m \cdot q^{\frac{n-t}{m}}\right)}{\partial m} = (\delta_0(\beta))^m \cdot \ln(\delta_0) \cdot q^{\frac{n-t}{m}} + (\delta_0(\beta))^m \cdot q^{\frac{n-t}{m}} \cdot \ln q \cdot \left(-\frac{n-t}{m^2}\right)$$
$$= (\delta_0(\beta))^m \cdot q^{\frac{n-t}{m}} \cdot \left(\ln(\delta_0(\beta)) - \ln q \cdot \frac{n-t}{m^2}\right).$$

Hence, the adversary just needs to search for the optimal $\beta_0 = \min_{\beta\in\mathbb{N}^+}\{T(m_0'(\beta), \beta)\}$, and then the optimal number of samples required is $m_0'(\beta_0)$.

5 BKW

In this section, the situation where hints (including perfect hints and modular hints with modulus q) are added to the BKW attack is considered. A matrix representation for BKW algorithm is presented in Section 5.1. To give a comparison, two methods of integrating hints to the BKW attack are discussed. Section 5.2 describes the first method which processes hints by adding them to the BKW attack directly. The second method is a procedure to carry out BKW attack on the new instance obtained by reducing the original LWE instance according to the way given in Section 3.3. A description as well as an analysis of this method can be seen in Section 5.3. To the best of our knowledge, this is the first time that hints are integrated into a BKW attack. Among these two proposed methods, we find the second one to be more beneficial. It is also worth mentioning that, as we will see later, BKW attack seems to be particularly compatible with our attack framework due to its construction.

5.1 The matrix representation of BKW

In this subsection, the two core stages – sample reduction and hypothesis testing – are both reformulated in a matrix form for more fundamental analysis.
Sample reduction Suppose that the adversary uses m original LWE samples, which

are denoted by $b = As + e \pmod q$. He/She selects the parameters *window width* β and *addition depth* α.

Then each row of A is divided into $\alpha + 1$ blocks, where the first α blocks each contains β entries, and the last one is made up of $n-\alpha\beta$ entries. In the j-th ($1 \le j \le \alpha$) iteration of the sample reduction stage, collisions on the j-th block are searched and the corresponding rows of A are added or subtracted together to produce new samples.

Let us take the first iteration as an example. Suppose that the adversary finds m_1 collisions on block 1, that is, there exists a matrix $P_1 \in \mathbb{Z}^{m_1 \times m}$, such that

$$P_1 \cdot A = A^{(1)},$$

where $A^{(1)} \in \mathbb{Z}^{m_1 \times n}$, the first β entries in each row of $A^{(1)}$ are all 0, and P_1 has rows with up to two non-zero entries in $\{-1, 1\}$.

Similarly, after the j-th ($2 \le j \le \alpha$) iteration, suppose that m_j samples are obtained, then there exists $P_j \in \mathbb{Z}^{m_j \times m_{j-1}}$, such that

$$P_j \cdot P_{j-1} \cdots P_1 \cdot A = P_j \cdot A^{(j-1)} = A^{(j)},$$

where $A^{(j)} \in \mathbb{Z}^{m_j \times n}$, the first $\beta \cdot j$ entries in each row of $A^{(j)}$ are all 0, and $P_1, \cdots, P_j$ are integer matrices with at most two non-zero entries that belong to $\{-1, 1\}$ per row. Let $P = P_\alpha \cdot P_{\alpha-1} \cdots P_1 \in \mathbb{Z}^{m_\alpha \times m}$, then after the sample reduction process, we have

$$PA = A^{(\alpha)}.$$

The first $\alpha \cdot \beta$ entries in each row of $A^{(\alpha)}$ are all 0. Let A' be the submatrix consisting of the $(\alpha\beta + 1)$-th to the n-th columns of $A^{(\alpha)}$ and $s' = s_{[\alpha\beta+1:n]}$, then $A's' = A^{(\alpha)}s$. We denote $b' = Pb \pmod q$, $e' = Pe \pmod q$, then

$$b' = P(As + e) = PAs + e' = A^{(\alpha)}s + e' = A's' + e' \pmod q.$$

To sum up, let $n' = n - td$, the original LWE instance $(A, b) \in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$ is transformed to another instance $(A', b') \in \mathbb{Z}_q^{m_\alpha \times n'} \times \mathbb{Z}_q^{m_\alpha}$. The dimension of the secret is reduced, at the cost of amplified noises.

Hypothesis testing Now we just need to check the $q^{n'}$ possibilities of s'. All values can be tested simultaneously by an FFT.

For each secret candidate $\widetilde{s'} \in \mathbb{Z}_q^{n'}$, it corresponds to an error candidate $\widetilde{e'} = b' - A'\widetilde{s'} \pmod q$ in $\mathbb{Z}_q^{m_\alpha}$. The distribution of $\widetilde{e'}$ in the two cases where $\widetilde{s'}$ is equal to s' or not is the key to distinguishing. When the guess is wrong, $\widetilde{e'}$ is considered to obey a uniform distribution in $\mathbb{Z}_q^{m_\alpha}$. While the true e' approximately follows a discrete Gaussian distribution. More specifically, each coefficient of e' could be regarded as a sum of 2^α entries of e, and the independence among the coefficients of e' is supposed. These actually imply the following assumption.

Assumption 4 *$e' = Pe$ and $PP^T = 2^\alpha I_{m_\alpha}$.*

From lemma 1, we have

$$e' = Pe \sim G_{m_\alpha, q}\left(0, P \cdot \sigma_\chi^2 I_m \cdot P^T\right) = G_{m_\alpha, q}\left(0, \sigma_\chi^2 2^\alpha I_{m_\alpha}\right).$$

Hence, for each $\widetilde{e'}$, the adversary needs to distinguish whether it obeys $G_{m_\alpha,q}\left(0,\sigma_\chi^2 2^\alpha I_{m_\alpha}\right)$ or $U(\mathbb{Z}_q^{m_\alpha})$. To further determine the number of final samples required (i.e. m_α), we regard each entry of $\widetilde{e'}$ as the inner product between $\widetilde{e'}$ and a specified vector, that is,

$$\widetilde{e'}_j = \left\langle \widetilde{e'}, \gamma_j \right\rangle,\ j = 1, 2, \cdots, m_\alpha,$$

where γ_j is the unit vector in $\mathbb{Z}^{m_\alpha}$ with only the j-th entry being 1. Then the advantage from each inner product could be estimated by lemma 3. A distinguisher is thus implied. For each key candidate $\widetilde{s'}$, we calculate

$$\frac{\sum_{j=1}^{m_\alpha} e^{-\frac{2\pi i\left\langle b'-A'\widetilde{s'},\gamma_j\right\rangle}{q}}}{m_\alpha} = \frac{\sum_{j=1}^{m_\alpha} e^{-\frac{2\pi i\left\langle \widetilde{e'},\gamma_j\right\rangle}{q}}}{m_\alpha} \longrightarrow \frac{\sum_{j=1}^{m_\alpha} \mathbf{B}\left(f_{\left\langle \widetilde{e'},\gamma_j\right\rangle}\right)}{m_\alpha}$$
$$= \frac{\sum_{j=1}^{m_\alpha} \widehat{f_{\left\langle \widetilde{e'},\gamma_j\right\rangle}}(1)}{m_\alpha} \begin{cases} = \frac{\sum_{j=1}^{m_\alpha} 0}{m_\alpha} = 0 & \widetilde{s'} \neq s' \\ \geq \frac{\sum_{j=1}^{m_\alpha} e^{-\frac{2\pi^2\cdot 2^\alpha \sigma_\chi^2 \|\gamma_j\|^2}{q^2}}}{m_\alpha} = e^{-\frac{2^{\alpha+1}\pi^2\sigma_\chi^2}{q^2}} := \epsilon & \widetilde{s'} = s' \end{cases}.$$

Therefore, the guessed candidate is the one that satisfies

$$s_0 = \text{argmax}_{\widetilde{s'}\in\mathbb{Z}_q^{n'}} \mathscr{R}e\left(\frac{\sum_{j=1}^{m_\alpha} e^{-\frac{2\pi i\left\langle b'-A'\widetilde{s'},\gamma_j\right\rangle}{q}}}{m_\alpha}\right).$$

According to the Chernoff-Hoeffding inequality (lemma 4),

$$m_\alpha = O\left(\frac{1}{\epsilon^2}\right) = C\cdot e^{\frac{2^{\alpha+2}\pi^2\sigma_\chi^2}{q^2}}$$

samples are sufficient to achieve a constant success rate, where C is a constant [10].

5.2 Constructing error-free samples using hints

Transforming hints into those of the secret seems to be more natural in the BKW attack. This is because now s and e play different roles in different stages, while in the primal attack and dual attack, they are combined to form a short vector S. In this subsection, we discuss the direct enhancement on BKW attack by hints. To be specific, the hints (including perfect hints and modular hints with modulus q) are directly added to the BKW attack against the original instance (A, b).

As we know, in the sample reduction stage, the colliding samples are added (or subtracted) to reduce the dimension of the secret that "works [11]". However, this magnifies the noises. Large noises also make it difficult to identify the true secret (or more precisely, part of the secret) among other candidates during the hypothesis testing stage. In

[10] Our result is consistent with that in [13], where C is regarded as a small constant.

[11] For example, after the j-th $(2 \leq j \leq \alpha)$ iteration, the first $\beta \cdot j$ entries in each row of $A^{(j)}$ are all 0. This implies that the first $\beta \cdot j$ entries of s do not work.

the following, we shall show that t perfect hints of s are bound to provide q^t error-free samples. Adding or subtracting such samples does not result in an increase in noises. Moreover, based on the decomposition idea in Section 3, t modular hints with modulus q could give the same information with a probability of $\left(\frac{\phi(q)}{q}\right)^2$.

Let us start with a specific explanation of the case with modular hints. Given the LWE instance $(A, b = As+e \pmod q) \in \mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m$ and $t(t < n)$ linearly independent modular hints $Y^T s = R \pmod q$, where $Y \in \mathbb{Z}_q^{n\times t}$ and $R \in \mathbb{Z}_q^t$. Just like before, let $\mathscr{V} = \text{Span}(Y)$, we define lattices $\mathscr{L} = \mathbb{Z}^n \cap \mathscr{V}, \mathscr{G} = \mathbb{Z}^n \cap \mathscr{V}^\perp$ and their bases $\mathtt{B}, \mathtt{D}$. According to Section 3.2, we could obtain $(\Pi_{\mathtt{B}})_q \cdot s \pmod q$ by these hints when conditions in equation (4) are met, and the probability of them being true is $\left(\frac{\phi(q)}{q}\right)^2$. In the following, we also focus on this case.

Now we consider how to incorporate this information into the sample reduction phase, in which the values (after $\bmod q$) of the inner products between s and all vectors in $\mathbb{Z}_q^n$ are taken into account. Actually, for any $a \in \mathbb{Z}^n$, $\langle a, s\rangle \pmod q$ could be decomposed using the orthogonal projection matrices onto $\Lambda_q(\mathtt{B}^T)$ and $\Lambda_q(\mathtt{D}^T)$. From proposition 5, we have

$$\begin{aligned}\langle a, s\rangle &= \langle (\Pi_{\mathtt{B}})_q \cdot a + (\Pi_{\mathtt{D}})_q \cdot a, (\Pi_{\mathtt{B}})_q \cdot s + (\Pi_{\mathtt{D}})_q \cdot s\rangle \\ &= \langle (\Pi_{\mathtt{B}})_q \cdot a, (\Pi_{\mathtt{B}})_q \cdot s\rangle + \langle (\Pi_{\mathtt{D}})_q \cdot a, (\Pi_{\mathtt{D}})_q \cdot s\rangle \pmod q.\end{aligned}$$

It is easy to see that for those $a \in \mathbb{Z}^n$ such that $(\Pi_{\mathtt{D}})_q \cdot a = 0 \pmod q$, we could directly calculate $\langle a, s\rangle = \langle (\Pi_{\mathtt{B}})_q \cdot a, (\Pi_{\mathtt{B}})_q \cdot s\rangle \pmod q$ by hints.

In fact, such a's exactly form the lattice $\Lambda_q(\mathtt{B}^T)$. According to corollary 1, suppose that $a = a_1 + a_2 + qu$, where $a_1 \in \Lambda_q(\mathtt{B}^T), a_2 \in \Lambda_q(\mathtt{D}^T), u \in \mathbb{Z}^n$. Then from proposition 1, $(\Pi_{\mathtt{D}})_q \cdot a = a_2 \pmod q$ and hence $(\Pi_{\mathtt{D}})_q \cdot a = 0 \pmod q \iff a_2 = 0 \pmod q \iff a = a_1 + qu \in \Lambda_q(\mathtt{B}^T)$.

To sum up, for any $a \in \Lambda_q(\mathtt{B}^T)$, the value of $\langle a, s\rangle \pmod q$ could be calculated directly without any queries. This gives a sample without noise. One might wonder how many such samples could the adversary obtain from the hints $Y^T s = R \pmod q$. Since $\Lambda_q(\mathtt{B}^T)$ is a subgroup of $\mathbb{Z}^n$ and $q\mathbb{Z}^n$ is a subgroup of $\Lambda_q(\mathtt{B}^T)$, the proportion of the vectors that belong to $\Lambda_q(\mathtt{B}^T)$ in $\mathbb{Z}_q^n$ is

$$\frac{\left|\mathbb{Z}_q^n \cap \Lambda_q(\mathtt{B}^T)\right|}{\left|\mathbb{Z}_q^n\right|} \left(= \frac{|\Lambda_q(\mathtt{B}^T)|}{|\mathbb{Z}^n|}\right) = \frac{1}{[\mathbb{Z}^n : \Lambda_q(\mathtt{B}^T)]} = \frac{1}{|\det(\mathtt{B}_q)|} = \frac{1}{\text{vol}(\Lambda_q(\mathtt{B}^T))},$$

and hence $\frac{q^n}{vol(\Lambda_q(\mathtt{B}^T))}$ samples without noises are available.

As we can see, this number is related to the volume of $\Lambda_q(\mathtt{B}^T)$. Since $\Lambda_q(\mathtt{B}^T) = \mathscr{L} + q\mathbb{Z}^n$, by applying the MLLL algorithm on $(\mathtt{B}\ qI_n)$, a basis of $\Lambda_q(\mathtt{B}^T)$ as well as vol $\left(\Lambda_q(\mathtt{B}^T)\right)$ could be obtained.

Remark 6. Actually, an estimation of vol $\left(\Lambda_q(\mathtt{B}^T)\right)$ could be given even without calculating the basis. We have done many experiments by taking $Y \leftarrow U\left(\mathbb{Z}_q^{n\times t}\right)$. A fact is discovered is that in this case $\mathtt{B}$ can also be approximated as uniform. Then from lemma 5, Pr $\left[\text{vol}\left(\Lambda_q(\mathtt{B}^T)\right) = q^{n-t}\right] \approx 1$ and $\frac{q^n}{q^{n-t}} = q^t$ samples without noises are gotten.

The case with perfect hints Now we suppose that t linearly independent perfect hints $Y^T s = R$ are obtained by the attacker, where $Y \in \mathbb{Z}^{n\times t}$ and $R \in \mathbb{Z}^t$. We define $\mathscr{V}, \mathscr{L}$ and $\mathtt{B}$ similarly. As described in Section 3.2, the adversary gets $s_{\mathscr{V}} = \Pi_{\mathscr{V}} \cdot s$ by these hints. Then for any $a \in \mathbb{Z}_q^n$ and $u \in \mathbb{Z}^n$,

$$\langle a, s\rangle = \langle a + qu, s\rangle = \left\langle (a+qu)_{\mathscr{V}}, s_{\mathscr{V}}\right\rangle + \left\langle (a+qu)_{\mathscr{V}^\perp}, s_{\mathscr{V}^\perp}\right\rangle \pmod q.$$

We notice that if $a + qu \in \mathscr{L}$, then

$$\langle a, s\rangle = \langle a + qu, s\rangle = \langle a + qu, s_{\mathscr{V}}\rangle \pmod q$$

can be computed. Further, it is easy to verify that

$$\left\{a \in \mathbb{Z}_q^n \middle| \exists u \in \mathbb{Z}^n, \text{ s.t. } a + qu \in \mathscr{L}\right\} = \Lambda_q(\mathtt{B}^T) \cap \mathbb{Z}_q^n.$$

To sum up, the same error-free samples can be obtained. The only difference is that, unlike the case with modular hints, the integration process of perfect hints always holds.

Remark 7. This is somewhat different from lattice attacks. According to [15], perfect hints and modular hints have different effects in a primal attack. The former is stronger, as they can cause changes both in dimension and volume. However, as we can see, in a BKW attack, modular hints and perfect hints are likely to bring the same boost, whether hints are added by the method given in Section 5.2 or Section 5.3. Let us try to give an explanation. As we mentioned earlier, perfect hints and modular hints are based on different rings. Since BKW is an attack built on $\mathbb{Z}_q$, a hint on $\mathbb{R}$ is no more helpful than that on $\mathbb{Z}_q$. To be specific, in the sample reduction stage, we only consider the value of $\langle a, s\rangle \pmod q$ for all $a \in \mathbb{Z}_q^n$. Although $s_{\mathscr{V}}$ provides more information of s than x_s, it could not give more error-free samples. On the contrary, the integration process of modular hints seems to be more convenient and all operations can be limited to $\mathbb{Z}_q$. Therefore, as long as the conditions in equation (4) hold, we suggest adding perfect hints in the form of modular hints to BKW.

5.3 Reducing the dimension in BKW

In the previous subsection, we show that some error-free samples could be obtained by perfect hints or modular hints with modulus q, using such samples for collisions avoids the amplification of noises. However, because the adversary has no control over the samples he/she can get from the LWE oracle, it is difficult to make full use of the information from hints. Therefore, another way of adding hints to BKW is considered.

As we mentioned earlier, the BKW attack consists of two core stages, sample reduction and hypothesis testing, in which the secret and the error play different roles. It is important to point out that, the dimension of the secret s (i.e. n) is a particularly critical parameter in the sample reduction stage, as it determines the number of required samples m, the window width β and hence the final attack cost. Therefore, it seems natural and reasonable to reduce the dimension of the secret following our attack framework. To be specific, using the method in Section 3.3, we can transform the original LWE instance (A, b) into another LWE instance (V, c) whose secret z is of dimension $n - t$.

As $A \leftarrow U\left(\mathbb{Z}_q^{m\times n}\right)$, we can think that $V \leftarrow U\left(\mathbb{Z}_q^{m\times(n-t)}\right)$. It is worth noting that the error vector e stays the same throughout this process, so does the sample size m [12].

It should be noted that, in the standard BKW algorithm [3, 19], the BKW attack works regardless of the distribution of the secret, as long as each coefficient of it belongs to $\mathbb{Z}_q$. So the secret-error transformation process is not necessary in a BKW attack [13]. We then directly perform the sample reduction stage on the new instance. Collisions between $\{v_j\}_{j=1}^m$ are looked for, instead of $\{a_j\}_{j=1}^m$. More specifically, as described in Section 5.1, we could find a matrix $P \in \mathbb{Z}^{m_\alpha\times m}$, such that $PP^T = 2^\alpha I_{m_\alpha}$ and the first $\alpha\cdot\beta$ entries in each row of $P\cdot V$ are 0. We denote the submatrix consisting of the $(\alpha\beta+1)$-th to the $(n-t)$-th columns of PV by V'. Let $z' = z_{[\alpha\beta+1:n-t]}, c' = Pc \pmod q$ and $e' = Pe \pmod q$, then a new instance $(V', c' = V'z' + e' \pmod q) \in \mathbb{Z}_q^{m_\alpha\times(n-t-\alpha\beta)} \times \mathbb{Z}_q^{m_\alpha}$ is obtained and z' can be found by the hypothesis testing stage. This process will be repeated until the whole z is gotten. Then the original secret s can also be solved since $s = x_s + y_s = x_s + (\mathit{\Pi}_{\mathtt{D}})_q \cdot y_s = x_s + \mathtt{D}(\mathtt{D}^T\mathtt{D})_q^{-1} z \pmod q$.

In particular, some of the techniques that can boost the sample reduction stage such as the coding techniques [20, 22], lazy modulus transformation [4] or quantization [24] are still applicable. The new algorithm for the BKW attack using modular hints with modulus q is summarized in algorithm 3.

Algorithm 3: BKW attack using modular hints with modulus q (main steps)

Input: The original instance $(A, b = As + e \pmod q) \in \mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m$ and $X \in \mathbb{Z}_q^{d\times t}, J \in \mathbb{Z}_q^t$, such that $X^T S = J \pmod q$.
Output: The secret s.
Step 1: Transform $X^T S = J \pmod q$ into hints of $s : Y^T s = R \pmod q$;
Step 2: Add hints of s and obtain a new instance $(V, c) \in \mathbb{Z}_q^{m\times(n-t)} \times \mathbb{Z}_q^m$;
Step 3: Perform the sample reduction procedure and obtain the instance $(V', c') \in \mathbb{Z}_q^{m_\alpha\times(n-t-\alpha\beta)} \times \mathbb{Z}_q^{m_\alpha}$;
Step 4: Find z' by the hypothesis testing process;
Step 5: Perform back substitution and recover the whole z;
Step 6: Obtain s by $s = x_s + \mathtt{D}(\mathtt{D}^T\mathtt{D})_q^{-1} z \pmod q$.

Essentially, after adding t modular hints with modulus q, the current attack cost can be viewed as that of a standard BKW attack against an LWE instance whose secret is of $n-t$ dimension. As done in [19, 22], we consider operations over $\mathbb{C}$ to have the

[12] There may be several samples that lose their effect after the integration of hints. Specifically, if $a_j \in \mathit{\Lambda}_q(\mathtt{B}^T)$, then $v_j = 0$. From another angle, in this case, $\langle a_j, s\rangle \pmod q$ can be calculated directly, so those noisy samples that correspond to a_j are no longer needed. Such a_j appears with a probability of $\frac{1}{vol(\mathit{\Lambda}_q(\mathtt{B}^T))} = \frac{1}{q^{n-t}}$. In fact, this is a natural extension of the no-hint case. Because even without hints, Pr $\left[a_j \leftarrow U(\mathbb{Z}_q^n); a_j = 0\right] = \frac{1}{q^n}$.

[13] We notice that a partial guessing step was introduced in [22], where the standard deviation of the secret entries plays a key role. In that case, one could also do the secret-error transformation as primal attack and dual attack.

same complexity as those over $\mathbb{Z}_q$ and let the small constant in the complexity of the fast Fourier transform be 1. The following is a corollary of the Theorem 17 in [19].

Corollary 2. *Given an LWE instance with parameters (n, q, σ_χ) and t modular hints with modulus q (or perfect hints). Let $\alpha, \beta \in \mathbb{N}^+$ such that $(\alpha+1)\cdot\beta = n - t$. For any $\epsilon \in (0,1)$, define $\epsilon' = \frac{1-\epsilon}{\alpha+1}$. For $0 \le j \le \alpha$, let $m(j,\epsilon) = 8\cdot\beta\cdot\log\left(\frac{q}{\epsilon}\right)\cdot\left(1-\frac{2\pi^2\sigma_\chi^2}{q^2}\right)^{-2^{\alpha+1-j}}$. Then, the time complexity of the BKW attack with success rate $\epsilon\cdot\left(\frac{\Phi(q)}{q}\right)^2$ is $c_1+c_2+c_3+c_4$, where*

$$\begin{cases} c_1 = \left(\frac{q^\beta-1}{2}\right)\cdot\left(\frac{\alpha\cdot(\alpha-1)}{2}\cdot(n+1-t) - \frac{\beta}{6}\left((\alpha+1)\cdot\alpha\cdot(\alpha-1)\right)\right) \\ c_2 = \sum_{j=0}^{\alpha} m(j,\epsilon')\cdot\frac{\alpha-j}{2}\cdot(n+2-t) \\ c_3 = 2\left(\sum_{j=0}^{\alpha} m(j,\epsilon')\right) + (n-t)\cdot q^\beta\cdot\log(q) \\ c_4 = \alpha\cdot(\alpha-1)\cdot\beta\cdot\frac{q^\beta-1}{2} \end{cases}.$$

The number of calls to the LWE oracle is

$$\alpha\cdot\frac{q^\beta-1}{2} + m(0,\epsilon),$$

and the memory complexity is

$$\left(\frac{q^\beta-1}{2}\cdot\alpha\cdot\left(n+1-t-\beta\cdot\frac{\alpha-1}{2}\right)\right) + m(0,\epsilon) + q^\beta.$$

Remark 8. As mentioned earlier, the structure of BKW makes it fit well with our framework. Firstly, since the dimension of s (not S or e) is a core parameter in the sample reduction phase, it makes the process of converting hints into those about s natural. Secondly, as BKW is built on $\mathbb{Z}_q$, perfect hints and modular hints with modulus q may be equivalent under certain conditions. This means that even if the attacker gets some perfect hints, our framework could still be used in a BKW attack, without any loss of information. Finally, if the partial guessing step is not performed, the secret-error transformation as well as additional samples are not necessary.

6 Experiments

In this section, we shall show the effect of modular hints with modulus q on the primal attack, dual attack and BKW attack respectively. The fact is discovered is that such hints can obviously improve these three attacks, especially when sufficiently many hints are available. In primal attack and dual attack, we take Newhope1024 as an example. As for BKW attack, Regev cryptosystem $(384, 147457, 39.19)$ is considered.

6.1 Primal attack and dual attack

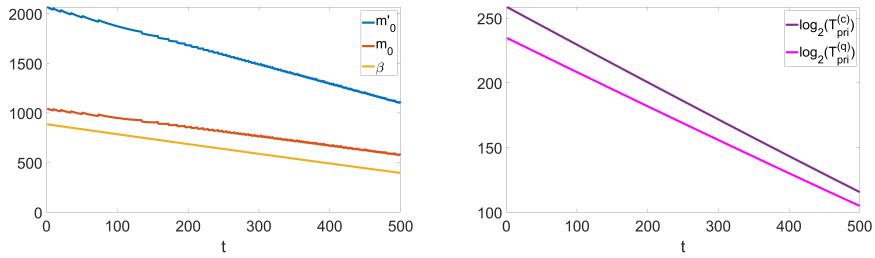
In Newhope1024 [6], $n = 1024, q = 12289$ and $\sigma_\chi = 2$. For each Newhope1024 instance, 2048 samples are available. So we limit the number of samples the adversary

can use to that. The success rate of the primal attack and dual attack (i.e. the probability of equation (5) being true) is $\left(1-\frac{1}{12289}\right)^3 \approx 0.999756$. In this subsection, we will show the relationship between the number of hints and the reduced cost of the primal attack and dual attack respectively.

For each number t, the following parameters are listed. β_0 represents the optimal blocksize and m_0' is the corresponding optimal number of samples. m_0 of these samples are used for searching short vectors in $L_{\mathbf{pri}}(W,g)$ or $L_{\mathbf{du}}(W)$ by BKZ. Given β_0, m_0', we denote the time complexities of the primal attack and dual attack in the classical case by $T_{\mathbf{pri}}^{(c)}$ and $T_{\mathbf{du}}^{(c)}$ respectively. While $T_{\mathbf{pri}}^{(q)}$ and $T_{\mathbf{du}}^{(q)}$ are for the quantum case.

Table 1: Primal attack with hints against Newhope1024.

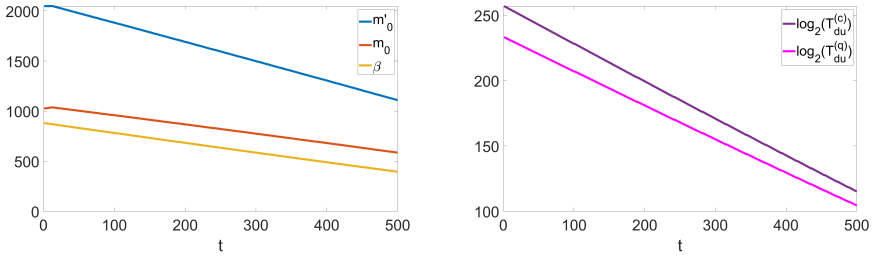
t	m_0'	m_0	β_0	$\log_2\left(T_{\mathbf{pri}}^{(c)}\right)$	$\log_2\left(T_{\mathbf{pri}}^{(q)}\right)$
0	2023	999	887	259.00	235.06
100	1856	932	786	229.51	208.29
200	1645	821	687	200.60	182.06
300	1487	763	588	171.70	155.82
400	1256	632	492	143.66	130.38
500	1086	562	396	115.63	104.94



As we shall see in table 1 and 2 , with the number t increases, the optimal blocksize β_0 as well as the logarithms of the costs $\log_2\left(T_{\mathbf{pri}}^{(c)}\right), \log_2\left(T_{\mathbf{pri}}^{(q)}\right), \log_2\left(T_{\mathbf{du}}^{(c)}\right), \log_2\left(T_{\mathbf{du}}^{(q)}\right)$ all decrease linearly. We know that the complexities for dual attack and primal attack are quite similar for most cryptosystems, this phenomenon is also inherited after adding hints. On average, in both cases, each modular hint can reduce the required blocksize by approximately 1, and multiple hints always result in a significant cost reduction. For examples, with just 100 hints, the blocksize can be reduced by 101 and the time complexity can be reduced by a factor of 2^{30} in both attacks in the classical case. Although the blocksize can only be taken as an integer in the BKZ algorithm, regarding it as a real number leads to relatively smooth curves of m_0' and m_0 in the primal attack. The left-hand figure in table 1 shows the case where the precision of β is set to 0.1. As for the dual attack, computing m_0' in equation (6) without rounding also gives a smoother result.

Table 2: Dual attack with hints against Newhope1024.

t	m_0'	m_0	β_0	$\log_2\left(T_{\mathbf{du}}^{(c)}\right)$	$\log_2\left(T_{\mathbf{du}}^{(q)}\right)$
0	2048	1024	882	257.54	233.73
100	1882	958	781	228.05	206.97
200	1691	867	683	199.44	181.00
300	1498	774	585	170.82	155.03
400	1305	681	489	142.79	129.59
500	1108	584	394	115.05	104.41



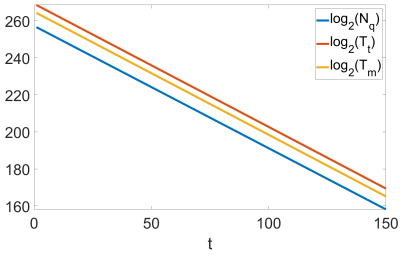
6.2 BKW attack

The setting of BKW attack is that an LWE oracle is given, i.e. we assume access to an unbounded number of LWE samples. The situations where different numbers of hints are added to an instance of Regev cryptosystem [33] with parameters $n = 384, q = 147457, \sigma_\chi = 39.19$ are shown in table 3.

We set the success rate of the algorithm to be $0.99 \cdot \left(\frac{\Phi(q)}{q}\right)^2 \approx 0.989987$. Then, for each number t, the following parameters are listed. The optimal addition depth α_0 that minimizes the cost, and its corresponding number of queries to the LWE oracle N_q. We denote the time complexity by T_t and the memory complexity by T_m.

Table 3: BKW attack with hints against Regev cryptosystem $(384, 147457, 39.19)$.

t	α_0	$\log_2(N_q)$	$\log_2(T_t)$	$\log_2(T_m)$
0	25	257.23	269.18	264.93
30	25	237.42	249.26	245.00
60	25	217.61	229.32	225.06
90	25	197.80	209.37	205.11
120	25	177.98	189.40	185.15
150	25	158.17	169.42	165.16



To give a more intuitive display of the changes in complexities after adding hints, we assume that $\beta = \frac{n-t}{\alpha+1} \in \mathbb{R}^*$, which has very little effect on the results. As we shall

see, $\log_2(N_q), \log_2(T_t), \log_2(T_m)$ all decrease linearly as t increases. With 90 hints, the number of queries can be decreased by a factor of 2^{60}, as do the time complexity T_t and memory complexity T_m. Moreover, it is mentioned in [3] that, the optimal α_0 usually depends on σ_χ and q. That is the reason why α_0 stays the same in table 3.

References

1. Albrecht, M., Deo, A., Paterson, K.: Cold boot attacks on ring and module lwe keys under the ntt. IACR Transactions on Cryptographic Hardware and Embedded Systems pp. 173–213 (08 2018). https://doi.org/10.46586/tches.v2018.i3.173-213
2. Albrecht, M.R., Cid, C., Faugère, J.C., Fitzpatrick, R., Perret, L.: Algebraic algorithms for lwe problems. ACM Communications in Computer Algebra **49**, 62 (aug 2015). https://doi.org/10.1145/2815111.2815158
3. Albrecht, M.R., Cid, C., Faugere, J.C., Fitzpatrick, R., Perret, L.: On the complexity of the bkw algorithm on lwe. Designs, Codes and Cryptography **74**(2), 325–354 (2015)
4. Albrecht, M.R., Faugère, J.C., Fitzpatrick, R., Perret, L.: Lazy modulus switching for the bkw algorithm on lwe. In: Krawczyk, H. (ed.) Public-Key Cryptography – PKC 2014. pp. 429–445. Springer Berlin Heidelberg (2014)
5. Albrecht, M.R., Göpfert, F., Virdia, F., Wunderer, T.: Revisiting the expected cost of solving usvp and applications to lwe. In: Takagi, T., Peyrin, T. (eds.) Advances in Cryptology – ASIACRYPT 2017. pp. 297–322. Springer International Publishing, Cham (2017)
6. Alkim, E., Avanzi, R., Bos, J., Ducas, L., de la Piedra, A., Pöppelmann, T., Schwabe, P., Stebila, D., Albrecht, M.R., Orsini, E., et al.: Newhope algorithm specifications and supporting documentation. NIST PQC Round **2** (2019)
7. Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P.: Post-quantum key Exchange—A new hope. In: 25th USENIX Security Symposium (USENIX Security 16). pp. 327–343. USENIX Association, Austin, TX (Aug 2016)
8. Amiet, D., Curiger, A., Leuenberger, L., Zbinden, P.: Defeating newhope with a single trace. In: Ding, J., Tillich, J.P. (eds.) Post-Quantum Cryptography – PQC 2020. pp. 189–205. Springer International Publishing, Cham (2020)
9. Applebaum, B., Cash, D., Peikert, C., Sahai, A.: Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In: Halevi, S. (ed.) Advances in Cryptology - CRYPTO 2009. pp. 595–618. Springer Berlin Heidelberg (2009)
10. Arora, S., Ge, R.: New algorithms for learning in presence of errors. In: Aceto, L., Henzinger, M., Sgall, J. (eds.) Automata, Languages and Programming. pp. 403–415. Springer Berlin Heidelberg (2011)
11. Avanzi, R., Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Seiler, G., Stehlé, D.: Crystals-kyber algorithm specifications and supporting documentation. NIST PQC Round **3** (2021)
12. Bos, J.W., Friedberger, S., Martinoli, M., Oswald, E., Stam, M.: Assessing the feasibility of single trace power analysis of frodo. In: Cid, C., Jacobson Jr., M.J. (eds.) Selected Areas in Cryptography – SAC 2018. pp. 216–234. Springer International Publishing, Cham (2018)
13. Budroni, A., Guo, Q., Johansson, T., Mårtensson, E., Wagner, P.S.: Making the bkw algorithm practical for lwe. In: Bhargavan, K., Oswald, E., Prabhakaran, M. (eds.) Progress in Cryptology – INDOCRYPT 2020. pp. 417–439. Springer International Publishing, Cham (2020)
14. Chen, Y.: Réduction de réseau et sécurité concrete du chiffrement completement homomorphe. Ph.D. thesis, Paris 7 (2013)

15. Dachman-Soled, D., Ducas, L., Gong, H., Rossi, M.: Lwe with side information: Attacks and concrete security estimation. In: Advances in Cryptology – CRYPTO 2020. pp. 329–358. Springer International Publishing, Cham (08 2020). https://doi.org/10.1007/978-3-030-56880-1_12
16. D'Anvers, J.P., Batsleer, S.: Multitarget decryption failure attacks and their application to saber and kyber. In: Hanaoka, G., Shikata, J., Watanabe, Y. (eds.) Public-Key Cryptography – PKC 2022. pp. 3–33. Springer International Publishing, Cham (2022)
17. D'Anvers, J.P., Guo, Q., Johansson, T., Nilsson, A., Vercauteren, F., Verbauwhede, I.: Decryption failure attacks on ind-cca secure lattice-based schemes. In: Lin, D., Sako, K. (eds.) Public-Key Cryptography – PKC 2019. pp. 565–598. Springer International Publishing, Cham (2019)
18. D'Anvers, J.P., Rossi, M., Virdia, F.: (one) failure is not an option: Bootstrapping the search for failures in lattice-based encryption schemes. In: Canteaut, A., Ishai, Y. (eds.) Advances in Cryptology – EUROCRYPT 2020. pp. 3–33. Springer International Publishing, Cham (2020)
19. Duc, A., Tramèr, F., Vaudenay, S.: Better algorithms for lwe and lwr. In: Oswald, E., Fischlin, M. (eds.) Advances in Cryptology – EUROCRYPT 2015. pp. 173–202. Springer Berlin Heidelberg (2015)
20. Guo, Q., Johansson, T., Mårtensson, E., Stankovski, P.: Coded-bkw with sieving. In: Takagi, T., Peyrin, T. (eds.) Advances in Cryptology – ASIACRYPT 2017. pp. 323–346. Springer International Publishing, Cham (2017)
21. Guo, Q., Johansson, T., Nilsson, A.: A key-recovery timing attack on post-quantum primitives using the fujisaki-okamoto transformation and its application on frodokem. In: Micciancio, D., Ristenpart, T. (eds.) Advances in Cryptology – CRYPTO 2020. pp. 359–386. Springer International Publishing, Cham (2020)
22. Guo, Q., Johansson, T., Stankovski, P.: Coded-bkw: Solving lwe using lattice codes. In: Gennaro, R., Robshaw, M. (eds.) Advances in Cryptology – CRYPTO 2015. pp. 23–42. Springer Berlin Heidelberg (2015)
23. Horlemann, A.L., Puchinger, S., Renner, J., Schamberger, T., Wachter-Zeh, A.: Information-set decoding with hints. In: Wachter-Zeh, A., Bartz, H., Liva, G. (eds.) Code-Based Cryptography. pp. 60–83. Springer International Publishing, Cham (2021)
24. Kirchner, P., Fouque, P.A.: An improved bkw algorithm for lwe with applications to cryptography and lattices. In: Gennaro, R., Robshaw, M. (eds.) Advances in Cryptology – CRYPTO 2015. pp. 43–62. Springer Berlin Heidelberg (2015)
25. Lenstra, A., Lenstra, H., László, L.: Factoring polynomials with rational coefficients. Mathematische Annalen **261**, 515–534 (12 1982). https://doi.org/10.1007/BF01457454
26. Li, S., Lu, X., Zhang, J., Li, B., Bi, L.: Predicting the concrete security of lwe against the dual attack using binary search. In: Gao, D., Li, Q., Guan, X., Liao, X. (eds.) Information and Communications Security. pp. 265–282. Springer International Publishing, Cham (2021)
27. Lu, X., Liu, Y., Zhang, Z., Jia, D., Xue, H., He, J., Li, B., Wang, K.: Lac: Practical ring-lwe based public-key encryption with byte-level modulus. Cryptology ePrint Archive, Report 2018/1009 (2018)
28. Lyness, J.N., Sørevik, T., Keast, P.: Notes on integration and integer sublattices. Math. Comp. **56**, 243–255 (1991). https://doi.org/10.1090/S0025-5718-1991-1052101-8
29. Martinet, J.: Perfect Lattices in Euclidean Spaces, vol. 327 (01 2003). https://doi.org/10.1007/978-3-662-05167-2
30. Micciancio, D., Regev, O.: Lattice-based cryptography. In: Bernstein, D.J., Buchmann, J., Dahmen, E. (eds.) Post-Quantum Cryptography – PQCrypto 2009. pp. 147–191. Springer Berlin Heidelberg (01 2009). https://doi.org/10.1007/978-3-540-88702-7_5
31. Pessl, P., Prokop, L.: Fault attacks on cca-secure lattice kems p. 37–60 (Feb 2021). https://doi.org/10.46586/tches.v2021.i2.37-60

32. Pohst, M.: A modification of the lll reduction algorithm. Journal of Symbolic Computation **4**, 123–127 (08 1987). https://doi.org/10.1016/S0747-7171(87)80061-5
33. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing. p. 84–93. STOC '05, Association for Computing Machinery, New York, NY, USA (2005). https://doi.org/10.1145/1060590.1060603
34. Zhao, C., Zheng, Z., Wang, X., Xu, G.: Distinguishing LWE instances using fourier transform: A refined framework and its applications. Cryptology ePrint Archive, Report 2019/1231 (2019), https://eprint.iacr.org/2019/1231

A The proof of proposition 1

For any $z \in \Lambda_p(A^T)$, suppose that $z = A\xi \pmod p$, then

$$(\Pi_A)_p \cdot z = A(A^T A)_p^{-1} A^T \cdot A\xi = A\xi = z \pmod p.$$

For any $y \in \Lambda_p^{\perp}(A^T)$, $A^T y = 0 \pmod p$, then

$$(\Pi_A)_p \cdot y = A(A^T A)_p^{-1} A^T \cdot y = 0 \pmod p.$$

B The proof of lemma 7

$$\begin{aligned}\text{vol}\left(\Lambda \cap \text{Span}(\Psi)^{\perp}\right) &= \frac{1}{\text{vol}\left((\Lambda \cap \text{Span}(\Psi)^{\perp})^*\right)} = \frac{1}{\text{vol}\left(\Pi_{\Psi}^{\perp} \cdot \Lambda^*\right)} = \frac{\text{vol}\left(\Lambda^* \cap \text{Span}(\Psi)\right)}{\text{vol}\left(\Lambda^*\right)} \\ &= \text{vol}\left(L(\Psi)\right) \cdot \text{vol}(\Lambda) = \sqrt{\det\left(\Psi^T \cdot \Psi\right)} \cdot \text{vol}(\Lambda).\end{aligned}$$

C The proof of proposition 4

Let us take $\Lambda_p(\mathtt{D}^T) = \Lambda_p^{\perp}(\mathtt{B}^T)$ as an example. Since $\mathtt{B}^T\mathtt{D} = O_{t\times(n-t)}$, it is easy to see that $\Lambda_p(\mathtt{D}^T) \subseteq \Lambda_p^{\perp}(\mathtt{B}^T)$. Conversely, when $\gcd\left(\det(\mathtt{B}^T\mathtt{B}), p\right) = 1$, from theorem 1, for any $x \in \mathbb{Z}^n$, we can suppose that $x = \mathtt{B}w + \mathtt{D}v + pu$, where $w \in \mathbb{Z}^t, v \in \mathbb{Z}^{n-t}$ and $u \in \mathbb{Z}^n$. Hence, if $x \in \Lambda_p^{\perp}(\mathtt{B}^T)$, then $0 = \mathtt{B}^T x = \mathtt{B}^T\mathtt{B}w \pmod p$. As $(\mathtt{B}^T\mathtt{B})_p^{-1}$ exists, we have $w = 0 \pmod p$. That means $x = \mathtt{D}v \pmod p$, i.e. $x \in \Lambda_p(\mathtt{D}^T)$.

D The proof of proposition 5

When $\gcd\left(\det(\mathtt{B}^T\mathtt{B}), p\right) = 1$, from corollary 1 and proposition 4, for any $v \in \mathbb{Z}^n$, it could be decomposed into $v = x + y + qu$, where $x \in \Lambda_p(\mathtt{B}^T) = \Lambda_p^{\perp}(\mathtt{D}^T), y \in \Lambda_p(\mathtt{D}^T) = \Lambda_p^{\perp}(\mathtt{B}^T)$ and $u \in \mathbb{Z}^n$. Then according to proposition 1,

$$((\Pi_{\mathtt{B}})_p + (\Pi_{\mathtt{D}})_p) \cdot v = (\Pi_{\mathtt{B}})_p \cdot v + (\Pi_{\mathtt{D}})_p \cdot v = x + y = v \pmod p.$$

E $\boldsymbol{L'_{\mathbf{pri}}(W,g) = L_{\mathbf{pri}}(W,g)}$

To show that $L'_{\mathbf{pri}}(W,g) = L_{\mathbf{pri}}(W,g)$, we only need to prove that $L_{\mathbf{pri}}(W,g) \subseteq \Lambda_q^{\perp}\left(\overline{P}\right)$, i.e. $\overline{P}^T \cdot B_{\mathbf{pri}}(W,g) = 0 \pmod q$.

As $\overline{P} = \begin{pmatrix} P \\ -K^T \end{pmatrix}$ and $B_{\mathbf{pri}}(W,g) = \begin{pmatrix} -I_{n-t} & 0 & 0 \\ W & qI_{m-n+t} & g \\ 0 & 0 & 1 \end{pmatrix}$, in the following, we shall show that (a) $P^T \cdot \begin{pmatrix} -I_{n-t} \\ W \end{pmatrix} = 0 \pmod q$ and (b) $P^T \cdot \begin{pmatrix} 0 \\ g \end{pmatrix} - K = 0 \pmod q$.

(a) Firstly, we reformulate W as $W = V'_{[n-t+1:m]} = -V_{[n-t+1:m]} \cdot \left(V_{[1:n-t]}\right)_q^{-1} = -A_{[n-t+1:m]} D_q^{\sim T} \left(A_{[1:n-t]} D_q^{\sim T}\right)_q^{-1} \pmod q$, then

$$P^T \cdot \begin{pmatrix} -I_{n-t} \\ W \end{pmatrix} = (X_2^T - X_1^T A_q^{\sim}) \cdot \begin{pmatrix} -I_{n-t} \\ -A_{[n-t+1:m]} D_q^{\sim T} \left(A_{[1:n-t]} D_q^{\sim T}\right)_q^{-1} \end{pmatrix}$$

$$= (X_2^T - X_1^T A_q^{\sim}) \cdot \begin{pmatrix} -I_{n-t} \\ -A_{[n-t+1:m]} D_q^{\sim T} \left(A_{[1:n-t]} D_q^{\sim T}\right)_q^{-1} \end{pmatrix} \cdot (A_{[1:n-t]} D_q^{\sim T}) \cdot \left(A_{[1:n-t]} D_q^{\sim T}\right)_q^{-1}$$

$$= (X_1^T A_q^{\sim} - X_2^T) \begin{pmatrix} A_{[1:n-t]} D_q^{\sim T} \\ A_{[n-t+1:m]} D_q^{\sim T} \end{pmatrix} \cdot \left(A_{[1:n-t]} D_q^{\sim T}\right)_q^{-1} = (X_1^T A_q^{\sim} - X_2^T) A D_q^{\sim T} \cdot \left(A_{[1:n-t]} D_q^{\sim T}\right)_q^{-1}$$

$$= (X_1^T - X_2^T A) \mathtt{D}_q^{\sim T} \left(A_{[1:n-t]} D_q^{\sim T}\right)_q^{-1} = 0 \pmod q,$$

since $X_1 - A^T X_2 \in \mathbb{Z}^n \cap \mathscr{V}$ and $\mathtt{D}$ is a basis of $\mathbb{Z}^n \cap \mathscr{V}^{\perp}$. Also because of this,

$$P^T \begin{pmatrix} 0 \\ g \end{pmatrix} - K = P^T c' - K = P^T (V'x + e) - K = P^T V' x = (X_1^T A_q^{\sim} - X_2^T) \cdot V (V_{[1:n-t]})_q^{-1} x$$

$$= (X_1^T A_q^{\sim} - X_2^T) \cdot A \cdot \mathtt{D}_q^{\sim T} \cdot (V_{[1:n-t]})_q^{-1} \cdot x = (X_1^T - X_2^T) \cdot \mathtt{D}_q^{\sim T} \cdot (V_{[1:n-t]})_q^{-1} \cdot x = 0 \pmod q.$$

F The proof of proposition 6

We denote $\Psi' = \begin{pmatrix} \frac{\psi_1}{l_1} & \cdots & \frac{\psi_t}{l_t} \end{pmatrix} \subseteq \mathbb{R}^{m \times t}$. As it is a set of primitive vectors with respect to Λ^*, it can be extended to a basis $\overline{\Psi'} = (\Psi' \star)$ of Λ^*, where the data in $\star$ could be omitted. Then $\overline{\Psi'}^{\sim T}$ is a basis of Λ and $\overline{\Psi'}^T \cdot \Lambda = \overline{\Psi'}^T \cdot \overline{\Psi'}^{\sim T} \mathbb{Z}^n = \mathbb{Z}^n$.

On the other hand, since $\overline{\Psi'}^T \cdot \Lambda = \begin{pmatrix} \Psi'^T \\ \star \end{pmatrix} \cdot \Lambda = \begin{pmatrix} \Psi'^T \cdot \Lambda \\ \star \end{pmatrix}$, we know that $\Psi'^T \cdot \Lambda = \mathbb{Z}^t$, i.e. $\left\langle \frac{\psi_j}{l_j}, \Lambda \right\rangle = \mathbb{Z}, j = 1, 2, \cdots, t$. This means that $\langle \psi_j, \Lambda \rangle = l_j \mathbb{Z}$ and $\langle \psi_j, \Lambda \rangle \pmod p = \mathbb{Z}_{\frac{p}{\gcd(p, l_j)}}, j = 1, 2, \cdots, t$. To sum up, we have

$$\Psi^T \Lambda \pmod p = \begin{pmatrix} \mathbb{Z}_{\frac{p}{\gcd(p,l_1)}} \\ \vdots \\ \mathbb{Z}_{\frac{p}{\gcd(p,l_t)}} \end{pmatrix} := \widetilde{\mathbb{Z}^t}.$$

We define the group morphism $\phi : \Lambda \to \widetilde{\mathbb{Z}^t}, x \mapsto \Psi^T x \pmod p$. It is an epimorphism and $\ker\phi = \Lambda \cap \Lambda_p^{\perp}(\Psi^T)$. Then from the fundamental homomorphism theorem,

$$\left| \frac{\Lambda}{\Lambda \cap \Lambda_p^{\perp}(\Psi^T)} \right| = \left| \widetilde{\mathbb{Z}^t} \right| = \left| \mathbb{Z}_{\frac{p}{\gcd(p,l_1)}} \right| \cdots \left| \mathbb{Z}_{\frac{p}{\gcd(p,l_t)}} \right| = \prod_{j=1}^{t} \frac{p}{\gcd(p, l_j)} = \frac{p^t}{\prod_{j=1}^{t} \gcd(p, l_j)}.$$

G A comparison

In [15], the adversary constructs the lattice $L_{\mathbf{pri}}(A,b) \subseteq \mathbb{Z}^{m+n+1}$ and searches the shortest non-zero vector of $L'_{\mathbf{pri}}(A,b) = L_{\mathbf{pri}}(A,b) \cap \Lambda_q^{\perp}(\overline{X}^T)$, where $\overline{X} = \begin{pmatrix} X \\ -J^T \end{pmatrix} \in \mathbb{Z}_q^{m+n+1}$. According to [15], this does not change the dimension of the lattice, i.e. $\dim\left(L'_{\mathbf{pri}}(A,b)\right) = \dim\left(L_{\mathbf{pri}}(A,b)\right) = m+n+1$. While from proposition 6, we know that $\mathrm{vol}\left(L'_{\mathbf{pri}}(A,b)\right) \leq q^t \cdot \mathrm{vol}\left(L_{\mathbf{pri}}(A,b)\right) = q^{m+t}$.

Different from [15], by our approach, when conditions in equation (5) are met, the dimension of the secret is bound to decrease by t using t modular hints. After all the transform steps, $\dim\left(L_{\mathbf{pri}}(W,g)\right) = m+1$ and $\mathrm{vol}\left(L_{\mathbf{pri}}(W,g)\right) = q^{m-n+t}$.

As we know, for a lattice, an increase in volume and a decrease in dimension both make it easier to solve the uSVP instance on it. Let β_0, β_1 be the optimal blocksize for the primal attack on $L_{\mathbf{pri}}(W,g)$ and $L'_{\mathbf{pri}}(A,b)$ respectively. Then we shall show that, $\beta_0 \leq \beta_1$ always holds when conditions in equation (5) are met. The equation holds only if $\mathrm{vol}\left(L'_{\mathbf{pri}}(A,b)\right) = q^{m+t}$. This is because in that case, from assumption 3,

$$\begin{aligned}
\beta_0 \quad &= \quad \mathrm{argmin}_{\beta\in\mathbb{N}^+}\left\{\exists m' > n,\ \text{s.t. } \sqrt{\beta}\cdot\sigma_\chi \leq \left(\delta_0(\beta)\right)^{2\beta-m'-2}\cdot q^{\frac{m'-n+t}{m'+1}}\right\} \\
&\overset{m=m'-n}{=\!=} \mathrm{argmin}_{\beta\in\mathbb{N}^+}\left\{\exists m \in \mathbb{N}^+,\ \text{s.t. } \sqrt{\beta}\cdot\sigma_\chi \leq \left(\delta_0(\beta)\right)^{2\beta-m-n-2}\cdot q^{\frac{m+t}{m+n+1}}\right\} = \beta_1.
\end{aligned}$$

To some extent, it shows that, an increase in volume by a factor of q^t has the same effect as a decrease in dimension by t.

Although the probability of $\mathrm{vol}\left(L'_{\mathbf{pri}}(A,b)\right) = q^{m+t}$ may be not low, there are also some other situations. An example is given as follows.

It is easy to see that $B_{\mathbf{pri}}^{-T}(A,b) = \begin{pmatrix} -I_n & \frac{A^T}{q} & 0 \\ 0 & \frac{1}{q}I_m & 0 \\ 0 & -\frac{1}{q}b^T & 1 \end{pmatrix}$ is a basis of $L_{\mathbf{pri}}(A,b)$. Hence, $\begin{pmatrix} I_t \\ O_{m\times t} \\ \star \end{pmatrix}$ $(t<n)$ is a set of primitive vectors of $L^*_{\mathbf{pri}}(A,b)$, where "$\star$" can be arbitrary. Now we suppose that q is a power of 2 and the hint description matrix $X = \begin{pmatrix} 2I_t \\ O_{m\times t} \end{pmatrix}$. Then, $J = X^T S = 2S_{[1:t]} \pmod q$ and $\overline{X} = \begin{pmatrix} 2I_t \\ O_{m\times t} \\ -2S_{[1:t]}^T \end{pmatrix}$. It is noticed that $\frac{1}{2}\overline{X}$ is primitive and from proposition 6, $\mathrm{vol}\left(L'_{\mathbf{pri}}(A,b)\right) = \frac{q^t}{2^t}\cdot\mathrm{vol}\left(L_{\mathbf{pri}}(A,b)\right) = \frac{q^{m+t}}{2^t}$.

Remark 9. It should be pointed out that, as the method of [15] requires a smaller number of samples, the matrix "A" in the attack against (A,b) should be a submatrix of the "A" in the attack against (W,g). But this does not affect our analysis above.