# Security of NewHope Under Partial Key Exposure

Dana Dachman-Soled*[1], Huijing Gong[1], Mukul Kulkarni**[2], and Aria Shahverdi[1]

[1] University of Maryland, College Park, USA
danadach@ece.umd.edu, gong@cs.umd.edu, ariash@umd.edu
[2] University of Massachusetts, Amherst, USA
mukul@cs.umass.edu

**Abstract.** Recently, several works have studied a leakage model that assumes leakage of some fraction of the NTT coordinates of the secret key in RLWE cryptosystems (or equivalently, intentionally sampling secrets with some fraction of NTT coordinates set to 0) [21,9]. This can be viewed as a partial key exposure problem, since for efficiency purposes, secret keys in RLWE cryptosystems are typically stored in their NTT representation. We extend this study by analyzing the security of the NewHope key exchange scheme under partial key exposure of 1/8-fraction of the NTT coordinates of the parties' secrets. We adopt the formalism of the decision Leaky-RLWE (Leaky-DRLWE) assumption introduced in [21], which posits that given leakage on a sufficiently small fraction of NTT coordinates of the secret, the remaining coordinates of the output remain indistinguishable from uniform. We note that the assumption of [21] is strictly weaker than the corresponding assumption of [9], which requires that the entire output remain indistinguishable from uniform. We show that, assuming that Leaky-DRLWE is hard for 1/8-fraction of leakage, the shared key $v$ (which is then hashed using a random oracle) is computationally indistinguishable from a random variable with average min-entropy 237, conditioned on the transcript and leakage, whereas without leakage the min-entropy is 256. Note that $2 \cdot 1738$ number of bits of information are leaked in this leakage model, and so the fact that any entropy remains in the shared 256-bit key is non-trivial.

## 1 Introduction

The cryptographic community is currently developing "post-quantum" cryptosystems — cryptosystems believed to remain secure even in the presence of a

* This work was supported in part by NSF grants #CNS-1933033, #CNS-1840893, #CNS-1453045 (CAREER), by a research partnership award from Cisco and by financial assistance award 70NANB15H328 from the U.S. Department of Commerce, National Institute of Standards and Technology.

** Part of this work was done while the author was a student at the University of Maryland.

quantum adversary — to replace known quantum-insecure cryptosystems based on the factoring and discrete log assumptions. One of the foremost avenues for efficient, post-quantum public key cryptography is the construction of cryptosystems from the Ring-LWE (RLWE) assumption. RLWE is often preferred in practice over standard LWE due to its algebraic structure, which allows for smaller public keys and more efficient implementations. In the RLWE setting, we typically consider rings of the form $R_q := \mathbb{Z}_q[x]/(x^n+1)$, where $n$ is a power of two and $q \equiv 1 \mod 2n$. The (decisional) RLWE problem is then to distinguish $(a, b = a \cdot s + e) \in R_q \times R_q$ from uniformly random pairs, where $s \in R_q$ is a random secret, the $a \in R_q$ is uniformly random and the error term $e \in R$ has small norm. A critical question is whether the additional algebraic structure of the RLWE problem renders it less secure than the standard LWE problem. Interestingly, to the best of our knowledge—for the rings used in practice and for practical parameter settings—the best attacks on RLWE are generic and can equally well be applied to standard LWE [45]. However, the situation with respect to robustness under leakage is quite different. While LWE is known to retain its security under leakage, as long as the secret has sufficiently high min-entropy conditioned on the leakage [32], the same is not always true for RLWE, as shown in several recent works [21,9]. In this work, we explore leakage models under which RLWE-based cryptosystems *can* be proven secure.

*The NTT transform.* A key technique for fast computation in the RLWE setting is usage of the *NTT transform* (similar to the Discrete Fourier Transform (DFT), but over finite fields) to allow for faster polynomial multiplication over the ring $R_q$. Specifically, applying the NTT transform to two polynomials $\boldsymbol{p}, \boldsymbol{p'} \in R_q$—resulting in two $n$-dimensional vectors, $\widehat{\boldsymbol{p}}, \widehat{\boldsymbol{p}}' \in \mathbb{Z}_q^n$—allows for *component-wise* multiplication and addition, which is highly efficient . Typically, the RLWE secret will then be stored in NTT form, and so leakage of coordinates of the NTT transform is a natural way to model partial key exposure attacks.

*NewHope key exchange protocol.* Our results focus on analysis of the NewHope key exchange protocol of [4] in the presence of partial key exposure. Briefly, NewHope key exchange is a post-quantum key exchange protocol that has been considered as a good candidate for practical implementation, due to its computational efficiency and low communication. Specifically, Google has experimented with large-scale implementation of NewHope in their Chrome browser [14] to determine the feasibility of switching over to post-quantum key exchange in the near-term.

*This work.* The goal of this work is to further the study of partial key exposure in RLWE based cryptosystems, initiated in [21] and [9]. Specifically, we adopt the notion of the decisional versions of Leaky RLWE assumptions introduced in [21], where the structured leakage occurs on the coordinates of the NTT transform of the LWE secret (and/or error) and analyze the security of the NewHope key exchange protocol under the decision version of the assumption.

### 1.1 Leaky RLWE Assumptions–Search and Decision Versions

We next briefly introduce the search and decision versions of the Leaky RLWE assumptions.

For $\boldsymbol{p} \in R_q := \mathbb{Z}_q/(x^n+1)$ we denote $\widehat{\boldsymbol{p}} := \mathsf{NTT}(\boldsymbol{p}) := (\boldsymbol{p}(\omega^1), \boldsymbol{p}(\omega^3), \ldots, \boldsymbol{p}(\omega^{2n-1}))$, where $\omega$ is a primitive $2n$-th root of unity modulo $q$, and is guaranteed to exist by choice of prime $q$, s.t. $q \equiv 1 \mod 2n$. Note that $\widehat{\boldsymbol{p}}$ is indexed by the set $\mathbb{Z}^*_{2n}$.

The search version of the Ring-LWE problem with leakage, denoted SRLWE, is parameterized by $(n' \in \{1,2,4,8,\ldots n\}, \mathcal{S} \subseteq \mathbb{Z}^*_{2n'})$. The goal is to recover the RLWE secret $\boldsymbol{s} = \mathsf{NTT}^{-1}(\widehat{\boldsymbol{s}})$, given samples from the distribution $D_{real,n',\mathcal{S}}$ which outputs $\left(\widehat{\boldsymbol{a}}, \widehat{\boldsymbol{a}} \cdot \widehat{\boldsymbol{s}} + \widehat{\boldsymbol{e}}, [\widehat{s_i}]_{i \equiv \alpha \bmod 2n' \,|\forall \alpha \in \mathcal{S}}\right)$, where $\boldsymbol{a}, \boldsymbol{s}$, and $\boldsymbol{e}$ are as in the standard RLWE assumption.

The decision version of the Ring-LWE problem with leakage, denoted DRLWE is parameterized by $(n' \in \{1,2,4,8,\ldots n\}, \mathcal{S} \subseteq \mathbb{Z}^*_{2n'})$. The goal is to distinguish the distributions $D_{real,n',\mathcal{S}}$ and $D_{sim,n',\mathcal{S}}$, where $D_{real,n',\mathcal{S}}$ is as above and $D_{sim,n',\mathcal{S}}$ outputs $\left(\widehat{\boldsymbol{a}}, \widehat{\boldsymbol{u}}, [\widehat{s_i}]_{i \equiv \alpha \bmod 2n' \,|\forall \alpha \in S}\right)$, where $\widehat{u_i} = \widehat{a_i} \cdot \widehat{s_i} + \widehat{e_i}$ for $i \equiv \alpha \mod 2n'$, $\alpha \in \mathcal{S}$ and $\widehat{u_i}$ is chosen uniformly at random from $\mathbb{Z}_q$, otherwise.

When $\mathcal{S} = \{\alpha\}$ consists of a single element, we abuse notation and write the Leaky-RLWE parameters as $(n', \alpha)$. Due to automorphisms on the NTT transform, Leaky-RLWE with parameters $(n', \mathcal{S})$ where $\mathcal{S} = \{\alpha_1, \alpha_2, \ldots, \alpha_t\}$, is equivalent to Leaky-RLWE with parameters $(n', \mathcal{S}')$, where $\mathcal{S}' = \alpha_1^{-1} \cdot S$ (multiply every element of $S$ by $\alpha_1^{-1}$).

### 1.2 Our Results

We show the following:

**Theorem 1.1 (Informal).** *Assuming that Leaky-DRLWE with leakage parameters $(8, \alpha = 1)$ and RLWE parameters $n = 1024, q = 12289$ and error distribution $\chi$[3] is hard, the shared key $v$ (which is then hashed using a random oracle) of the NewHope key exchange protocol is computationally indistinguishable from a random variable with average min-entropy 237, conditioned on the transcript and leakage of $[\hat{s}, \hat{e}, \hat{s}', \hat{e}', \hat{e}'']_{i \equiv \alpha \mod 16}$.*

Moreover, using known relationships between average min-entropy and min-entropy, we have that with all but $2^{-80}$ probability, the shared key $v$ is indistinguishable from a random variable that has min-entropy 157, conditioned on the transcript and leakage. Note that without leakage, the min-entropy is only 256. This means that the number of leaked bits is far larger than the min-entropy, so the fact that any entropy remains is non-trivial. Indeed, bounding the remaining entropy will require precise analysis of the "key reconciliation" step of the NewHope algorithm.

As mentioned above, due to automorphisms on the NTT transform [38], setting $\alpha = 1$ is WLOG, and $\alpha$ can be any value in $\mathbb{Z}^*_{16}$. While the above may

[3] $\chi$ is a rounded Gaussian with standard deviation $\sqrt{8}$, as in the NewHopew.

seem straightforward, given that we are already assuming hardness of Leaky-DRLWE, the challenge comes not in the computational part of the analysis (which indeed essentially substitutes instances of Leaky-DRLWE for instances of DRLWE), but in the information-theoretic part of the analysis. Specifically, we must show that given the adversary's additional knowledge about $\boldsymbol{v}$, as well as the transcript, which includes the reconciliation information (corresponding to the output of a randomized function of $\boldsymbol{v}$), the input $v$ to the random oracle still has sufficiently high min-entropy. For a discussion of our proof techniques, see Section 1.3.

The above theorem could be made more general, and stated in asymptotic form for broader settings of leakage parameters $(n', \mathcal{S})$. However, there is one step in the proof that is not fully generic (although we believe it should hold for wide ranges of parameters) and so for simplicity we choose to state the theorem in terms of the concrete parameters above. Very informally, for the proof to go through, we need to argue existence of a vector of a certain form, where existence depends on the parameter settings of $n$, $q$, $n'$ and $\mathcal{S}$. For this step of the proof we can apply a heuristic argument and we confirm existence experimentally for the concrete parameter settings. We discuss the details of the heuristic argument in Section 4.4.

*Choice of $n' = 8$ in Theorem 1.1.* Experimental results from prior work indicated that the search version of Leaky RLWE is easy for parameters $(n', \alpha = 1)$, where $n' = 4$ (recall that setting $\alpha = 1$ is WLOG), and seems hard for parameters $(n', \alpha = 1)$, where $n' = 8$ and $\alpha \in \mathbb{Z}_{16}^*$. This, combined with their search-to-decision reduction, support the conjecture that the decision version of Leaky RLWE holds (i.e. $D_{real,8,1} \approx D_{sim,8,1}$), for the NewHope parameter settings of $n = 1024$, $q = 12289$, and $\chi = \Psi_{16}$, where $\Psi_{16}$ is centered binomial distribution with parameter 16. [4]

### 1.3 Technical Overview

**Overview of NewHope Algorithm.** We start with an overview of the NewHope key-exchange protocol of [3] and then provide the necessary details relevant to this work. The protocol starts by server $P_1$ choosing a uniform random polynomial from ring $R_q$ as public key $\boldsymbol{a}$ (note that the elements of $R_q$ are polynomials) and sharing it with client $P_2$. Both $P_1$ and $P_2$ sample the RLWE secrets (resp. errors) $\boldsymbol{s}$ and $\boldsymbol{s'}$ locally. The parties then exchange the RLWE samples $\boldsymbol{b}, \boldsymbol{u}$.

At this point both the parties share an approximate of shared secret $\boldsymbol{a} \cdot \boldsymbol{s} \cdot \boldsymbol{s'}$. $P_2$ then generates some additional information $\boldsymbol{r}$ using $P_1$'s RLWE instance $\boldsymbol{b}$, and shares it with $P_1$. Both the parties then apply a reconciliation function $\mathsf{Rec}$ on their approximate inputs locally. The protocol ensures that after running $\mathsf{Rec}$, the parties agree on the exact same value $v$.

Finally, the parties apply hash function on $v$ (as instantiation of random oracle) to agree on the key. Thus, the security proof can now rely on the unpre-

[4] The centered binomial distribution is defined in Section 4.1.

dictability of random oracle on input $v$, rather than arguing that $v$ is indistinguishable from a uniform random value.

**Resilience of NewHope to Partial Key Exposure.** Recall that $P_2$ generates additional information $\boldsymbol{r}$ for $P_1$, which is generated by applying a function $\mathsf{HelpRec}$ locally on input $\boldsymbol{v}$ derived using $P_1$'s RLWE instance $\boldsymbol{b}$ and $P_2$'s secret $\boldsymbol{s}'$. The ring element $\boldsymbol{v} \in \mathbb{Z}_q^n$ that is input to the $\mathsf{HelpRec}$ function in the NewHope protocol is split into vectors $\mathbf{x}_i \in \mathbb{Z}_q^4$, $i \in \{0, \ldots, n/4-1\}$ and then the $\mathsf{HelpRec}$ function is run individually on each $\mathbf{x}_i$. It is not hard to show that, under the Leaky-DRLWE assumption, the distribution over the $\mathbf{x}_i$ (given the transcript and the leakage), for $i \in \{n/8, \ldots, n/4-1\}$ is indistinguishable from uniform random in $\mathbb{Z}_q^4$ and for $i \in \{0, \ldots, n/8-1\}$, is indistinguishable from uniform random, given a single linear constraint. Specifically, for $i \in \{0, \ldots, n/8-1\}$, the $\mathbf{x}_i$ is uniform random, conditioned on $\boldsymbol{c}_{\omega,\alpha} \cdot \mathbf{x}_i = \gamma_i$, for a known $\boldsymbol{c}_{\omega,\alpha}$ and $\gamma_i$. The technically difficult part of the proof is showing that, with high probability over $\gamma_i$, the min-entropy of $\mathsf{Rec}(\mathbf{x}_i, \mathbf{r}_i)$ is close to 1, conditioned on *both* the output of $\mathsf{HelpRec}(\mathbf{x}_i; b) = \mathbf{r}_i$ (for a bit $b \in \{0,1\}$) and the linear constraint $\boldsymbol{c}_{\omega,\alpha} \cdot \mathbf{x}_i = \gamma_i$. This indicates that the probability of guessing the corresponding bit is close to $1/2$, even with respect to an adversary who sees *both* the transcript and the leakage.

We handle this by showing the existence of a bijective map: $(\mathbf{x}_i, b') \to (\mathbf{x}'_i, b' \oplus 1)$ such that, $\mathsf{HelpRec}(\mathbf{x}_i, b) = \mathsf{HelpRec}(\mathbf{x}'_i, b')$ $(= \mathbf{r})$ with high probability $1-p$, and it guarantees $\mathsf{Rec}(\mathbf{x}_i, \mathbf{r}) = 1 \oplus \mathsf{Rec}(\mathbf{x}'_i, \mathbf{r})$. Specifically, we set $\mathbf{x}' = \mathbf{x} + \mathbf{w}$ as the bijective relation. Unlike the original proof from NewHope protocol where $\mathbf{w}_i = (b - b' + q)(1/2, 1/2, 1/2, 1/2)$, we need $\mathbf{w}_i$ to be close to $(q/2, q/2, q/2, q/2)$ and also satisfy an additional linear constraint $\boldsymbol{c}_{\omega,\alpha} \cdot \mathbf{w}_i = 0$ to ensure $\boldsymbol{c}_{\omega,\alpha} \cdot \mathbf{x}'_i = \gamma_i$, which is the information that can be derived about $\mathbf{x}_i$ for $i \in \{0, \ldots, n/8-1\}$ from the leakage. In this setting, we can easily prove that if $\mathsf{HelpRec}(\mathbf{x}_i, b) = (\mathbf{x}_i, b)$ $(= \mathbf{r})$ then $\mathsf{Rec}(\mathbf{x}_i, \mathbf{r}) = 1 \oplus \mathsf{Rec}(\mathbf{x}'_i, \mathbf{r})$ following similar argument as in NewHope paper. Then it remains to show that $\mathsf{HelpRec}(\mathbf{x}_i, b) = \mathsf{HelpRec}(\mathbf{x}'_i, b')$ $(= \mathbf{r})$ with high probability $1-p$. Since $\mathsf{HelpRec}(\mathbf{x}; b) = \mathsf{CVP}_{\tilde{D}_4}\left(\frac{2^r}{q}(\mathbf{x} + b\mathbf{g})\right)$ mod $2^r$ as defined, it is equivalent to prove $\mathsf{CVP}_{\tilde{D}_4}(\mathbf{z}) = \mathsf{CVP}_{\tilde{D}_4}(\mathbf{z} + \boldsymbol{\beta})$ with high probability $1-p$, where $\mathbf{z}, \boldsymbol{\beta}$ are variables that depend on $\mathbf{x}, \mathbf{w}$ which are later defined explicitly in Section 4.1. [5] We then analyze the case-by-case probability that algorithm $\mathsf{CVP}_{\tilde{D}_4}$ on input $\mathbf{z}$ and on input $\mathbf{z} + \boldsymbol{\beta}$ disagree in the first three steps and eventually bound the probability that $\mathsf{CVP}_{\tilde{D}_4}(\mathbf{z}) \neq \mathsf{CVP}_{\tilde{D}_4}(\mathbf{z} + \boldsymbol{\beta})$.

### 1.4 Related Work

*Partial key exposure.* There is a large body of work on partial key exposure attacks on RSA, beginning with the seminal work of Boneh et al. [10]. Partial key exposure attacks on RSA are based on a cryptanalytic method known as

[5] Here, $\mathbf{v}' = \mathsf{CVP}_{\mathcal{L}}(\mathbf{v})$ denotes, the output of running Closest Vector Problem solver, on input vector $\mathbf{v}$, which returns vector $\mathbf{v}'$ which is the closest lattice vector to $\mathbf{v}$ in lattice $\mathcal{L}$. The lattice $\tilde{D}_4$, is defined in Section 4.1.

Coppersmith's method [19,18]. There has been a long sequence of improved partial key exposure attacks on RSA, see for example [8,30,48,50].

*Leakage-resilient cryptography.* The study of provably secure, leakage-resilient cryptography was introduced by the work of Dziembowski and Pietrzak in [29]. Pietrzak [46] also constructed a leakage-resilient stream-cipher. Brakerski et al. [16] showed how to construct a schemes secure against an attacker who leaks at each time period. There are other works as well considering continual leakage [26,36]. There are also work on leakage-resilient signature scheme [35,13,40].

*Robustness of Lattice-based scheme.* One of the first and important work is by Goldwasser et al. [33] which shows that LWE is secure even in the cases where secret key is taken from an arbitrary distribution with sufficient entropy and even in the presence of hard-to-invert auxiliary inputs. Additionally they constructed a symmetric-key encryption scheme based on standard LWE assumption, that is robust to secret key leakage. Authors of [1] showed that the public-key scheme of [47] is robust against an attacker which can measure large fraction of secret key without increasing the size of secret key. Dodis et al. [27] presented construction in the case where the leakage is a one way function of the secret (exponentially hard to invert). Their construction are related to LWE assumptions. Dodis et al. [25] presented a construction of public-key cryptosystems based on LWE in the case where the adversary is given any computationally uninvertible function of the secret key. Albrecht et al. [2] consider the ring-LWE and investigate cold boot attacks on schemes based on these problem. They specifically looked into two representation of secret key, namely, polynomial coefficients and encoding of the secret key using a number theoretic transform (NTT). Dachman-Soled et al. [20] considered the leakage resilience of a RLWE-based public key encryption scheme for specific leakage profiles. Stange [49] ishowed that given multiple samples of RLWE instances such that the public key for every instance lies in some specific subring, one can reduce the original RLWE problem to multiple independent RLWE problems over the subring.

Recently, Bolboceanu et al. [9] considered the setting of "Order LWE," where the LWE secret is sampled from an *order*. One example of this considered by [9] is sampling the RLWE secret from an ideal $I \subseteq qR$. It is straightforward to see that sampling the RLWE secret uniformly at random from $R_q$ and then leaking the NTT coordinates $i$ such that $i = \alpha \mod 2n'$ is *equivalent* to sampling the RLWE secret from the ideal $I$ that containsgit those elements whose NTT transform is 0 in positions $i$ such that $i = \alpha \mod 2n'$. Bolboceanu et al. [9] present both positive results (cases in which a security reduction can still be proved) and a negative result (cases in which the LWE assumption can be broken). However, when fixes the leakage rate to 1/8, neither of these results covers practical parameter ranges of dimension, modulus and noise rate. As mentioned previously, their decisional assumption is strictly stronger than the assumption adopted in this work. In recent work of Brakerski and Döttling [15] it was shown that the distributions with sufficiently high noise lossiness will lead to hard instances of entropic LWE, which are special kind of LWE samples where the distrubtion of the secret can be from a family of distributions.

*Lattice-based key exchange.* An important research direction is the design of practical, lattice-based key exchange protocols, which are post-quantum secure. Some of the most influential proposed key exchange protocols include those introduced by Ding [24], Peikert [43], and the NewHope protocol of Alkim et al. [4]. We also mention the Frodo protocol of Bos et al. [11], the Kyber protocol of Bos et al [12], the NTRU protocol of Chen at al. [17], the Round5 protocol of Garcia-Morchon et al. [31], the SABER protocol of D'Anvers et al. [23], the Threebears protocols of Hamburg [34], the NTRU Prime protocol of Bernstein et al. [7], and the LAC protocol of Lu et al. [37], which are the other lattice-based KEMs that were selected as candidates for Round 2 of the NIST Post-Quantum Cryptography standardization effort.

## 2 Preliminaries

For a positive integer $n$, we denote by $[n]$ the set $\{0, \ldots, n-1\}$. We denote vectors in boldface $\boldsymbol{x}$ and matrices using capital letters $\boldsymbol{A}$. For vector $\boldsymbol{x}$ over $\mathbb{R}^n$ or $\mathbb{C}^n$, define the $\ell_2$ norm as $\|\boldsymbol{x}\|_2 = \left(\sum_i |x_i|^2\right)^{1/2}$. We write as $\|\boldsymbol{x}\|$ for simplicity. We use the notation $\approx_{t(n),p(n)}$ to indicate that adversaries running in time $t(n)$ can distinguish two distributions with probability at most $p(n)$.

### 2.1 Lattices and background

Let $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ denote the cycle, i.e. the additive group of reals modulo 1. We also denote by $\mathbb{T}_q$ its cyclic subgroup of order $q$, i.e., the subgroup given by $\{0, 1/q, \ldots, (q-1)/q\}$.

Let $H$ be a subspace, defined as $H \subseteq \mathbb{C}^{\mathbb{Z}_m^*}$, (for some integer $m \geq 2$),

$$H = \{\boldsymbol{x} \in \mathbb{C}^{\mathbb{Z}_m^*} : x_i = \overline{x_{m-i}}, \forall i \in \mathbb{Z}_m^*\}.$$

A *lattice* is a discrete additive subgroup of $H$. We exclusively consider the full-rank lattices, which are generated as the set of all linear integer combinations of some set of $n$ linearly independent *basis* vectors $B = \{\boldsymbol{b}_j\} \subset H$:

$$\Lambda = \mathcal{L}(B) = \left\{ \sum_j z_j \boldsymbol{b}_j : z_j \in \mathbb{Z} \right\}.$$

The *determinant* of a lattice $\mathcal{L}(B)$ is defined as $|\det(B)|$, which is independent of the choice of basis $B$. The *minimum distance* $\lambda_1(\Lambda)$ of a lattice $\Lambda$ (in the Euclidean norm) is the length of a shortest nonzero lattice vector.

The *dual lattice* of $\Lambda \subset H$ is defined as following, where $\langle \cdot, \cdot \rangle$ denotes the inner product.

$$\Lambda^\vee = \{\boldsymbol{y} \in H : \forall \boldsymbol{x} \in \Lambda, \langle \boldsymbol{x}, \overline{\boldsymbol{y}} \rangle = \sum_i x_i y_i \in \mathbb{Z}\}.$$

Note that, $(\Lambda^\vee)^\vee = \Lambda$, and $\det(\Lambda^\vee) = 1/\det(\Lambda)$.

**Theorem 2.1.** *Let $\mathcal{L} \subseteq \mathbb{R}^n$ be a full dimensional lattice, and let $B$ denote a basis of $\mathcal{L}$. Let $K \subseteq \mathbb{R}^n$ be a convex body. Let $\varepsilon > 0$ denote a scaling such that $\mathcal{P}(B) \cup -\mathcal{P}(B) \subseteq \varepsilon K$. For all $r > \varepsilon$, we have that*

$$(r-\varepsilon)^n \frac{\mathrm{Vol_n(K)}}{\det(\mathcal{L})} \leq |rK \cap \mathcal{L}| \leq (r+\varepsilon)^n \frac{\mathrm{Vol_n(K)}}{\det(\mathcal{L})}.$$

*Proof.* Details can be found in [22]. □

### 2.2 Volume of Hypercube Clipped by One Hyperplane

In this subsection, we consider a unit hypercube and a half hyperspace over $n$-dimension and want to know volume of their intersection, which can be handled by the following theorem.

Let $[n]$ be an ordered set $\{0, 1, \ldots, n-1\}$. Let $|\cdot|$ denote the cardinality of a set. For $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1}) \in \mathbb{R}^n$, we define $\mathbf{v}_0$ as $\mathbf{v}_0 := \{i \in [n] \mid v_i = 0\}$. Let $F^0$ be a set of all vertices that each coordinate is either 0 or 1, written as $F^0 = \{(v_0, v_1, \ldots, v_{n-1}) \mid v_i = 0 \text{ or } 1 \text{ for all } i.\}$.

**Theorem 2.2.** *([6], revisited by [41, Theorem 1])*

$$\mathrm{vol}([0,1]^n \cap H^+) = \sum_{\mathbf{v} \in F^0 \cap H^+} \frac{(-1)^{|\mathbf{v}_0|} g(\mathbf{v})^n}{n! \prod_{t=1}^n a_t},$$

where the half space $H_1^+$ is defined by

$$\{\mathbf{t} \mid g(\mathbf{t}) := \mathbf{a} \cdot \mathbf{t} + r_1 = a_0 x_0 + a_1 x_1 + \cdots + a_{n-1} x_{n-1} + r_1 \geq 0\}$$

with $\prod_{t=1}^n a_t \neq 0$.

We now present some background on Algebraic Number Theory.

### 2.3 Algebraic Number Theory

For a positive integer $m$, the $m^{th}$ *cyclotomic number field* is a field extension $K = \mathbb{Q}(\zeta_m)$ obtained by adjoining an element $\zeta_m$ of order $m$ (i.e. a primitive $m^{th}$ root of unity) to the rationals. The minimal polynomial of $\zeta_m$ is the $m^{th}$ *cyclotomic polynomial*

$$\Phi_m(X) = \prod_{i \in \mathbb{Z}_m^*} (X - \omega_m^i) \in \mathbb{Z}[X],$$

where $\omega_m \in \mathbb{C}$ is any primitive $m^{th}$ root of unity in $\mathbb{C}$.

For every $i \in \mathbb{Z}_m^*$, there is an embedding $\sigma_i : K \to \mathbb{C}$, defined as $\sigma_i(\zeta_m) = \omega_m^i$. Let $n = \varphi(m)$, the totient of $m$. The *trace* $\mathrm{Tr} : K \to \mathbb{Q}$ and *norm* $\mathrm{N} : K \to \mathbb{Q}$ can be defined as the sum and product, respectively, of the embeddings:

$$\mathrm{Tr}(x) = \sum_{i \in [n]} \sigma_i(x) \quad \text{and} \quad \mathrm{N}(x) = \prod_{i \in [n]} \sigma_i(x).$$

For any $x \in K$, the $l_p$ *norm* of $x$ is defined as $\|x\|_p = \|\sigma(x)\|_p = (\sum_{i\in[n]} |\sigma_i(x)|^p)^{1/p}$. We omit $p$ when $p = 2$. Note that the appropriate notion of norm $\|\cdot\|$ is used throughout this paper depending on whether the argument is a vector over $\mathbb{C}^n$, or whether the argument is an element from $K$; whenever the context is clear.

### 2.4 Ring of Integers and Its Ideals

Let $R \subset K$ denote the set of all algebraic integers in a number field $K$. This set forms a ring (under the usual addition and multiplication operations in $K$), called the *ring of integers* of $K$. Ring of integers in $K$ is written as $R = \mathbb{Z}[\zeta_m]$.

The (absolute) discriminant $\Delta_K$ of $K$ measures the geometric sparsity of its ring of integers. The discriminant of the $m^{th}$ cyclotomic number field $K$ is

$$\Delta_K = \left( \frac{m}{\prod\limits_{\text{prime } p|m} p^{1/(p-1)}} \right)^n \leq n^n,$$

in which the product in denominator runs over all the primes dividing $m$.

An (*integral*) *ideal* $\mathcal{I} \subseteq R$ is a non-trivial (i.e. $\mathcal{I} \neq \varnothing$ and $\mathcal{I} \neq \{0\}$) additive subgroup that is closed under multiplication by $R$, i,e., $r \cdot a \in \mathcal{I}$ for any $r \in R$ and $a \in \mathcal{I}$. The *norm* of an ideal $\mathcal{I} \subseteq R$ is the number of cosets of $\mathcal{I}$ as an addictive subgroup in $R$, defined as *index* of $\mathcal{I}$, i.e., $\mathrm{N}(\mathcal{I}) = |R/\mathcal{I}|$. Note that $\mathrm{N}(\mathcal{I}\mathcal{J}) = \mathrm{N}(\mathcal{I})\mathrm{N}(\mathcal{J})$.

A *fractional* ideal $\mathcal{I}$ in $K$ is defined as a subset such that $\mathcal{I} \subseteq R$ is an integral ideal for some nonzero $d \in R$. Its norm is defined as $\mathrm{N}(\mathcal{I}) = \mathrm{N}(d\mathcal{I})/\mathrm{N}(d)$. An *ideal lattice* is a lattice $\sigma(\mathcal{I})$ embedded from a fractional ideal $\mathcal{I}$ by $\sigma$ in $H$. The determinant of an ideal lattice $\sigma(\mathcal{I})$ is $\det(\sigma(\mathcal{I})) = \mathrm{N}(\mathcal{I}) \cdot \sqrt{\Delta_K}$. For simplicity, however, most often when discussing about ideal lattice, we omit mention of $\sigma$ since no confusion is likely to arise.

**Lemma 2.3** ([39]). *For any fractional ideal $\mathcal{I}$ in a number field $K$ of degree $n$,*

$$\sqrt{n} \cdot N^{1/n}(\mathcal{I}) \leq \lambda_1(\mathcal{I}) \leq \sqrt{n} \cdot N^{1/n}(\mathcal{I}) \cdot \sqrt{\Delta_K^{1/n}}.$$

For any *fractional* ideal $\mathcal{I}$ in $K$, its *dual* ideal is defined as

$$\mathcal{I}^\vee = \{a \in K : \mathrm{Tr}(a\mathcal{I}) \subset \mathbb{Z}\}.$$

**Definition 2.4.** *For $R = \mathbb{Z}[\zeta_m]$, define $g = \prod_p (1-\zeta_p) \in R$, where $p$ runs over all* odd *primes dividing $m$. Also, define $t = \frac{\hat{m}}{g} \in R$, where $\hat{m} = \frac{m}{2}$ if $m$ is even, otherwise $\hat{m} = m$.*

The dual ideal $R^\vee$ of $R$ is defined as $R^\vee = \langle t^{-1} \rangle$, satisfying $R \subseteq R^\vee \subseteq \hat{m}^{-1}R$. For any fractional ideal $\mathcal{I}$, its dual is $\mathcal{I}^\vee = \mathcal{I}^{-1} \cdot R^\vee$. The quotient $R_q^\vee$ is defined as $R_q^\vee = R^\vee / qR^\vee$.

**Fact 2.5** ([39]). *Assume that $q$ is a prime satisfying $q = 1 \mod m$, so that $\langle q \rangle$ splits completely into $n$ distinct ideals of norm $q$. The prime ideal factors of $\langle q \rangle$ are $\mathfrak{q}_i = \langle q \rangle + \langle \zeta_m - \omega_m^i \rangle$, for $i \in \mathbb{Z}_m^*$. By Chinese Reminder Theorem, the natural ring homomorphism $R/\langle q \rangle \to \prod_{i\in\mathbb{Z}_m^*} (R/\mathfrak{q}_i) \cong (\mathbb{Z}_q^n)$ is an isomorphism.*

### 2.5 Ring-LWE

We next present the formal definition of the ring-LWE problem as given in [39].

**Definition 2.6** (**Ring-LWE Distribution**). *For a "secret" $s \in R_q^\vee$ (or just $R^\vee$) and a distribution $\chi$ over $K_\mathbb{R}$, a sample from the ring-*$\mathsf{LWE}$ *distribution $A_{s,\chi}$ over $R_q \times (K_\mathbb{R}/qR^\vee)$ is generated by choosing $a \leftarrow R_q$ uniformly at random, choosing $e \leftarrow \chi$, and outputting $(a, b = a \cdot s + e \bmod qR^\vee)$.*

**Definition 2.7** (**Ring-LWE, Average-Case Decision**). *The* average-case decision *version of the ring-*$\mathsf{LWE}$ *problem, denoted $DRLWE_{q,\chi}$, is to distinguish with non-negligible advantage between independent samples from $A_{s,\chi}$, where $s \leftarrow \chi$ is sampled from the error distribution, and the same number of uniformly random and independent samples from $R_q \times (K_\mathbb{R}/qR^\vee)$.*

**Theorem 2.8.** *[39, Theorem 2.22] Let $K$ be the $m^{\text{th}}$ cyclotomic number field having dimension $n = \varphi(m)$ and $R = \mathcal{O}_K$ be its ring of integers. Let $\alpha = \alpha(n) > 0$, and $q = q(n) \geq 2$, $q = 1 \bmod m$ be a $\mathsf{poly}(n)$-bounded prime such that $\alpha q \geq \omega(\sqrt{\log n})$. Then there is a polynomial-time quantum reduction from $\tilde{O}(\sqrt{n}/\alpha)$-approximate $\mathsf{SIVP}$ (or $\mathsf{SVP}$) on ideal lattices in $K$ to the problem of solving $DRLWE_{q,\chi}$ given only $l$ samples, where $\chi$ is the Gaussian distribution $D_\xi$ for $\xi = \alpha \cdot q \cdot (nl/\log(nl))^{1/4}$.*

### 2.6 Number Theoretic Transform (NTT)

Let $R_q := \mathbb{Z}_q[x]/x^n + 1$ be the ring of polynomials, with $n = 2^d$ for any positive integer $d$. Also, let $m = 2n$ and $q = 1 \bmod m$. For, $\omega$ a $m^{\text{th}}$ root of unity in $\mathbb{Z}_q$ the NTT of polynomial $\boldsymbol{p} = \sum_{i=0}^{n-1} p_i x^i \in R_q$ is define as,

$$\widehat{\boldsymbol{p}} = \mathsf{NTT}(\boldsymbol{p}) := \sum_{i=0}^{n-1} \widehat{p}_i x^i$$

where the NTT coefficients $\widehat{p}_i$ are defined as: $\widehat{p}_i = \sum_{j=0}^{n-1} p_j \omega^{j(2i+1)}$.

The function $\mathsf{NTT}^{-1}$ is the inverse of function $\mathsf{NTT}$, defined as

$$\boldsymbol{p} = \mathsf{NTT}^{-1}(\widehat{\boldsymbol{p}}) := \sum_{i=0}^{n-1} p_i x^i$$

where the NTT inverse coefficients $p_i$ are defined as: $p_i = n^{-1} \sum_{j=0}^{n-1} \widehat{p}_j \omega^{i(2j+1)}$.

We next present the definitions of min-entropy and average min-entropy.

### 2.7 Min-Entropy and Average Min-Entropy

**Definition 2.9** (Min-Entropy). *A random variable $X$ has* min-entropy *$k$, denoted $H_\infty(X) = k$, if*

$$\max_x \Pr[X = x] = 2^{-k}.$$

**Definition 2.10** (Average Min-Entropy)**.** *Let* $(X, Z)$ *be a pair of random variables. The* average min entropy *of* $X$ *conditioned on* $Z$ *is*

$$\tilde{H}_\infty(X \mid Z) \stackrel{def}{=} -\log E_{z \leftarrow Z} \max_x \Pr[X = x \mid Z = z].$$

**Lemma 2.11** ([28])**.** *For any* $\delta > 0$*,* $H_\infty(X \mid Z = z)$ *is at least* $\tilde{H}_\infty(X \mid Z) - \log(1/\delta)$ *with probability at least* $1 - \delta$ *over the choice of* $z$*.*

## 3 Search and Decisional RLWE with Leakage

In this section we define the search and decisional ring-LWE problem with structured leakage on the secret key (i.e. partial key exposure). The definition is similar to the definition 2.7.

Ring elements (polynomials) $\boldsymbol{p}$ are stored as a vector of their coefficients $(p_0, \ldots, p_{n-1})$. For $p \in R_q$ we denote $\widehat{\boldsymbol{p}} := \mathsf{NTT}(\boldsymbol{p}) := (\boldsymbol{p}(\omega^1), \boldsymbol{p}(\omega^3), \ldots, \boldsymbol{p}(\omega^{2n-1}))$, where $\omega$ is a $2n$-th primitive root of unity in $\mathbb{Z}_q$ (which exists since $q$ is prime and $q \equiv 1 \mod 2n$), and $\boldsymbol{p}(\omega^i)$ for $i \in \mathbb{Z}^*_{2n}$ denotes evaluation of the polynomial $\boldsymbol{p}$ at $\omega^i$. Note that $\widehat{\boldsymbol{p}}$ is indexed by the set $\mathbb{Z}^*_{2n}$.

**Definition 3.1** (**Ring-LWE, Search with Leakage**)**.** *The* search *version of the ring-*LWE *problem with leakage, denoted* $SRLWE_{q,\psi,n',\mathcal{S}}$*, is parameterized by* $(n' \in \{1, 2, 4, 8, \ldots n\}, \mathcal{S} \subseteq \mathbb{Z}^*_{2n'})$*. The experiment chooses* $\boldsymbol{s} \leftarrow \chi$*, where* $\boldsymbol{s} = \mathsf{NTT}^{-1}(\widehat{\boldsymbol{s}})$*. The goal of the adversary is to recover* $\boldsymbol{s}$*, given independent samples from the distribution* $D_{real,n',\mathcal{S}}$*, which outputs* $\left(\widehat{\boldsymbol{a}}, \widehat{\boldsymbol{a}} \cdot \widehat{\boldsymbol{s}} + \widehat{\boldsymbol{e}}, [\widehat{s_i}]_{i \equiv \alpha \bmod 2n' \mid \forall \alpha \in \mathcal{S}}\right)$ *where* $\boldsymbol{a}, \boldsymbol{e}$ *are obtained from* $A_{s,\psi}$ *as described in definition 2.6.*

**Definition 3.2** (**Ring-LWE, Decision with Leakage**)**.** *The* decision *version of the ring-*LWE *problem with leakage, denoted Leaky-*$DRLWE_{q,\psi,n',\mathcal{S}}$*, is parameterized by* $(n' \in \{1, 2, 4, 8, \ldots n\}, \mathcal{S} \subseteq \mathbb{Z}^*_{2n'})$*. The experiment chooses* $\boldsymbol{s} \leftarrow \chi$*, where* $\boldsymbol{s} = \mathsf{NTT}^{-1}(\widehat{\boldsymbol{s}})$*. The goal of the adversary is to distinguish between independent samples from the distributions* $D_{real,n',\mathcal{S}}$ *and* $D_{sim,n',\mathcal{S}}$*, where* $D_{real,n',\mathcal{S}}$ *outputs* $\left(\widehat{\boldsymbol{a}}, \widehat{\boldsymbol{a}} \cdot \widehat{\boldsymbol{s}} + \widehat{\boldsymbol{e}}, [\widehat{s_i}]_{i \equiv \alpha \bmod 2n' \mid \forall \alpha \in \mathcal{S}}\right)$ *where* $\boldsymbol{a}, \boldsymbol{e}$ *are obtained from* $A_{s,\psi}$ *as described in definition 2.6. And the* $D_{sim,n',\mathcal{S}}$ *outputs* $\left(\widehat{\boldsymbol{a}}, \widehat{\boldsymbol{u}}, [\widehat{s_i}]_{i \equiv \alpha \bmod 2n' \mid \forall \alpha \in S}\right)$ *where* $\boldsymbol{a}, \boldsymbol{e}$ *are obtained from* $A_{s,\psi}$ *as described in Definition 2.6,and*

$$\widehat{u_i} = \widehat{a_i} \cdot \widehat{s_i} + \widehat{e_i} \quad \mid \quad i \equiv \alpha \bmod 2n' \; \forall \alpha \in S$$

*and*

$$\widehat{u_i} \leftarrow \mathbb{Z}_q$$

*chosen uniformly random, otherwise.*

Note that in the above definitions, the adversary can receive the leakage $[\widehat{e_i}]_{i \equiv \alpha \bmod 2n' \mid \forall \alpha \in S}$ for each error vector as well, since given $\widehat{\boldsymbol{a}}$ and $[\widehat{s_i}]_{i \equiv \alpha \bmod 2n' \mid \forall \alpha \in S}$, the adversary can derive $[\widehat{e_i}]_{i \equiv \alpha \bmod 2n' \mid \forall \alpha \in S}$.

**Fact 3.3.** *If decisional RLWE with leakage parameterized by $(n', \mathcal{S})$ as above is hard for uniformly distributed $\widehat{\boldsymbol{a}}$, then it is also hard for $\widehat{\boldsymbol{a}}$ that is arbitrarily distributed in positions $i$ such that $i \equiv \alpha \mod 2n'$, $\alpha \in \mathcal{S}$ and uniformly distributed elsewhere.*

This is because given an RLWE instance with leakage $\left(\widehat{\boldsymbol{a}}, \widehat{\boldsymbol{u}}, [\widehat{s}_i]_{i \equiv \alpha \bmod 2n' \,|\forall \alpha \in S}\right)$, for $i \equiv \alpha \mod 2n'$, $\alpha \in \mathcal{S}$ one can change the instance from $\widehat{a}_i$ to $\widehat{a}'_i$ by adding $(\widehat{a}'_i - \widehat{a}_i) \cdot \widehat{s}_i$ from the $i$-th coordinate of $\widehat{\boldsymbol{u}}$.

When $\mathcal{S} = \{\alpha\}$ consists of a single element, we abuse notation and write the Leaky-RLWE parameters as $(n', \alpha)$.

## 4 Leakage Analysis of New Hope Key Exchange

### 4.1 New Hope Key Exchange scheme

It contains New Hope key exchange scheme and subroutines of HelpRec and Rec.

In this section we revise some important results and algorithms from [3].

Let $\tilde{D}_4$ be a lattice as defined below:

$$\tilde{D}_4 = \mathbb{Z}^4 \cup \boldsymbol{g} + \mathbb{Z}^4 \text{ where } \boldsymbol{g}^t = \left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right)$$

Let, $\boldsymbol{B} = (\boldsymbol{u}_0, \boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{g})$ be the basis of $\tilde{D}_4$, where $\boldsymbol{u}_i$ are the canonical basis vectors of $\mathbb{Z}^4$. Note that $\boldsymbol{u}_3 = \boldsymbol{B} \cdot (-1, -1, -1, 2)^t$. Also, let $\mathscr{V}$ be the Voronoi cell of $\tilde{D}_4$. [6]

Note that, $\boldsymbol{u}_0, \boldsymbol{u}_1, \boldsymbol{u}_2$, and $2\boldsymbol{g}$ are in $\mathbb{Z}^4$. Therefore, a vector in $\tilde{D}_4/\mathbb{Z}^4$ can be checked by simply checking the parity of its last coordinate when represented with basis $\boldsymbol{B}$. We can now use a simple encoding and decoding scheme to represent a bit. The encoding algorithm is as follows: $\mathsf{Encode}(k \in \{0,1\}) = k\boldsymbol{g}$. For decoding to $\tilde{D}_4/\mathbb{Z}^4$, the correctness requires that the error vector $\boldsymbol{e} \in \mathscr{V}$. As noted in [3], this is equivalent to checking if $\|\boldsymbol{e}\|_1 \leq 1$. We can now present the decoding algorithm as follows in figure 4.1 :

**Algorithm 4.1** (Algorithm 1)**.** Decode *($\boldsymbol{x} \in \mathbb{R}^4/\mathbb{Z}^4$)*

***Ensure:*** *A bit $k$ such that $k\boldsymbol{g}$ is a closest vector to $\boldsymbol{x} + \mathbb{Z}^4 : \boldsymbol{x} - k\boldsymbol{g} \in \mathscr{V} + \mathbb{Z}^4$*

1 $\quad \boldsymbol{v} = \boldsymbol{x} - \lfloor \boldsymbol{x} \rceil$
2 $\quad$ ***return*** *0 if $\|\boldsymbol{v}\|_1 \leq 1$ and 1 otherwise*

**Lemma 4.2.** *(Lemma C.1 [3]) For any $k \in \{0,1\}$ and any $\boldsymbol{e} \in \mathbb{R}^4$ such that $\|\boldsymbol{e}\|_1 < 1$, we have* $\mathsf{Decode}(k\boldsymbol{g} + \boldsymbol{e}) = k$.

[6] For more details and background on reconciliation mechanism of NewHope, please refer to [3] (section 5 and appendix C)

Let us now present the algorithm CVP (Closest Vector Problem), which will be used as subroutine in reconciliation algorithms, as follows:

**Algorithm 4.3** (Algorithm 2). $\mathsf{CVP}_{\tilde{D}_4}$ *($\boldsymbol{x} \in \mathbb{R}^4$)*

***Ensure:*** *An integer vector $\boldsymbol{z}$ such that $\boldsymbol{Bz}$ is a closest vector to $\boldsymbol{x}$ : $\boldsymbol{x} - \boldsymbol{Bz} \in \mathscr{V}$*

$\boldsymbol{v}_0 \leftarrow \lfloor \boldsymbol{x} \rceil$
$\boldsymbol{v}_1 \leftarrow \lfloor \boldsymbol{x} - \boldsymbol{g} \rceil$
***if*** $(\|\boldsymbol{x} - \boldsymbol{v}_0\| < 1)$ ***then*** $k \leftarrow 0$ ***else*** $k \leftarrow 1$
$(v_0, v_1, v_2, v_3)^t \leftarrow \boldsymbol{v}_k$
***return*** $(v_0, v_1, v_2, k)^t + v_3 \cdot (-1, -1, -1, 2)^t$

Next, we define the $r$-bit reconciliation as,

$$\mathsf{HelpRec}(\boldsymbol{x}; b) = \mathsf{CVP}_{\tilde{D}_4}\left(\frac{2^r}{q}(\boldsymbol{x} + b\boldsymbol{g})\right) \bmod 2^r,$$

where $b \in \{0, 1\}$ is a uniformly chosen random bit.

**Lemma 4.4.** *(Lemma C.2 [3]) Assume $r \geq 1$ and $q \geq 9$. For any $\boldsymbol{x} \in \mathbb{Z}_q^4$, set $\boldsymbol{r} := \mathsf{HelpRec}(\boldsymbol{x}) \in \mathbb{Z}_{2^r}^4$. Then, $\frac{1}{q}\boldsymbol{x} - \frac{1}{2^r}\boldsymbol{Br} \bmod 1$ is close to a point of $\tilde{D}_4/\mathbb{Z}^4$, precisely, for $\alpha = \frac{1}{2^r} + \frac{2}{q}$: $\frac{1}{q}\boldsymbol{x} - \frac{1}{2^r}\boldsymbol{Br} \in \alpha\mathscr{V} + \mathbb{Z}^4$ or $\frac{1}{q}\boldsymbol{x} - \frac{1}{2^r}\boldsymbol{Br} \in \boldsymbol{g} + \alpha\mathscr{V} + \mathbb{Z}^4$. Additionally, for $\boldsymbol{x}$ uniformly chosen in $\mathbb{Z}_q^4$ we have $\mathsf{Decode}\left(\frac{1}{q}\boldsymbol{x} - \frac{1}{2^r}\boldsymbol{Br}\right)$ is uniform in $\{0, 1\}$ and independent of $\boldsymbol{r}$.*

Let, $\mathsf{Rec}(\boldsymbol{x}, \boldsymbol{r}) = \mathsf{Decode}\left(\frac{1}{q}\boldsymbol{x} - \frac{1}{2^r}\boldsymbol{Br}\right)$.
We can now define the following reconciliation protocol:

**Algorithm 4.5** (Protocol 1). *Reconciliation protocol in $q\tilde{D}_4/q\mathbb{Z}^4$*

| ***Alice*** | | ***Bob*** |
|---|---|---|
| $\boldsymbol{x}' \in \mathbb{Z}_q^4$ | $\boldsymbol{x}' \approx \boldsymbol{x}$ | $\boldsymbol{x}' \in \mathbb{Z}_q^4$ |
| | $\xleftarrow{\boldsymbol{r}}$ | $\boldsymbol{r} \leftarrow \mathsf{HelpRec}(\boldsymbol{x}) \in \mathbb{Z}_{2^r}^4$ |
| $k' \leftarrow \mathsf{Rec}(\boldsymbol{x}', \boldsymbol{r})$ | | $k \leftarrow \mathsf{Rec}(\boldsymbol{x}, \boldsymbol{r})$ |

**Lemma 4.6.** *(Lemma C.3 [3]) If $\|\boldsymbol{x} - \boldsymbol{x}'\|_1 < \left(1 - \frac{1}{2^r}\right) \cdot q - 2$, then by the above protocol 4.5 $k = k'$. Additionally, if $\boldsymbol{x}$ is uniform, then $k$ is uniform independently of $\boldsymbol{r}$.*

We define centered binomial distribution $\Psi_{16}$ as the subtraction of two binomial distribution $B(16, 0.5)$ and $\Psi_{16}^n$ is $n$ draw from that distribution.

We now present the complete NewHope key exchange protocol given in [3] as protocol 4.7.

**Algorithm 4.7** (Protocol 2). *Parameters:* $q = 12289$, $n = 1024$ *Error Distribution:* $\Psi_{16}$

| ***Alice (server)*** | | ***Bob (client)*** |
|---|---|---|
| *Sample:* $\boldsymbol{a} \leftarrow R_q$ | | |
| $\boldsymbol{s}, \boldsymbol{e} \longleftarrow \Psi_{16}^n$ | | $\boldsymbol{s'}, \boldsymbol{e'}, \boldsymbol{e''} \longleftarrow \Psi_{16}^n$ |
| $\widehat{\boldsymbol{s}} := \mathsf{NTT}(\boldsymbol{s}), \widehat{\boldsymbol{e}} := \mathsf{NTT}(\boldsymbol{e})$ | | $\widehat{\boldsymbol{s}}' := \mathsf{NTT}(\boldsymbol{s'}), \widehat{\boldsymbol{e}}' := \mathsf{NTT}(\boldsymbol{e'})$ |
| | | $\widehat{\boldsymbol{e}}'' := \mathsf{NTT}(\boldsymbol{e''})$ |
| $\widehat{\boldsymbol{b}} := \widehat{\boldsymbol{a}} \cdot \widehat{\boldsymbol{s}} + \widehat{\boldsymbol{e}}$ | $\xrightarrow{\widehat{\boldsymbol{a}}, \widehat{\boldsymbol{b}}}$ | |
| | | $\widehat{\boldsymbol{u}} := \widehat{\boldsymbol{a}} \cdot \widehat{\boldsymbol{s}}' + \widehat{\boldsymbol{e}}'$ |
| | | $\widehat{\boldsymbol{v}} := \widehat{\boldsymbol{b}} \cdot \widehat{\boldsymbol{s}}' + \widehat{\boldsymbol{e}}''$ |
| | | $\boldsymbol{v} := \mathsf{NTT}^{-1}(\widehat{\boldsymbol{v}})$ |
| | $\xleftarrow{(\widehat{\boldsymbol{u}}, \boldsymbol{r})}$ | $\boldsymbol{r} \leftarrow \mathsf{HelpRec}(\boldsymbol{v})$ |
| $\boldsymbol{w} := \mathsf{NTT}^{-1}(\widehat{\boldsymbol{u}} \cdot \widehat{\boldsymbol{s}})$ | | $v \leftarrow \mathsf{Rec}(\boldsymbol{v}, \boldsymbol{r})$ |
| $v \leftarrow \mathsf{Rec}(\boldsymbol{w}, \boldsymbol{r})$ | | $\mu \leftarrow \mathsf{SHA3-256}(v)$ |
| $\mu \leftarrow \mathsf{SHA3-256}(v)$ | | |

### 4.2 Security with Auxiliary Inputs

In this section we consider a modification to Protocol 4.7 in which all binomial random variables are instead drawn from discrete Gaussians with corresponding standard deviation $\sigma$. Specifically, we assume that the coefficients of the secret and error vectors are drawn from $D_{\tilde{\sigma}}$ (a discretized, Gaussian distribution with probability mass function proportional to $e^{-\pi x^2/(\tilde{\sigma}^2)}$), where $\tilde{\sigma} = \sqrt{2\pi} \cdot \sigma$. [7]

We prove in Corollary 4.15 that the distribution over $v$, given the transcript of the modified protocol, is (with all but negligible probability) indistinguishable from a distribution with high min-entropy. By the analysis of [3] leveraging Renyi divergence and the random oracle model, this is sufficient to argue security in the presence of leakage.

The proof of Corollary 4.15 has two components. In the first (computational and information-theoretic) component (proof of Theorem 4.8), we analyze the distribution of $\boldsymbol{v}$, conditioned on the transcript that *does not include the reconciliation information* $\boldsymbol{r}$ and show that it is close to another distribution over $\boldsymbol{v'}$. In the second (information-theoretic only) component (proof of Theorem 4.9), we analyze the expected min-entropy of $v \leftarrow \mathsf{Rec}(\boldsymbol{v'}, \boldsymbol{r})$, conditioned on the adversary's view which now additionally includes the reconciliation information $\boldsymbol{r} \leftarrow \mathsf{HelpRec}(\boldsymbol{v'}, b)$. These are then combined to obtain Corollary 4.15.

The view of the adversary in the modified protocol consists of the tuple

$$\mathsf{View}_A := (\widehat{\boldsymbol{a}}, \widehat{\boldsymbol{b}}, \widehat{\boldsymbol{u}}, [\widehat{s}_i, \widehat{e}_i, \widehat{s}'_i, \widehat{e}'_i, \widehat{e}''_i]_{i \equiv \alpha \mod 2n'}).$$

[7] The proof of statistical closeness of binomial distribution $\Psi_{16}^n$, and discrete gaussian distribution with $\sigma = \sqrt{8}$ can be found in Appendix B of the papers [3,4] which introduced NewHope protocol.

Moreover, note that $\widehat{v}_i = \widehat{b}_i \cdot \widehat{s}'_i + \widehat{e}''_i$, so $[\widehat{v}_i]_{i \equiv \alpha \mod 2n'}$ is deducible from the view.

Let $\eta_\epsilon(\Lambda)$ be the smoothing parameter of lattice $\Lambda$ defined as follows:

$$\Lambda := \{\boldsymbol{w} \mid \langle (1, \omega^{n/n'}, \omega^{2n/n'}, \ldots, \omega^{(n'-1)n/n'}), \boldsymbol{w} \rangle = 0 \mod q\},$$

where $\omega$ is a $2n$-th primitive root of unity modulo $q$.

**Theorem 4.8.** *If the Ring-LWE decision problem with leakage is hard as defined in Section 3 with parameters $(n' = 8, \alpha \in \mathbb{Z}^*_{2n'})$, and error distribution $D_{\tilde{\sigma}}$, where $\tilde{\sigma} \geq \eta_\epsilon(\Lambda)$, then*

*(1) The marginal distribution over $[\widehat{v}_i]_{i \equiv \alpha \mod 2n'}$, is point-wise, multiplicatively $(1+\epsilon)^{n/n'}$-close to uniform random over $\mathbb{Z}_q^{n/n'}$, where we may set $\epsilon = 1/166$, when $n' = 8$ for NewHope parameters.*
*(2) Given the adversary's view, $\mathsf{View}_A$,*

$$[\widehat{v}_i]_{i \not\equiv \alpha \mod 2n'}$$

*is computationally indistinguishable from uniform random over $\mathbb{Z}_q^{n-n/n'}$.*

*Proof.* We prove the above theorem by considering the adversary's view in a sequence of hybrid distributions.
***Hybrid*** $H_0$**:** This is the real world distribution

$$(\widehat{\boldsymbol{a}}, \widehat{\boldsymbol{b}}, \widehat{\boldsymbol{u}}, [\widehat{s}_i, \widehat{e}_i, \widehat{s}', \widehat{e}'_i, \widehat{e}''_i]_{i \equiv \alpha \mod 2n'}, \widehat{\boldsymbol{v}}).$$

***Hybrid*** $H_1$**:** Here we replace $\tilde{\boldsymbol{b}}$ by $\widehat{\boldsymbol{b}}'$, where $\widehat{\boldsymbol{b}}'_i = \widehat{\boldsymbol{b}}_i$ for $i \equiv \alpha \mod 2n'$ and $\widehat{\boldsymbol{b}}'_i$ is chosen uniformly at random from $\mathbb{Z}_q$ for $i \not\equiv \alpha \mod 2n'$.

$$(\widehat{\boldsymbol{a}}, \widehat{\boldsymbol{b}}', \widehat{\boldsymbol{u}}, [\widehat{s}_i, \widehat{e}_i, \widehat{s}', \widehat{e}'_i, \widehat{e}''_i]_{i \equiv \alpha \mod 2n'}, \widehat{\boldsymbol{v}}).$$

**Claim 4.1.** $H_0 \approx H_1$

Claim 4.1 follows from the decision ring-LWE with leakage assumption Definition 3.2 and Fact 3.3.

***Hybrid*** $H_2$**:** This is same as hybrid $H_1$ except we replace $\widehat{\boldsymbol{u}}$ by $\widehat{\boldsymbol{u}}'$ and $\widehat{\boldsymbol{v}}$ by $\widehat{\boldsymbol{v}}'$, where $\widehat{\boldsymbol{u}}'_i = \widehat{\boldsymbol{u}}_i$, $\widehat{\boldsymbol{v}}'_i = \widehat{\boldsymbol{v}}_i$, for $i \equiv \alpha \mod 2n'$ and $\widehat{\boldsymbol{u}}'_i$, $\widehat{\boldsymbol{v}}'_i$ are chosen uniformly at random from $\mathbb{Z}_q$ for $i \not\equiv \alpha \mod 2n'$.

$$(\widehat{\boldsymbol{a}}, \widehat{\boldsymbol{b}}', \widehat{\boldsymbol{u}}', [\widehat{s}_i, \widehat{e}_i, \widehat{s}', \widehat{e}'_i, \widehat{e}''_i]_{i \equiv \alpha \mod 2n'}, \widehat{\boldsymbol{v}}').$$

**Claim 4.2.** $H_1 \approx H_2$

Claim 4.2 follows from the decision ring-LWE with leakage assumption Definition 3.2 and Fact 3.3.

We now analyze the distribution over $[\widehat{v}']_{i \equiv \alpha \mod 2n'}$ in Hybrid $H_2$. First, note that the distribution over $[\widehat{v}']_{i \equiv \alpha \mod 2n'}$ is unchanged in Hybrids $H_0, H_1, H_2$.

Further, we show that for every vector $\boldsymbol{w} \in Z_q^{n/n'}$, $\Pr[[\widehat{v}']_{i \equiv \alpha \mod 2n'} = \boldsymbol{w}] \leq \frac{(1+\epsilon)^{n/n'}}{q^{n/n'}}$ (for $\epsilon$ as in the statement of Theorem 4.8). In fact, we will show that the above holds for $[\widehat{e}'']_{i \equiv \alpha \mod 2n'}$ and use the fact that for $i \equiv \alpha \mod 2n'$, $\widehat{v}'_i = \widehat{e}''_i + \widehat{b}'_i \cdot \widehat{s}'_i = \widehat{e}''_i + \widehat{b}_i \cdot \widehat{s}'_i$. This is sufficient to prove item (1) of Theorem 4.8.

We observe that there is a bijection between the vector $[\widehat{e}''_i]_{i \equiv \alpha \mod 2n'}$ and the polynomial $\boldsymbol{f} := \boldsymbol{e}'' \mod (x^{n/n'} - (\omega^\alpha)^{n/n'})$, where $\omega$ is a $2n$-th primitive root of unity modulo $q$. We further assume WLOG that $\alpha = 1$, as this does not affect the computations, due to the ring automorphisms [38]. Now, each of the coordinates of $\boldsymbol{f}$ is equal to $f_i := [1, \omega^{n/n'}, \omega^{2n/n'}, \ldots, \omega^{(n'-1)n/n'}] \cdot [\boldsymbol{e}''_{i+j \cdot n/n'}]_{j \in \{0,\ldots,n'-1\}}$, where each coordinate of $\boldsymbol{e}''$ is drawn independently from $D_{\tilde{\sigma}}$ (a discretized, Gaussian distribution with probability mass function proportional to $e^{-\pi x^2/(\tilde{\sigma}^2)}$). Since the $n/n'$ coordinates of $\boldsymbol{f}$ are independent, it is sufficient to show that for each coordinate $f_i$, and any value $\tilde{f}_i \in Z_q$, $\Pr[f_i = \tilde{f}_i] \leq \frac{1+\epsilon}{q}$.

Towards this goal, consider the lattice $\Lambda$ defined as follows:

$$\Lambda := \{\boldsymbol{w} \mid \langle (1, \omega^{n/n'}, \omega^{2n/n'}, \ldots, \omega^{(n'-1)n/n'}), \boldsymbol{w} \rangle = 0 \mod q\}.$$

We will show that $\tilde{\sigma}$ is larger than the smoothing parameter, $\eta_\epsilon(\Lambda)$, of this lattice. By definition, this implies that for each coordinate $f_i$, and any value $\tilde{f}_i \in \mathbb{Z}_q$, $\Pr[f_i = \tilde{f}_i] \leq \frac{1+\epsilon}{q}$, which completes our argument.

We upperbound $\eta_\epsilon(\Lambda)$, via the bound of [42, Lemma 3.3] on the smoothing parameter of a lattice, observing that $\Lambda$ has dimension $n'$:

$$\eta_\epsilon(\Lambda) \leq \sqrt{\frac{\ln(2n'(1+1/\epsilon))}{\pi}} \cdot \lambda_{n'}(\Lambda), \tag{1}$$

where $\lambda_{n'}(\Lambda)$ is the $n'$-th successive minimum of $\Lambda$.

Now, we consider applying the above to NewHope parameter settings with $n' = 8$ and $\epsilon = 1/166$. Specifically, with standard deviation $\sigma = \sqrt{8}$ for error (as in NewHope), the discrete Gaussian with the same standard deviation has pdf proportional to

$$e^{-x^2/(2 \cdot \sigma^2)} = e^{-x^2/(2 \cdot \sqrt{8}^2)} = e^{-\pi x^2/(\sqrt{16 \cdot \pi}^2)} = e^{-\pi x^2/(\tilde{\sigma}^2)},$$

where $\tilde{\sigma} = 4\sqrt{\pi} \geq 7.0898154$.

Plugging in our parameters in (1), we have that $\eta_{1/166}(\Lambda) \leq \sqrt{\frac{\ln(16 \cdot 167)}{\pi}} \cdot \lambda_8(\Lambda)$, where and $\lambda_8(\Lambda)$ is upperbounded by the maximum length over the vectors in the reduced basis of $\Lambda$ output by the BKZ algorithm. Since $\Lambda$ is a dimension 8 lattice, we are able to efficiently compute $\lambda_8(\Lambda) \leq 4.472136$ using Sage's BKZ 2.0 implementation. Thus, we have that $\eta_{1/166}(\Lambda) \leq 7.08753 \leq \tilde{\sigma}$.

We conclude as we have now shown that (1) and (2) of Theorem 4.8 hold in Hybrid 2. □

*Switching from NTT to polynomial representation.* We showed that in Hybrid $H_2$, given fixed $[\widehat{v}'_i]_{i\equiv\alpha \bmod 2n'}$, the distribution over $[\widehat{v}'_i]_{i\not\equiv\alpha \bmod 2n'}$ is uniform random. We now characterize the induced distribution of $\mathbf{x} := \boldsymbol{v}'$ (i.e. the polynomial form), given $[\widehat{v}'_i]_{i\equiv\alpha \bmod 2n'}$. Henceforth, we assume for simplicity that $n' = 8$. Given $[\widehat{v}'_i]_{i\equiv\alpha \bmod 16}$ an attacker can recover $\boldsymbol{y}(x) = \boldsymbol{v}'(x) \mod (x^{n/8} - (\omega^\alpha)^{n/8})$. Thus the leaked information forms a linear equation as follow:

$$\sum_{k=0}^{7} (\omega^\alpha)^{\frac{kn}{8}} v'_{\frac{kn}{8}+i} = y_i,$$

where $i \in \{0, \ldots, n/8 - 1\}$.

For $i \in \{0, \ldots, n/8 - 1\}$, fix $v'_{\frac{kn}{8}+i}$, for $k \in \{1, 3, 5, 7\}$ then we have

$$\sum_{k=0}^{3} (\omega^\alpha)^{\frac{2kn}{n'}} v'_{\frac{2kn}{n'}+i} = y_i - \sum_{\kappa=0}^{3} (\omega^\alpha)^{\frac{(2k+1)n}{8}} v'_{\frac{(2k+1)n}{8}+i}. \tag{2}$$

Let $\gamma_i$ be the right hand side of (2). Let $\boldsymbol{c}_{\omega,\alpha} = [1 \ (\omega^\alpha)^{n/4} \ (\omega^\alpha)^{n/2} \ (\omega^\alpha)^{3n/4}]$. Thus the linear constraint corresponding to (2) can be written as $f_{\omega,j}(\mathbf{x}_i) := \boldsymbol{c}_{\omega,\alpha} \cdot \mathbf{x}_i = \gamma_i$, where $\mathbf{x}_i \in \mathbb{Z}_q^4$. Recall that due to automorphisms, we may assume $\alpha = 1$.

*Distributions over polynomial representation.* For every fixed setting of $[\widehat{v}'_i]_{i\equiv\alpha \bmod 2n'}$, the distribution over $[\mathbf{x}_i]_{i\in\{n/8,\ldots,n/4-1\}} = [\boldsymbol{v}'_{\frac{kn}{8}+j}]_{j\in\{0,\ldots,n/8-1\},k\in\{1,3,5,7\}}$ is uniform random. This corresponds to setting $\mathbf{x}_i \leftarrow \mathbb{Z}_q^4$ uniformly at random, for $i \in \{n/8, \ldots, n/4 - 1\}$. Given $[\widehat{v}'_i]_{i\equiv\alpha \bmod 2n'}$ and the fixed values of $\mathbf{x}_i$, the distribution over $[\mathbf{x}_i]_{i\in\{0,\ldots,n/8-1\}} = [v'_{\frac{kn}{8}+j}]_{j\in\{0,\ldots,n/8-1\},k\in\{0,2,4,6\}}$, which we denote by $\mathcal{S}_{\boldsymbol{\gamma}} = (\mathcal{S}_{\gamma_0}, \ldots, \mathcal{S}_{\gamma_{n/8-1}})$, corresponds to, for each $i \in \{0, \ldots, n/8 - 1\}$, choosing $\mathbf{x}_i \in \mathbb{Z}_q^4$ uniformly at random, conditioned on $\boldsymbol{c}_{\omega,\alpha} \cdot \mathbf{x}_i = \gamma_i$. Let $\Psi$ be the distribution over $\boldsymbol{\gamma}$.[8] Since (once we fix $[\mathbf{x}_i]_{i\in\{n/8,\ldots,n/4-1\}}$) there is a bijection between $[\widehat{v}'_i]_{i\equiv\alpha \bmod 2n'}$ and the values of the constraints $[\gamma_i]_{i\in\{0,\ldots,n/8-1\}}$, so by (1) of Theorem 4.8 we have that for every fixed $\tilde{\boldsymbol{\gamma}}$, $\Pr_\Psi[\boldsymbol{\gamma} = \tilde{\boldsymbol{\gamma}}] \leq \frac{(1+1/166)^{128}}{q^{n/8}}$.

*Analyzing the average min-entropy of $v$.* To summarize the analysis above, conditioned on the view of the adversary, for each $i \in \{n/8, \ldots, n/4-1\}$, $\mathbf{x}_i$ is sampled uniformly and independently. Once these values are fixed, we can consider the resulting distribution $\Psi$ over $\boldsymbol{\gamma} = \gamma_0, \ldots, \gamma_{n/8-1}$. For each $i \in \{0, \ldots, n/8 - 1\}$, $\mathbf{x}_i$ is sampled independently from $\mathcal{S}_{\gamma_i}$ (defined in the preceding paragraph).

Clearly, for $i \in \{n/8, \ldots, n/4 - 1\}$, since $\mathbf{x}_i \leftarrow \mathbb{Z}_q^4$ are sampled uniformly at random and independently, we can use the same analysis as in [3] to prove that, conditioned on the output of $\mathsf{HelpRec}$, the output of $\mathsf{Rec}$ for $i \in \{n/8, \ldots, n/4-1\}$ has (average) min-entropy exactly 1, conditioned on the leakage and transcript.

[8] Not to be confused with $\Psi_16$ which denotes a centered binomial distribution and was used as an error distribution in Section 4.1.

Thus, it remains to show that for $i \in \{0, \ldots, n/8-1\}$, conditioned on the output of $\mathsf{HelpRec}$, the output of $\mathsf{Rec}$ has high average min-entropy.

For $\gamma_i \in \mathbb{Z}_q$, recall that $\mathcal{S}_{\gamma_i}$ is the set of $\mathbf{x}_i \in \mathbb{Z}_q^4$ that satisfy $\boldsymbol{c}_{\omega,\alpha} \cdot \mathbf{x}_i = \gamma_i$. Note that the sets $\mathcal{S}_{\gamma_i}, \gamma_i \in \mathbb{Z}_q$ form a partition of $\mathbb{Z}_q^4$. Let $\mathcal{R}_{\gamma_i}$ be the distribution over outputs $\mathbf{r}$ of $\mathsf{HelpRec}(\mathbf{x}_i; b)$ when $\mathbf{x}_i$ is chosen uniformly at random from $\mathcal{S}_{\gamma_i}$ and $b$ is chosen uniformly at random from $\{0,1\}$.

For $i \in \{0, \ldots, n/8-1\}$, the average min-entropy of the output of $\mathsf{Rec}$, conditioned on the output of $\mathsf{HelpRec}$ is equal to:

$$-\log_2 \left( E_{\boldsymbol{\gamma} \leftarrow \Psi, [\mathbf{r}_i \sim \mathcal{R}_{\gamma_i}]_{i \in \{0,\ldots,n/8-1\}}} \left[ \prod \max_{\beta \in \{0,1\}} \Pr_{\substack{\mathbf{x}_i \sim \mathcal{S}_{\gamma_i} \\ b \sim \{0,1\}}} [\mathsf{Rec}(\mathbf{x}_i, \mathbf{r}_i) = \beta \mid \mathsf{HelpRec}(\mathbf{x}_i; b) = \mathbf{r}_i] \right] \right).$$

We can rewrite the above expression as follows:

$$E_{\boldsymbol{\gamma} \leftarrow \Psi, [\mathbf{r}_i \sim \mathcal{R}_{\gamma_i}]_{i \in \{0,\ldots,n/8-1\}}} \left[ \prod \max_{\beta \in \{0,1\}} \Pr_{\substack{\mathbf{x}_i \sim \mathcal{S}_{\gamma_i} \\ b \sim \{0,1\}}} [\mathsf{Rec}(\mathbf{x}_i, \mathbf{r}_i) = \beta \mid \mathsf{HelpRec}(\mathbf{x}_i; b) = \mathbf{r}_i] \right]$$

$$= \sum_{\boldsymbol{\gamma}} E_{[\mathbf{r}_i \sim \mathcal{R}_{\gamma_i}]_{i \in \{0,\ldots,n/8-1\}}} \left[ \prod \max_{\beta \in \{0,1\}} \Pr_{\substack{\mathbf{x}_i \sim \mathcal{S}_{\gamma_i} \\ b \sim \{0,1\}}} [\mathsf{Rec}(\mathbf{x}_i, \mathbf{r}_i) = \beta \mid \mathsf{HelpRec}(\mathbf{x}_i; b) = \mathbf{r}_i] \right] \cdot \Pr_{\Psi}[\boldsymbol{\gamma}]$$

$$\leq \sum_{\boldsymbol{\gamma}} E_{[\mathbf{r}_i \sim \mathcal{R}_{\gamma_i}]_{i \in \{0,\ldots,n/8-1\}}} \left[ \prod \max_{\beta \in \{0,1\}} \Pr_{\substack{\mathbf{x}_i \sim \mathcal{S}_{\gamma_i} \\ b \sim \{0,1\}}} [\mathsf{Rec}(\mathbf{x}_i, \mathbf{r}_i) = \beta \mid \mathsf{HelpRec}(\mathbf{x}_i; b) = \mathbf{r}_i] \right] \cdot \frac{(1+1/166)^{128}}{q^{n/8}}$$

$$= (1+1/166)^{128} E_{\boldsymbol{\gamma} \leftarrow Z_q^{n/8}, [\mathbf{r}_i \sim \mathcal{R}_{\gamma_i}]_{i \in \{0,\ldots,n/8-1\}}} \left[ \prod \max_{\beta \in \{0,1\}} \Pr_{\substack{\mathbf{x}_i \sim \mathcal{S}_{\gamma_i} \\ b \sim \{0,1\}}} [\mathsf{Rec}(\mathbf{x}_i, \mathbf{r}_i) = \beta \mid \mathsf{HelpRec}(\mathbf{x}_i; b) = \mathbf{r}_i] \right]$$

$$= (1+1/166)^{128} \prod_i E_{\gamma_i \leftarrow Z_q^{n/8}, [\mathbf{r}_i \sim \mathcal{R}_{\gamma_i}]_{i \in \{0,\ldots,n/8-1\}}} \left[ \max_{\beta \in \{0,1\}} \Pr_{\substack{\mathbf{x}_i \sim \mathcal{S}_{\gamma_i} \\ b \sim \{0,1\}}} [\mathsf{Rec}(\mathbf{x}_i, \mathbf{r}_i) = \beta \mid \mathsf{HelpRec}(\mathbf{x}_i; b) = \mathbf{r}] \right].$$

Thus, we can lower bound the average min-entropy of the output of $\mathsf{Rec}$ for all blocks $i \in \{0, \ldots, n/8-1\}$ by analyzing the expectation for a single block $E_{\gamma_i \leftarrow Z_q^{n/8}, [\mathbf{r}_i \sim \mathcal{R}_{\gamma_i}]_{i \in \{0,\ldots,n/8-1\}}} \left[ \max_{\beta \in \{0,1\}} \Pr_{\substack{\mathbf{x}_i \sim \mathcal{S}_{\gamma_i} \\ b \sim \{0,1\}}} [\mathsf{Rec}(\mathbf{x}_i, \mathbf{r}_i) = \beta \mid \mathsf{HelpRec}(\mathbf{x}_i; b) = \mathbf{r}_i] \right]$, taking the negative log, multiplying by 128 (the number of blocks) and subtracting $\log_2(1+1/166)^{128} \approx 1.1091$.

*Remark 4.2.1.* In the following, we drop the subscript $i$ from the variables $\mathbf{x}_i, \mathbf{r}_i, \gamma_i$, since we focus on a single block at a time.

**Theorem 4.9.** *We have that:*

$$E_{\gamma\leftarrow Z_q,\mathbf{r}\sim\mathcal{D}_\gamma}\left[\max_{\beta\in\{0,1\}}\Pr_{\substack{\mathbf{x}\sim\mathcal{S}_\gamma\\ b\sim\{0,1\}}}[\mathsf{Rec}(\mathbf{x},\mathbf{r})=\beta\mid\mathsf{HelpRec}(\mathbf{x};b)=\mathbf{r}]\right]\leq 1/2+p/2,$$

*where*

$$p:=2-2\left(\frac{\frac{q}{2^r}-2q^{1/4}-1}{\frac{q}{2^r}}\right)^4+\left(\frac{1+\frac{1}{2q^{1/4}}}{1-\frac{2^{r+1}}{q}}\right)^4\cdot\left(\frac{2^{r+10}}{3q^{3/4}}-\frac{2^{3r+10}}{3q^{9/4}}+\frac{2^{4r+10}}{q^3}\right)$$

.

*Proof.* We prove the theorem by showing that for linear constraint $\boldsymbol{c}_{\omega,\alpha}$, there exists a bijective mapping $\psi_{\boldsymbol{c}_{\omega,\alpha}}(\mathbf{x})=\mathbf{x}'$, such that, with high probability at least $1-p$ over uniform $\mathbf{x}$, all the following conditions hold:

$$\boldsymbol{c}_{\omega,\alpha}\cdot\mathbf{x}=\boldsymbol{c}_{\omega,\alpha}\cdot\mathbf{x}' \tag{3}$$

$$(\mathbf{r}=)\ \mathsf{HelpRec}(\mathbf{x};b)=\mathsf{HelpRec}(\mathbf{x}';b'), \tag{4}$$

$$\mathsf{Rec}(\mathbf{x},\mathbf{r})=1\oplus\mathsf{Rec}(\mathbf{x}',\mathbf{r}), \tag{5}$$

where $b'=b\oplus 1$.

Now the above conditions imply that:

$$\frac{1}{q}\cdot\sum_{(\gamma,\mathbf{r})}\Pr_{\mathcal{R}_\gamma}[\mathbf{r}]\cdot\Pr_{\substack{\mathbf{x}\sim\mathcal{S}_\gamma\\ b\sim\{0,1\}}}[\mathsf{HelpRec}(\mathbf{x};b)\neq\mathsf{HelpRec}(\mathbf{x}';b')\mid\mathsf{HelpRec}(\mathbf{x};b)=\mathbf{r}]\leq p. \tag{6}$$

Let $p_{\gamma,\mathbf{r}}:=\Pr_{\substack{\mathbf{x}\sim\mathcal{S}_\gamma\\ b\sim\{0,1\}}}[\mathsf{HelpRec}(\mathbf{x};b)\neq\mathsf{HelpRec}(\mathbf{x}';b')\mid\mathsf{HelpRec}(\mathbf{x};b)=\mathbf{r}]$. Note that $\max_{\beta\in\{0,1\}}\Pr_{\substack{\mathbf{x}\sim\mathcal{S}_\gamma\\ b\sim\{0,1\}}}[\mathsf{Rec}(\mathbf{x},\mathbf{r})=\beta\mid\mathsf{HelpRec}(\mathbf{x};b)=\mathbf{r}]\leq 1/2+p_{\gamma,\mathbf{r}}/2$.

This is sufficient to prove Theorem 4.9, since

$$\begin{aligned}
&E_{\gamma\leftarrow Z_q,\mathbf{r}\sim\mathcal{D}_\gamma}[\max_{\beta\in\{0,1\}}\Pr_{b\sim\{0,1\},\mathbf{x}\sim\mathcal{S}_\gamma}[\mathsf{Rec}(\mathbf{x},\mathbf{r})=\beta\mid\mathsf{HelpRec}(\mathbf{x};b)=\mathbf{r}]]\\
\leq&\frac{1}{q}\cdot\sum_{(\gamma,\mathbf{r})}\Pr_{\mathcal{R}_\gamma}[\mathbf{r}]\cdot(1/2+p_{\gamma,\mathbf{r}}/2)\\
=&1/2+\frac{1}{q}\cdot\sum_{(\gamma,\mathbf{r})}\Pr_{\mathcal{R}_\gamma}[\mathbf{r}]\cdot p_{\gamma,\mathbf{r}}/2\\
=&\frac{1}{2}+\frac{1}{2q}\sum_{(\gamma,\mathbf{r})}\Pr_{\mathcal{R}_\gamma}[\mathbf{r}]\cdot\Pr_{\substack{\mathbf{x}\sim\mathcal{S}_\gamma\\ b\sim\{0,1\}}}[\mathsf{HelpRec}(\mathbf{x};b)\neq\mathsf{HelpRec}(\mathbf{x}';b')\mid\mathsf{HelpRec}(\mathbf{x};b)=\mathbf{r}]\\
\leq&1/2+p/2,
\end{aligned}$$

where the last inequality follows from (6).

We now turn to defining $\psi_{\boldsymbol{c}_{\omega,\alpha}}$ and proving that with probability at least $1-p$ over uniform $\mathbf{x}$, (3), (4) and (5) hold.

*Defining $\psi_{\boldsymbol{c}_{\omega,\alpha}}$ so that (3) always holds.* (3) holds if and only if there exists a vector $\mathbf{w} \in \mathbb{Z}_q^4$ such that $\mathbf{x}' = \mathbf{x}+\mathbf{w}$, where $\mathbf{w} \in \ker(\boldsymbol{c}_{\omega,\alpha})$, where ker is the set of $\mathbf{w}'$ such that $\boldsymbol{c}_{\omega,\alpha} \cdot \mathbf{w}' = 0$. Let $\mathbf{W}$ to be a set of all vectors $\mathbf{vt} = (vt_0, vt_1, vt_2, vt_3)$ where $vt_i \in [\frac{q}{2} \pm q^{1/4}] \cap \mathbb{Z}$. By conducting an exhausive search, we observe that the intersection of set $\ker(\boldsymbol{c}_{\omega,\alpha})$ and set $\mathbf{W}$ is nonempty given parameter setting of [3], namely fixing $q = 12289, n = 1024, \omega = 7$, $\ker(f_{\omega,j}) \cap \mathbf{W} \neq \varnothing$ for all $\alpha \in \mathbb{Z}_{16}^*$. [9] Define $\psi_{\boldsymbol{c}_{\omega,\alpha}}(\mathbf{x}) := \mathbf{x} + \mathbf{w}$, where $\mathbf{w} \in \ker(\boldsymbol{c}_{\omega,\alpha}) \cap \mathbf{W}$. Therefore, as long as $\ker(\boldsymbol{c}_{\omega,\alpha}) \cap \mathbf{W}$ is non-empty (which holds for typical parameter settings), condition (3) holds with probability 1 over choice of $\mathbf{x}$.

*If (4) holds then (5) holds.* We now show that if $\mathbf{x}$ is such that $\mathsf{HelpRec}(\mathbf{x}; b) = \mathsf{HelpRec}(\mathbf{x} + \mathbf{w}; b')$ then if $\mathsf{HelpRec}(\mathbf{x}; b) = \mathbf{r}$, $\mathsf{Rec}(\mathbf{x}, \mathbf{r}) = 1 \oplus \mathsf{Rec}(\mathbf{x} + \mathbf{w}, \mathbf{r})$.

**Lemma 4.10.** *Given* $\mathsf{HelpRec}(\mathbf{x}; b) = \mathsf{HelpRec}(\mathbf{x} + \mathbf{w}; b') = \mathbf{r}$, $\mathsf{Rec}(\mathbf{x}, \mathbf{r}) = 1 \oplus \mathsf{Rec}(\mathbf{x} + \mathbf{w}, \mathbf{r})$.

*Proof.* Recall that $\mathbf{g} = (1/2, 1/2, 1/2, 1/2)^T$. Proved by [5, Lemma C.2], we have

$$\mathsf{HelpRec}(\mathbf{x}; b) = \mathsf{HelpRec}(\mathbf{x} + q\mathbf{g}) \quad (= \mathbf{r})$$
$$\mathsf{Rec}(\mathbf{x}, \mathbf{r}) = 1 \oplus \mathsf{Rec}(\mathbf{x} + q\mathbf{g}, \mathbf{r})$$

Additionally, since $\|\mathbf{w} - q\mathbf{g}\|_1 \leq 4q^{1/4} < (1 - 1/2^r) \cdot q - 2$, by [5, Lemma C.3], $\mathsf{Rec}(\mathbf{x} + \mathbf{w}, \mathbf{r}) = \mathsf{Rec}(\mathbf{x} + q\mathbf{g}, \mathbf{r})$, Thus we conclude $\mathsf{Rec}(\mathbf{x}, \mathbf{r}) = 1 \oplus \mathsf{Rec}(\mathbf{x} + \mathbf{w}, \mathbf{r})$. □

*(4) holds with probability $1 - p$ over $\mathbf{x}$.* Hence, it remains to show that for all $\mathbf{w} \in \ker(\boldsymbol{c}_{\omega,\alpha}) \cap \mathbf{W}$ and $f_{\omega,j}(\mathbf{x}) = \gamma$, with high probability at least $1 - p$ over choice of $\mathbf{x} \leftarrow \mathbb{Z}_q^4$, $b \leftarrow \{0, 1\}$, $\mathsf{HelpRec}(\mathbf{x}; b) = \mathsf{HelpRec}(\mathbf{x} + \mathbf{w}; b')$ holds.

Let $\boldsymbol{\delta} = (\delta_0, \delta_1, \delta_2, \delta_3)$ be a vector such that $\mathbf{x} + \mathbf{w} = \mathbf{x} + q\mathbf{g} + \boldsymbol{\delta}$. Then $|\delta_i| \leq q^{1/4}$. Since $\mathbf{g} \in D_4$, we have $\mathsf{HelpRec}(\mathbf{x}; b) = \mathsf{HelpRec}(\mathbf{x} + q\mathbf{g}; b')$ [3]. For simplicity, let $\mathbf{z} = \frac{2^r}{q}(\mathbf{x} + q\mathbf{g} + b'\mathbf{g}) \in \frac{2^r}{2q}\mathbb{Z}_{2q}^4$, vector $\boldsymbol{\beta} = (\beta_0, \beta_1, \beta_2, \beta_3)$ denote $\frac{2^r}{q}\boldsymbol{\delta}$. Recall that $\mathsf{HelpRec}(\mathbf{x}; b) = \mathsf{CVP}_{\tilde{D}_4}\left(\frac{2^r}{q}(\mathbf{x} + b\mathbf{g})\right) \mod 2^r$. Thus, the proposition $(\mathsf{HelpRec}(\mathbf{x} + q\mathbf{g}; b') =) \mathsf{HelpRec}(\mathbf{x}; b) = \mathsf{HelpRec}(\mathbf{x} + \mathbf{w}; b')$ is equivalent to $\mathsf{CVP}_{\tilde{D}_4}(\mathbf{z}) = \mathsf{CVP}_{\tilde{D}_4}(\mathbf{z} + \boldsymbol{\beta})$, which remains to be proved valid with probability at least $1 - p$.

For the following analysis, refer to Figure 4.3, which describes the $\mathsf{CVP}_{\tilde{D}_4}$ algorithm. Let $\boldsymbol{v}_0, \boldsymbol{v}_1, k$ be the values computed in steps 1, 2, 3 of $\mathsf{CVP}_{\tilde{D}_4}(\mathbf{z})$ algorithm, shown in Figure 4.3 and let $\boldsymbol{v}_0', \boldsymbol{v}_1', k'$ be the values computed in step 1, 2, 3 of $\mathsf{CVP}_{\tilde{D}_4}(\mathbf{z} + \boldsymbol{\beta})$ algorithm.

By definition of $\mathsf{CVP}_{\tilde{D}_4}$, it is clear to see that if none of the following three conditions is satisfied, then $\mathsf{CVP}_{\tilde{D}_4}(\mathbf{z}) = \mathsf{CVP}_{\tilde{D}_4}(\mathbf{z} + \boldsymbol{\beta})$ is granted.

(a) $\boldsymbol{v}_0' \neq \boldsymbol{v}_0$.
(b) $\boldsymbol{v}_1' \neq \boldsymbol{v}_1$

[9] Note that this is the only part of the analysis that is not generic in terms of parameter settings. For more discussion, See Section 4.4.

(c) $k' \neq k$

Before analyzing probability in each condition above, we first present the following lemma, which will allow us to switch from analyzing the probabilities over choice of $(\mathbf{x}, b)$ to analyzing probabilities over choice of $\mathbf{z}$.

**Lemma 4.11.** *Given* $\mathbf{g}, \mathbf{x}, \mathbf{z} = \frac{2^r}{q}(\mathbf{x} + q\mathbf{g} + b'\mathbf{g})$ *as defined above, for any set* $\mathcal{D}' \subseteq \frac{2^r}{2q}\mathbb{Z}_{2q}^4$*, the probability that* $\mathbf{x}$ *in set* $\mathcal{D} = \{\mathbf{x} \mid \frac{2^r}{q}(\mathbf{x} + q\mathbf{g} + b'\mathbf{g}) \in \mathcal{D}'\}$ *over choice of* $\mathbf{x} \leftarrow \mathbb{Z}_q^4$ *and choice of* $b' \leftarrow \{0, 1\}$ *equals to the probability that* $\mathbf{z}$ *in set* $\mathcal{D}'$ *over choice of* $\mathbf{z} \leftarrow \frac{2^r}{2q}\mathbb{Z}_{2q}^4$*, denoted by* $\mathrm{Prob}_{\mathbf{x},b'}[\mathbf{x} \in \mathcal{D}] = \mathrm{Prob}_{\mathbf{z}}[\mathbf{z} \in \mathcal{D}']$.

*Proof.* We compute $\mathrm{Prob}_{\mathbf{x},b'}[\mathbf{x} \in \mathcal{D}]$ given the condition $b' = 0$ and the condition $b' = 1$. As $b'$ is equivalent to the "doubling" trick (See [44] for example), the corresponding $\mathbf{x} + q\mathbf{g} + b'\mathbf{g}$ when $b' = 0$ is distributed as odd numbers over $\mathbb{Z}_{2q}^4$, written as $2\mathbb{Z}_{2q}^4 + \mathbb{Z}_{2q}^4$. When $b' = 1$, $\mathbf{x} + q\mathbf{g} + b'\mathbf{g}$ is distributed as even numbers over is over $\mathbb{Z}_{2q}^4$, written as $2\mathbb{Z}_{2q}^4$. Thus we have

$$\mathrm{Prob}_{\mathbf{x},b'}[\mathbf{x} \in \mathcal{D}] = \frac{1}{2}\mathrm{Prob}_{\mathbf{x},0}\left[\frac{2^r}{q}(\mathbf{x} + q\mathbf{g}) \in \mathcal{D}'\right] + \frac{1}{2}\mathrm{Prob}_{\mathbf{x},1}\left[\frac{2^r}{q}(\mathbf{x} + q\mathbf{g} + \mathbf{g}) \in \mathcal{D}'\right] \tag{7}$$

$$= \frac{1}{2}\frac{\left|\frac{2^r}{2q}(2\mathbb{Z}_{2q}^4 + \mathbb{Z}_{2q}^4) \cap \mathcal{D}'\right|}{\left|\frac{2^r}{2q}(2\mathbb{Z}_{2q}^4 + \mathbb{Z}_{2q}^4)\right|} + \frac{1}{2}\frac{\left|\frac{2^r}{2q}(2\mathbb{Z}_{2q}^4) \cap \mathcal{D}'\right|}{\left|\frac{2^r}{2q}(2\mathbb{Z}_{2q}^4)\right|} \tag{8}$$

$$= \frac{\left|\left(\frac{2^r}{2q}(2\mathbb{Z}_{2q}^4 + \mathbb{Z}_{2q}^4) \cup \frac{2^r}{2q}(2\mathbb{Z}_{2q}^4)\right) \cap \mathcal{D}'\right|}{\frac{2^r}{2q}(\mathbb{Z}_{2q}^4)} \tag{9}$$

$$= \frac{\left|\frac{2^r}{2q}(\mathbb{Z}_{2q}^4) \cap \mathcal{D}'\right|}{\frac{2^r}{2q}(\mathbb{Z}_{2q}^4)} = \mathrm{Prob}_{\mathbf{z}}[\mathbf{z} \in \mathcal{D}'] \tag{10}$$

as desired. □

We omit to mention distribution of $b'$ for simplicity.

We next analyze probability of the three conditions (a), (b), (c) in Lemmas 4.12, 4.13 and 4.14.

**Lemma 4.12** (Bounding the probability of (a))**.** *Given* $\boldsymbol{v}_0, \boldsymbol{v}_0', \boldsymbol{v}_1, \boldsymbol{v}_1', k, k', \mathbf{z}, \boldsymbol{\beta}$ *as defined above, probability that* $\boldsymbol{v}_0' \neq \boldsymbol{v}_0$ *(denoted by* $\mathrm{Prob}_{\mathbf{x}}[\boldsymbol{v}_0' \neq \boldsymbol{v}_0]$ *) is at most* $1 - \left(\frac{\frac{q}{2^r} - 2q^{1/4} - 1}{\frac{q}{2^r}}\right)^4$ *over choice of* $\mathbf{x} \leftarrow \mathbb{Z}_q^4$.

*Proof.* Recall that $|\delta_i| \leq q^{1/4}$. Then we have $|\beta_i| \leq \frac{2^r}{q^{3/4}}$. We assume that $\frac{2^r}{q^{3/4}} \leq 1/2$, which would be the case for typical parameter settings (for example $r = 2, q = 12289$). When the event that $\boldsymbol{v}_0' \neq \boldsymbol{v}_0$ happens, it indicates existing an $i$ such that, $\lfloor z_i \rceil \neq \lfloor z_i + \beta_i \rceil$. We start by computing the probability over choice of $\mathbf{x} \leftarrow \mathbb{Z}_q^4$ that given $i$, event $\lfloor z_i \rceil = \lfloor z_i + \beta_i \rceil$ occurs, denoted by $\mathrm{Prob}_{\mathbf{x}}[\lfloor z_i \rceil = \lfloor z_i + \beta_i \rceil]$. We divide the analysis into two cases.

(1) Suppose that $z_i - \lfloor z_i \rceil \geq 0$, then $\lfloor z_i - \frac{2^r}{q^{3/4}} \rceil = \lfloor z_i \rceil$. In order to achieve $\lfloor z_i + \beta_i \rceil = \lfloor z_i \rceil$, we need $\lfloor z_i + \frac{2^r}{q^{3/4}} \rceil = \lfloor z_i \rceil$. Without loss of generality, we assume $0 \leq z_i < 1/2 \mod 2^r$, where $\lfloor z_i \rceil = 0$. Thus it can be easily verified that if $0 \leq z_i < 1/2 - \frac{2^r}{q^{3/4}}$, we can ensure $\lfloor z_i + \frac{2^r}{q^{3/4}} \rceil = 0$.

(2) Suppose that $z_i - \lfloor z_i \rceil < 0$, then $\lfloor z_i + \frac{2^r}{q^{3/4}} \rceil = \lfloor z_i \rceil$. Similarly, in order to achieve $\lfloor z_i + \beta_i \rceil = \lfloor z_i \rceil$, we need $\lfloor z_i - \frac{2^r}{q^{3/4}} \rceil = \lfloor z_i \rceil$. Without loss of generality, we assume $-1/2 \leq z_i < 0 \mod 2^r$, where $\lfloor z_i \rceil = 0$. Thus it can easily verified that if $-1/2 + \frac{2^r}{q^{3/4}} \leq z_i < 0$, we can ensure $\lfloor z_i + \frac{2^r}{q^{3/4}} \rceil = 0$.

Combining both cases, by Lemma 4.11, we then derive that

$$\mathrm{Prob}_{\mathbf{x}}[\lfloor z_i \rceil = \lfloor z_i + \beta_i \rceil] \geq \frac{\left| \left[-1/2 + \frac{2^r}{q^{3/4}}, 1/2 - \frac{2^r}{q^{3/4}}\right) \cap \frac{2^r}{2q}\mathbb{Z}_{2q} \right|}{\left| [-1/2, 1/2) \cap \frac{2^r}{2q}\mathbb{Z}_{2q} \right|} \tag{11}$$

$$\geq \frac{\left| \left[\frac{2q}{2^r}(-1/2 + \frac{2^r}{q^{3/4}}), \frac{2q}{2^r}(1/2 - \frac{2^r}{q^{3/4}})\right) \cap \mathbb{Z}_{2q} \right|}{\left| \left[-\frac{q}{2^r}, \frac{q}{2^r}\right) \cap \mathbb{Z}_{2q} \right|} \tag{12}$$

$$= \frac{2\lfloor \frac{q}{2^r} - 2q^{1/4} \rfloor + 1}{2\lfloor \frac{q}{2^r} \rfloor + 1} \tag{13}$$

$$\geq \frac{\frac{q}{2^r} - 2q^{1/4} - 1}{\frac{q}{2^r}} \tag{14}$$

Since $\mathrm{Prob}_{\mathbf{x}}[\exists i, \lfloor z_i \rceil \neq \lfloor z_i + \beta_i \rceil] = 1 - \mathrm{Prob}_{\mathbf{x}}[\lfloor z_i \rceil = \lfloor z_i + \beta_i \rceil, \forall i]$. Therefore, we have

$$\mathrm{Prob}_{\mathbf{x}}[\boldsymbol{v}_0' \neq \boldsymbol{v}_0] \leq 1 - \left(\frac{\frac{q}{2^r} - 2q^{1/4} - 1}{\frac{q}{2^r}}\right)^4$$

as desired. □

**Lemma 4.13** (Bounding the probability of (b))**.** *Given $\boldsymbol{v}_0, \boldsymbol{v}_0', \boldsymbol{v}_1, \boldsymbol{v}_1', k, k', \mathbf{z}, \boldsymbol{\beta}$ as defined above, probability that $\boldsymbol{v}_1' \neq \boldsymbol{v}_1$ (denoted by $\mathrm{Prob}_{\mathbf{x}}[\boldsymbol{v}_1' \neq \boldsymbol{v}_1]$) is at most $1 - \left(\frac{\frac{q}{2^r} - 2q^{1/4} - 1}{\frac{q}{2^r}}\right)^4$ over choice of $\mathbf{x} \leftarrow \mathbb{Z}_q^4$.*

The proof proceeds exactly the same as proof of Lemma 4.12 by substituting $\mathbf{z}$ with $\mathbf{z} + \mathbf{g}$.

**Lemma 4.14** (Bounding the probability of (c))**.** *Given $\boldsymbol{v}_0, \boldsymbol{v}_0', \boldsymbol{v}_1, \boldsymbol{v}_1', k, k', \mathbf{z}, \boldsymbol{\beta}$ as defined above, probability that $k' \neq k$ (denoted by $\mathrm{Prob}_{\mathbf{x}}[k' \neq k]$) is at most $\left(\frac{1 + \frac{1}{2q^{1/4}}}{1 - \frac{2^{r+1}}{q}}\right)^4 \cdot \left(\frac{2^{r+10}}{3q^{3/4}} - \frac{2^{3r+10}}{3q^{9/4}} + \frac{2^{4r+10}}{q^3}\right)$ over choice of $\mathbf{x} \leftarrow \mathbb{Z}_q^4$.*

*Proof.* We divide our proof into two cases: (1) Suppose $k = 0$ and $k' = 1$, which indicates $\|\mathbf{z} - \boldsymbol{v}_0\|_1 < 1$ and $\|\mathbf{z} + \boldsymbol{\beta} - \boldsymbol{v}_0'\|_1 \geq 1$ . We denote by $\mathrm{Prob}_{\mathbf{x}}[k = 0, k' = 1]$ probability that $k = 0$ and $k' = 1$ over choice of $\mathbf{x}$. (2) Suppose $k = 1$

and $k' = 0$, which indicates $\|\mathbf{z} - \boldsymbol{v}_0\|_1 \geq 1$ and $\|\mathbf{z} + \boldsymbol{\beta} - \boldsymbol{v}'_0\|_1 < 1$ . We denote by $\text{Prob}_{\mathbf{x}}[k = 1, k' = 0]$ probability that $k = 1$ and $k' = 0$ over choice of $\mathbf{x}$.

Without loss of generality, we assume that $-1/2 \leq z_i < 1/2 \mod 2^r$ for $i = 0, 1, 2, 3$. Then we have $\boldsymbol{v}_0 = \mathbf{0}$.

*Case 1*: By Lemma 4.11, $\text{Prob}_{\mathbf{x}}[k = 0, k' = 1]$ is equivalent to the probability that $\mathbf{z}$ satisfies

$$|z_0| + |z_1| + |z_2| + |z_3| < 1, \text{and}$$
$$|z_0 + \beta_0| + |z_1 + \beta_1| + |z_2 + \beta_2| + |z_3 + \beta_3| > 1,$$

over choice of $\mathbf{z} \leftarrow \frac{2^r}{2q}\mathbb{Z}^4_{2q} \cap [-1/2, 1/2)^4 \mod 2^r$. As $|z_i + \beta_i| \leq |z_i| + |\beta_i|$ by Triangle Inequality, we can upper-bound $\text{Prob}_{\mathbf{x}}[k = 0, k' = 1]$ by the probability that $\mathbf{z}$ satisfies

$$|z_0| + |z_1| + |z_2| + |z_3| < 1, \text{and}$$
$$|z_0| + |z_1| + |z_2| + |z_3| + |\beta_0| + |\beta_1| + |\beta_2| + |\beta_3| > 1,$$

over choice of $\mathbf{z} \leftarrow \frac{2^r}{2q}\mathbb{Z}^4_{2q} \cap [-1/2, 1/2)^4 \mod 2^r$. Since $|\beta_0| + |\beta_1| + |\beta_2| + |\beta_3| \leq 4 \cdot \frac{2^r}{q^{3/4}}$, we can further upper-bound $\text{Prob}_{\mathbf{x}}[k = 0, k' = 1]$ by the probability that $\mathbf{z}$ satisfies

$$1 - 4 \cdot \frac{2^r}{q^{3/4}} < |z_0| + |z_1| + |z_2| + |z_3| < 1,$$

over choice of $\mathbf{z} \leftarrow \frac{2^r}{2q}\mathbb{Z}^4_{2q} \cap [-1/2, 1/2)^4 \mod 2^r$.

Let $\Delta = 4 \cdot \frac{2^r}{q^{3/4}}$. We then can obtain the upperbound of $\text{Prob}_{\mathbf{x}}[k = 0, k' = 1]$ by computing the cardinality of set where each element is in $\frac{2^r}{2q}\mathbb{Z}^4_{2q}$ and satisfies the following two conditions:

$$1 - \Delta < |z_0| + |z_1| + |z_2| + |z_3| < 1 \tag{15}$$
$$-1/2 \ \leq \ z_i < \ 1/2 \text{ , for } i = 0, 1, 2, 3 \tag{16}$$

divided by the cardinality of set where each element is in $\frac{2^r}{2q}\mathbb{Z}^4_{2q}$ and only satisfies the equation (16).

Similarly for *Case 2*, by Lemma 4.11, $\text{Prob}_{\mathbf{x}}[k = 1, k' = 0]$ is equivalent to the probability that $\mathbf{z}$ satisfies

$$|z_0| + |z_1| + |z_2| + |z_3| \geq 1, \text{and}$$
$$|z_0 + \beta_0| + |z_1 + \beta_1| + |z_2 + \beta_2| + |z_3 + \beta_3| < 1,$$

over choice of $\mathbf{z} \leftarrow \frac{2^r}{2q}\mathbb{Z}^4_{2q} \cap [-1/2, 1/2)^4 \mod 2^r$. Since $|z_i + \beta_i| \geq |z_i| - |\beta_i|$ and $|\beta_0| + |\beta_1| + |\beta_2| + |\beta_3| \leq 4 \cdot \frac{2^r}{q^{3/4}}$, we can further upper -bounded $\text{Prob}_{\mathbf{x}}[k = 1, k' = 0]$ by the probability that $\mathbf{z}$ satisfies

$$1 \leq |z_0| + |z_1| + |z_2| + |z_3| < 1 + 4 \cdot \frac{2^r}{q^{3/4}},$$

over choice of $\mathbf{z} \leftarrow \frac{2^r}{q}\mathbb{Z}_q^4 \cap [-1/2, 1/2)^4 \mod 2^r$.

We can then obtain the upperbound of $\text{Prob}_{\mathbf{x}}[k = 1, k' = 0]$ by computing the cardinality of set where each element is in $\frac{2^r}{2q}\mathbb{Z}_{2q}^4$ and satisfies the following two conditions:

$$1 \leq |z_0| + |z_1| + |z_2| + |z_3| < 1 + \Delta \tag{17}$$
$$-1/2 \ \leq \ z_i < \ 1/2 \ , \text{for } i = 0, 1, 2, 3 \tag{18}$$

by the cardinality of set that each element is in $\frac{2^r}{2q}\mathbb{Z}_{2q}^4$ and only satisfies the Equation 18.

Thus, by combining both cases, we have $\text{Prob}_{\mathbf{x}}[k' \neq k] = \text{Prob}_{\mathbf{x}}[k = 0, k' = 1] + \text{Prob}_{\mathbf{x}}[k = 1, k' = 0]$ upperbounded by the cardinality of set where each element is in $\frac{2^r}{2q}\mathbb{Z}_{2q}^4$ and satisfies the following two conditions:

$$1 - \Delta < |z_0| + |z_1| + |z_2| + |z_3| < 1 + \Delta \tag{19}$$
$$-1/2 \ \leq \ z_i < \ 1/2 \ , \text{for } i = 0, 1, 2, 3 \tag{20}$$

by the cardinality of set where elements are in $\frac{2^r}{2q}\mathbb{Z}_{2q}^4$ and satisfies the the Equation 20.

Note that, disregarding the distribution of $\mathbf{z}$, (20) defines a unit hypercube $[-1/2, 1/2)^4$ centered at origin and (19) defines a hyper-object clipped by two hyperplanes in each octant. We denote by $\text{Vol}_{cube}$ the hypercube volume. Let $\text{Vol}_{clip}$ be the hypervolume where each points satisfies both (19) and (20), which is equivalent to say, $\text{Vol}_{clip}$ is hypervolume of hypercube defined in (20) clipped by two hyperplanes in each octant, as defined in (19).

If $\mathbf{x}$ is sampled from $\mathbb{R}^4$, it is easy to see that probability $\text{Prob}_{\mathbf{x}}[k' \neq k]$ is upperbounded by the ratio of $\text{Vol}_{clip}$ to $\text{Vol}_{cube}$.

For the rest of the proof, we first compute the ratio of $\text{Vol}_{clip}$ to $\text{Vol}_{cube}$ and then approximate the upperbound of $\text{Prob}_{\mathbf{x}}[k' \neq k]$ by discretizing hypervolumes into lattice points, as $\mathbf{z}$ is instead sampled from $\frac{2^r}{2q}\mathbb{Z}_{2q}^4$, which is a lattice.

Towards computing the volumes, we need to amplify each dimension by 2 in (15) and (16) for adapting Theorem 2.2 where unit hypercube is defined as $[0, 1]^n$. $\text{Vol}_{clip}$ and $\text{Vol}_{cube}$ is $i^{\text{th}}$ octant. Let $\text{Vol}_{clip}^i$ denote $\text{Vol}_{clip}$ in the $i^{\text{th}}$ octant, and $\text{Vol}_{cube}^i$ denote $\text{Vol}_{cube}$ in $i^{\text{th}}$ octant. Thus, in the $i^{\text{th}}$ octant, we have

$$2 - 2\Delta < t_0 + t_1 + t_2 + t_3 < 2 + 2\Delta \tag{21}$$
$$0 \leq t_i < 1, \text{ for } i = 0, 1, 2, 3, \tag{22}$$

where $t_i = 2z_i$.

Define two hyperspace as follows:

$$H_1^+ := \{\mathbf{t} \mid g_1(\mathbf{t}) := -t_0 - t_1 - t_2 - t_3 + 2(1 - \Delta) \geq 0\}$$

$$H_2^+ := \{\mathbf{t} \mid g_2(\mathbf{t}) := -t_0 - t_1 - t_2 - t_3 + 2(1+\Delta) \geq 0\}$$

Then it is easy to see that

$$\mathrm{Vol}^1_{clip} \leq \frac{\mathrm{Vol}([0,1]^4 \cap H_2^+) - \mathrm{Vol}([0,1]^4 \cap H_1^+)}{2^4}.$$

where $2^4$ in denominator is a scalar to neutralize amplification

By Theorem 2.2 and substituting $\Delta$ with $4q^{1/4} \cdot \frac{2^r}{q}$, we obtain

$$\begin{aligned}
\mathrm{Vol}^1_{clip} &= \frac{1}{2^4} \cdot \frac{1}{24}\left((2+2\Delta)^4 - 4(1+2\Delta)^4 + 6(2\Delta)^4 - (2-2\Delta)^4 + 4(1-2\Delta)^4\right) \\
&= \frac{1}{2^4} \cdot \frac{1}{24}(64\Delta - 128\Delta^3 + 96\Delta^4) \\
&= \frac{1}{2^4}\left(\frac{2^{4r+10}}{q^3} - \frac{2^{3r+10}}{3q^{9/4}} + \frac{2^{r+5}}{3q^{3/4}}\right)
\end{aligned}$$

We claim that $\mathrm{Vol}^1_{clip} = \mathrm{Vol}^i_{clip}$ for $i = 2, 3, ..., 16$. It can be easily checked by showing a bijective map $f_i : \mathbf{z} \leftrightarrow \mathbf{z}'$ which maps elements from first octant to the $i^{\text{th}}$ octant, such that if $\mathbf{z}$ satisfies the conditions (19) and (20), then $\mathbf{z}'$ satisfies the conditions (19) and (20), and if $\mathbf{z}$ satisfies the condition (20) but not satisfies (19), then $\mathbf{z}'$ satisfies the condition (20) but not satisfies (19). One trivial example of such map is to let $\mathbf{z}$ be the absolute value of $\mathbf{z}'$.

Additionally, it is obvious to see that $\mathrm{Vol}^i_{cube} = 1/2^4, \forall i$. Thus, we have

$$\frac{\mathrm{Vol}_{clip}}{\mathrm{Vol}_{cube}} = \frac{\mathrm{Vol}^1_{clip}}{\mathrm{Vol}^1_{cube}} = \frac{2^{4r+10}}{q^3} - \frac{2^{3r+10}}{3q^{9/4}} + \frac{2^{r+5}}{3q^{3/4}}.$$

It remains to approximate $\frac{\mathrm{Vol}^1_{clip} \cap \mathcal{L}_\mathbf{z}}{\mathrm{Vol}^1_{cube} \cap \mathcal{L}_\mathbf{z}}$, where $\mathcal{L}_\mathbf{z} = \frac{2^r}{2q}\mathbb{Z}^4_{2q}$.

Since both of the hypercube and the hyperclip in first octant are convex as they are intersections of hyperspaces, by Theorem 2.1, we can derive that

$$\frac{\mathrm{Vol}^1_{clip} \cap \mathcal{L}_\mathbf{z}}{\mathrm{Vol}^1_{cube} \cap \mathcal{L}_\mathbf{z}} \leq \frac{(1+\varepsilon)^4 \frac{\mathrm{Vol}^1_{clip}}{\det(\mathcal{L}_\mathbf{z})}}{(1-\varepsilon')^4 \frac{\mathrm{Vol}^1_{cube}}{\det(\mathcal{L}_\mathbf{z})}} = \left(\frac{1+\varepsilon}{1-\varepsilon'}\right)^4 \cdot \frac{\mathrm{Vol}^1_{clip}}{\mathrm{Vol}^1_{cube}},$$

where $\mathcal{P}(B) \cup -\mathcal{P}(B) \subseteq \varepsilon \cdot \mathrm{Vol}^1_{clip}$, $\mathcal{P}(B) \cup -\mathcal{P}(B) \subseteq \varepsilon' \cdot \mathrm{Vol}^1_{cube}$ and $B$ is a basis of $\mathcal{L}_\mathbf{z}$.

To get a small $\varepsilon$, we begin by carving a hypercube $[\frac{1}{4} - \frac{1}{4}\Delta, \frac{1}{4} + \frac{1}{4}\Delta]^4$, which is contained in $\mathrm{Vol}^1_{clip}$. Let $B = \{(\frac{2^r}{2q}, 0, 0, 0), (0, \frac{2^r}{2q}, 0, 0), (0, 0, \frac{2^r}{2q}, 0), (0, 0, 0, \frac{2^r}{2q})\}$. Then $\mathcal{P}(B)$ forms a hypercube with side length $\frac{2^r}{2q}$. Thus, by letting $\varepsilon = \frac{1}{2q^{1/4}}$ as $\frac{2^r}{2q} \cdot 2 \leq \varepsilon \cdot \frac{1}{2}\Delta$, we can guarantee that $\mathcal{P}(B) \cup -\mathcal{P}(B) \subseteq \varepsilon \cdot \mathrm{Vol}^1_{clip}$. Similarly, since $\mathrm{Vol}^1_{cube}$ is a hypercube, it is easy to see that by letting $\varepsilon' = \frac{2^{r+1}}{q}$, $\mathcal{P}(B) \cup -\mathcal{P}(B) \subseteq \varepsilon' \cdot \mathrm{Vol}^1_{cube}$.

Combining the above, we obtain

$$\frac{\mathrm{Vol}^1_{clip} \cap \mathcal{L}_{\mathbf{z}}}{\mathrm{Vol}^1_{cube} \cap \mathcal{L}_{\mathbf{z}}} \leq \left(\frac{1+\frac{1}{2q^{1/4}}}{1-\frac{2^{r+1}}{q}}\right)^4 \cdot \left(\frac{2^{4r+10}}{q^3} - \frac{2^{3r+10}}{3q^{9/4}} + \frac{2^{r+5}}{3q^{3/4}}\right),$$

as desired. □

Combining Lemmas 4.12, 4.13 and 4.14, we conclude that, for all $\mathbf{w} \in \ker(\boldsymbol{c}_{\omega,\alpha}) \cap \mathbf{W}$ and $f_{\omega,j}(\mathbf{x}) = \gamma$, the probability that $\mathsf{HelpRec}(\mathbf{x}) = \mathsf{HelpRec}(\mathbf{x}+\mathbf{w})$ holds over choice of $\mathbf{x} \in \mathbb{Z}_q^4$ is at least

$$1 - 2\left(1 - \left(\frac{\frac{q}{2^r} - 2q^{1/4} - 1}{\frac{q}{2^r}}\right)^4\right) - \left(\frac{1+\frac{1}{2q^{1/4}}}{1-\frac{2^{r+1}}{q}}\right)^4 \cdot \left(\frac{2^{4r+10}}{q^3} - \frac{2^{3r+10}}{3q^{9/4}} + \frac{2^{r+5}}{3q^{3/4}}\right).$$

□

Using known relationships between average min-entropy and min-entropy, we have that:

**Corollary 4.15.** *With all but $2^{-k}$ probability, the distribution over $v$, given the transcript of the modified protocol as well as leakage $1 \mod 16$ positions of $\hat{\boldsymbol{s}}, \hat{\boldsymbol{s}}', \hat{\boldsymbol{e}}, \hat{\boldsymbol{e}}', \hat{\boldsymbol{e}}''$, is indistinguishable from a distribution that has min-entropy $n/8 + n/8 \cdot (-\log_2(1/2+p)) - k$.*

### 4.3 Instantiating the Parameters

We instantiate the parameters as chosen in NewHope protocol: $q = 12289, n = 1024, \omega = 7, r = 2$, then we get

$$p := 2 - 2\left(\frac{\frac{q}{2^r} - 2q^{1/4} - 1}{\frac{q}{2^r}}\right)^4 + \left(\frac{1+\frac{1}{2q^{1/4}}}{1-\frac{2^{r+1}}{q}}\right)^4 \cdot \left(\frac{2^{4r+10}}{q^3} - \frac{2^{3r+10}}{3q^{9/4}} + \frac{2^{r+5}}{3q^{3/4}}\right) \tag{23}$$

$$\approx 0.10092952876519123 \tag{24}$$

Therefore, under this concrete parameter setting, the distribution with leakage and transcript as defined above is indistinguishable from a distribution that has average min-entropy $128 + 128 \cdot (-\log_2(1/2 + 0.10092952876519123/2)) - 1.10910222427 \approx 237$. Moreover, with all but $2^{-80}$ probability, the distribution with leakage and transcript as defined above is indistinguishable from a distribution that has min-entropy 157.

### 4.4 On the Non-Generic Part of the Analysis

Recall that in the analysis, we experimentally confirm that there exists a vector $\mathbf{w} \in \ker(\boldsymbol{c}_{\omega,\alpha}) \cap \mathbf{W}$.

We can support this heuristically by noting that $\mathbf{W}$ has size $(2q^{1/4})^4 = 16q$. On the other hand, the probability that a random vector in $\mathbb{Z}_q^4$ is in $\ker(\boldsymbol{c}_{\omega,\alpha})$ is

$1/q$. So heuristically, we expect that $1/q$-fraction (approx. 16) of the vectors in $\mathbf{W}$ will also be in $\ker(\boldsymbol{c}_{\omega,\alpha})$.

A similar analysis can be done for other leakage patterns $(n', \mathcal{S})$. Recall that our experimental attacks support the conclusion that Leaky-SRLWE is easy when the fraction of structured leakage is at least $1/4$. We may also consider parameter settings $(n', \mathcal{S})$ such that $|\mathcal{S}| = 2$ and $\frac{|\mathcal{S}|}{n'} = 1/8$. In this case, instead of a single linear constraint $\boldsymbol{c}_{\omega,\alpha}$ on a single $\mathbf{x}_i$, we have two linear constraints on $\mathbf{x}_i, \mathbf{x}_{i+n/16}$. This means we will have a linear system of 8 variables and two constraints, denoted by $\mathsf{M}_{\omega,\mathcal{S}}$. Thus, $\mathbf{W}$ will be equal to $[\frac{q}{2} \pm q^{1/4}]^8$. So the size of $\mathbf{W}$ will be $(2q^{1/4})^8 = 256q^2$ and the probability that a random vector in $Z_q^4$ is in $\ker(\mathsf{M}_{\omega,\mathcal{S}})$ is $1/q^2$. So heuristically, we expect that $1/q^2$-fraction (approx. 256) of the vectors in $\mathbf{W}$ will also be in $\ker(\mathsf{M}_{\omega,\mathcal{S}})$. Given this, the rest of the analysis proceeds nearly identically.

## References


1. Akavia, A., Goldwasser, S., Vaikuntanathan, V.: Simultaneous hardcore bits and cryptography against memory attacks. In Reingold, O., ed.: TCC 2009. Volume 5444 of LNCS., Springer, Heidelberg (March 2009) 474–495
2. Albrecht, M.R., Deo, A., Paterson, K.G.: Cold Boot Attacks on Ring and Module LWE Keys Under the NTT. IACR Transactions on Cryptographic Hardware and Embedded Systems (2018) 173–213
3. Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P.: Post-quantum key exchange - a new hope. Cryptology ePrint Archive, Report 2015/1092 (2015) http://eprint.iacr.org/2015/1092.
4. Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P.: Post-quantum key exchange - A new hope. In Holz, T., Savage, S., eds.: USENIX Security 2016, USENIX Association (August 2016) 327–343
5. Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P.: Post-quantum key exchange - a new hope. Cryptology ePrint Archive, Report 2015/1092 (2015) https://eprint.iacr.org/2015/1092.
6. Barrow, D., Smith, P.: Spline notation applied to a volume problem. The American Mathematical Monthly **86**(1) (1979) 50–51
7. Bernstein, D.J., Chuengsatiansup, C., Lange, T., Vredendaal, C.V.: NTRU Prime . https://ntruprime.cr.yp.to/index.html
8. Blömer, J., May, A.: New partial key exposure attacks on RSA. In Boneh, D., ed.: CRYPTO 2003. Volume 2729 of LNCS., Springer, Heidelberg (August 2003) 27–43
9. Bolboceanu, M., Brakerski, Z., Perlman, R., Sharma, D.: Order-LWE and the Hardness of Ring-LWE with Entropic Secrets. In: Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8-12, 2019, Proceedings, Part II. (2019) 91–120
10. Boneh, D., Durfee, G., Frankel, Y.: An attack on RSA given a small fraction of the private key bits. In Ohta, K., Pei, D., eds.: ASIACRYPT'98. Volume 1514 of LNCS., Springer, Heidelberg (October 1998) 25–34
11. Bos, J.W., Costello, C., Ducas, L., Mironov, I., Naehrig, M., Nikolaenko, V., Raghunathan, A., Stebila, D.: Frodo: Take off the ring! Practical, quantum-secure key exchange from LWE. In Weippl, E.R., Katzenbeisser, S., Kruegel, C., Myers, A.C., Halevi, S., eds.: ACM CCS 2016, ACM Press (October 2016) 1006–1018

12. Bos, J.W., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Seiler, G., Stehlé, D.: CRYSTALS - kyber: A cca-secure module-lattice-based KEM. In: 2018 IEEE European Symposium on Security and Privacy, EuroS&P 2018, London, United Kingdom, April 24-26, 2018. (2018) 353–367
13. Boyle, E., Segev, G., Wichs, D.: Fully leakage-resilient signatures. Journal of Cryptology **26**(3) (July 2013) 513–558
14. Braithwaite, M.: Experimenting with Post-Quantum Cryptography. https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html Accessed: 2018-10-09.
15. Brakerski, Z., Döttling, N.: Hardness of LWE on General Entropic Distributions. Cryptology ePrint Archive, Report 2020/119 (2020) https://eprint.iacr.org/2020/119.
16. Brakerski, Z., Kalai, Y.T., Katz, J., Vaikuntanathan, V.: Overcoming the hole in the bucket: Public-key cryptography resilient to continual memory leakage. In: 51st FOCS, IEEE Computer Society Press (October 2010) 501–510
17. Chen, C., Danba, O., Hoffstein, J., Hulsing, A., Rijneveld, J., Schanck, J.M., Schwabe, P., Whyte, W., Zhang, Z.: NTRU. https://ntru.org/resources.shtml
18. Coppersmith, D.: Finding a small root of a bivariate integer equation; factoring with high bits known. In Maurer, U.M., ed.: EUROCRYPT'96. Volume 1070 of LNCS., Springer, Heidelberg (May 1996) 178–189
19. Coppersmith, D.: Finding a small root of a univariate modular equation. In Maurer, U.M., ed.: EUROCRYPT'96. Volume 1070 of LNCS., Springer, Heidelberg (May 1996) 155–165
20. Dachman-Soled, D., Gong, H., Kulkarni, M., Shahverdi, A.: On the leakage resilience of ideal-lattice based public key encryption. Cryptology ePrint Archive, Report 2017/1127 (2017) https://eprint.iacr.org/2017/1127.
21. Dachman-Soled, D., Gong, H., Kulkarni, M., Shahverdi, A.: (In)Security of Ring-LWE Under Partial Key Exposure. Journal of Mathematical Cryptology, to appear. Preliminary version in MathCrypt '19 **2018** (2018) 1068
22. Dadush, D., Regev, O.: Lecture Note of Fundamental Domains, Lattice Density, and Minkowski Theorems (2018)
23. D'Anvers, J., Karmakar, A., Roy, S.S., Vercauteren, F.: SABER. https://www.esat.kuleuven.be/cosic/pqcrypto/saber/
24. Ding, J.: A Simple Provably Secure Key Exchange Scheme Based on the Learning with Errors Problem. IACR Cryptology ePrint Archive **2012** (2012) 688
25. Dodis, Y., Goldwasser, S., Kalai, Y.T., Peikert, C., Vaikuntanathan, V.: Public-key encryption schemes with auxiliary inputs. In Micciancio, D., ed.: TCC 2010. Volume 5978 of LNCS., Springer, Heidelberg (February 2010) 361–381
26. Dodis, Y., Haralambiev, K., López-Alt, A., Wichs, D.: Cryptography against continuous memory attacks. In: 51st FOCS, IEEE Computer Society Press (October 2010) 511–520
27. Dodis, Y., Kalai, Y.T., Lovett, S.: On cryptography with auxiliary input. In Mitzenmacher, M., ed.: 41st ACM STOC, ACM Press (May / June 2009) 621–630
28. Dodis, Y., Ostrovsky, R., Reyzin, L., Smith, A.D.: Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. SIAM J. Comput. **38**(1) (2008) 97–139
29. Dziembowski, S., Pietrzak, K.: Leakage-resilient cryptography. In: 49th FOCS, IEEE Computer Society Press (October 2008) 293–302
30. Ernst, M., Jochemsz, E., May, A., de Weger, B.: Partial key exposure attacks on RSA up to full size exponents. In Cramer, R., ed.: EUROCRYPT 2005. Volume 3494 of LNCS., Springer, Heidelberg (May 2005) 371–386

31. Garcia-Morchon, O., Zhang, Z., Bhattacharya, S., Rietman, R., Tolhuizen, L., Torre-Arce, J., Baan, H., O., M., Saarinen, Fluhrer, S., Laarhoven, T., Player, R., Cheon, J.H., Son, Y.: Round5. https://round5.org/
32. Goldwasser, S., Kalai, Y.T., Peikert, C., Vaikuntanathan, V.: Robustness of the Learning with Errors Assumption. In: Innovations in Computer Science - ICS 2010, Tsinghua University, Beijing, China, January 5-7, 2010. Proceedings. (2010) 230–240
33. Goldwasser, S., Kalai, Y.T., Peikert, C., Vaikuntanathan, V.: Robustness of the learning with errors assumption. In Yao, A.C.C., ed.: ICS 2010, Tsinghua University Press (January 2010) 230–240
34. Hamburg, M.: ThreeBears. https://sourceforge.net/projects/threebears/
35. Katz, J., Vaikuntanathan, V.: Signature schemes with bounded leakage resilience. In Matsui, M., ed.: ASIACRYPT 2009. Volume 5912 of LNCS., Springer, Heidelberg (December 2009) 703–720
36. Lewko, A.B., Lewko, M., Waters, B.: How to leak on key updates. In Fortnow, L., Vadhan, S.P., eds.: 43rd ACM STOC, ACM Press (June 2011) 725–734
37. 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) https://eprint.iacr.org/2018/1009.
38. Lyubashevsky, V., Peikert, C., Regev, O.: On Ideal Lattices and Learning with Errors over Rings. J. ACM **60**(6) (November 2013) 43:1–43:35
39. Lyubashevsky, V., Peikert, C., Regev, O.: A toolkit for ring-LWE cryptography. Cryptology ePrint Archive, Report 2013/293 (2013) http://eprint.iacr.org/2013/293.
40. Malkin, T., Teranishi, I., Vahlis, Y., Yung, M.: Signatures resilient to continual leakage on memory and computation. In Ishai, Y., ed.: TCC 2011. Volume 6597 of LNCS., Springer, Heidelberg (March 2011) 89–106
41. Marichal, J.L., Mossinghoff, M.J.: Slices, slabs, and sections of the unit hypercube. arXiv preprint math/0607715 (2006)
42. Micciancio, D., Regev, O.: Worst-case to average-case reductions based on gaussian measures. SIAM Journal on Computing **37**(1) (2007) 267–302
43. Peikert, C.: Lattice Cryptography for the Internet. In: Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014, Waterloo, ON, Canada, October 1-3, 2014. Proceedings. (2014) 197–219
44. Peikert, C.: Lattice cryptography for the internet. In Mosca, M., ed.: Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014, Springer, Heidelberg (October 2014) 197–219
45. Peikert, C.: How (not) to instantiate ring-LWE. In Zikas, V., De Prisco, R., eds.: SCN 16. Volume 9841 of LNCS., Springer, Heidelberg (August / September 2016) 411–430
46. Pietrzak, K.: A leakage-resilient mode of operation. In Joux, A., ed.: EUROCRYPT 2009. Volume 5479 of LNCS., Springer, Heidelberg (April 2009) 462–482
47. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In Gabow, H.N., Fagin, R., eds.: 37th ACM STOC, ACM Press (May 2005) 84–93
48. Sarkar, S., Sengupta, S., Maitra, S.: Partial key exposure attack on RSA - improvements for limited lattice dimensions. In Gong, G., Gupta, K.C., eds.: INDOCRYPT 2010. Volume 6498 of LNCS., Springer, Heidelberg (December 2010) 2–16

49. Stange, K.E.: Algebraic aspects of solving Ring-LWE, including ring-based improvements in the Blum-Kalai-Wasserman algorithm. Cryptology ePrint Archive, Report 2019/183 (2019) https://eprint.iacr.org/2019/183.
50. Takayasu, A., Kunihiro, N.: Partial key exposure attacks on RSA: Achieving the boneh-durfee bound. In Joux, A., Youssef, A.M., eds.: SAC 2014. Volume 8781 of LNCS., Springer, Heidelberg (August 2014) 345–362