Partial Key Exposure in Ring-LWE-Based Cryptosystems: Attacks and Resilience

Dana Dachman-Soled*, Huijing Gong, Mukul Kulkarni, and Aria Shahverdi

University of Maryland, College Park, USA
danadach@ece.umd.edu, gong@cs.umd.edu, {mukul@terpmail, ariash@terpmail}.umd.edu

Abstract. We initiate the study of partial key exposure in ring-LWE-based cryptosystems. Specifically, we

- Introduce the search and decision Leaky-RLWE assumptions (Leaky-SRLWE, Leaky-DRLWE), to formalize the hardness of search/decision RLWE under leakage of some fraction of coordinates of the NTT transform of the RLWE secret and/or error.
- Present and implement an efficient key exposure attack that, given certain 1/4-fraction of the coordinates of the NTT transform of the RLWE secret, along with RLWE instances, recovers the full RLWE secret for standard parameter settings.
- Present a search-to-decision reduction for Leaky-RLWE for certain types of key exposure.
- Analyze the security of NewHope key exchange under partial key exposure of 1/8-fraction of the secrets and error. We show that, assuming that Leaky-DRLWE is hard for these parameters, the shared key v (which is then hashed using a random oracle) is computationally indistinguishable from a random variable with average min-entropy 238, conditioned on transcript and leakage, whereas without leakage the min-entropy is 256.

1 Introduction

Partial key exposure attacks. Many of the cryptanalytic attacks on RSA are based on the seminal "Coppersmith's method," [17,16] which provides an efficient lattice-based algorithm to solve for small roots of a polynomial over a modulus. One of the most beautiful applications of Coppersmith's method is to so-called "partial key exposure attacks" on RSA, introduced by Boneh, Durfee, and Frankel [9]. This class of attacks shows that given 1/2 of the bits of the secret key—either the most or least significant—it is possible to efficiently recover the entire key. The original attack worked for only certain choices of parameters, but a long line of follow-up works have greatly improved the applicability of these results [8,26,41,42]. Partial key exposure attacks are not meant to model realistic leakage attacks (since the attacks only work when the leakage is highly structured), although vulnerability of RSA to key exposure has been exploited in practice, due to flaws in certain prime generation algorithms [7,36]. The main motivation to study these attacks is that they provide a setting in which the algebraic structure of a cryptosystem can be exploited to obtain improvements far beyond what is naively expected. Say, after exposing 1024 bits of a 2048-bit RSA key, one could still hope to maintain the security level of 1024-bit RSA. These attacks show that, in fact, no security at all is maintained after exposing 1024 bits in specific positions. This helps to further our understanding of the algebraic structure of the cryptosystem and how that structure can be leveraged in cryptanalytic attacks.

Enter post-quantum. Recently there has been a huge effort in the cryptographic community to develop "post-quantum" cryptosystems that remain secure even in the presence of quantum adversary. One of the foremost avenues for viable post-quantum public key cryptography is to construct schemes from Ring-LWE (RLWE) assumptions—currently 12 out of 69 submissions for the first round of NIST submissions are based on assumptions in the ring setting. 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

[*] This work is supported in part by NSF grants #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.

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 [38].

The NTT transform. One key method for speeding up computations 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 model for key exposure attacks.

NewHope key exchange protocol. Some of 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 [13] 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 initiate a study of partial key exposure in RLWE based cryptosystems and explore both positive and negative results in this setting. Specifically, we (1) define search and decision versions of Leaky RLWE assumptions, where the structured leakage occurs on the coordinates of the NTT transform of the LWE secret (and/or error); (2) present partial key exposure attacks on RLWE, given 1/4-fraction of structured leakage on the secret key; (3) present a search to decision reduction for the Leaky RLWE assumptions; and (4) 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 ω 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 R-SLWE, is parameterized by $(n' \in \{1, 2, 4, 8, \ldots n\}, \mathcal{S} \subseteq \mathbb{Z}_{2n'}^*)$. The goal is to recover the R-LWE secret $\boldsymbol{s} = \mathsf{NTT}^{-1}(\widehat{\boldsymbol{s}})$, given samples from the distribution $D_{real,n',\mathcal{S}}$ which outputs $\left(\widehat{\boldsymbol{a}}, \widehat{\boldsymbol{a}} \cdot \widehat{\boldsymbol{s}} + \widehat{\boldsymbol{e}}, [\widehat{s}_i]_{i \equiv \alpha \bmod 2n' \mid \forall \alpha \in \mathcal{S}}\right)$, 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 R-SLWE 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 $\left(\widehat{\boldsymbol{a}}, \widehat{\boldsymbol{u}}, [\widehat{s}_i]_{i \equiv \alpha \bmod 2n' \mid \forall \alpha \in S}\right)$, 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', α). 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 α_1^{-1}), See the Technical Overview for additional discussion.

1.2 Our Results

Partial key exposure attacks. We develop attacks on leaky search-RLWE that crucially leverage the algebraic structure of the ring setting. Our attacks demonstrate that leaky search-RLWE is *easy* for leakage parameter settings $(n' = 4, \alpha = 1)$ and $(n' = 8, \mathcal{S} = \{1, 7\})$, $(n' = 8, \mathcal{S} = \{1, 15\})$, under the NewHope parameter settings of $n = 1024$, $q = 12289$, and $\chi = \varPsi_{16}$ (centered binomial distribution of parameter 16). We present and implement efficient algorithms to fully recover the RLWE secret, given specific 1/4-fraction of the positions in the NTT transform of the RLWE secret. We emphasize that the algebraic structure of the ring setting is intrinsic to our results on partial key exposure. In addition, we were also able to successfully recover the entire RLWE secret for $n = 1024$, $q = 12289$ and $\chi = \psi_{16}$ for leakage patterns $(1, 7)$ mod 16 in roughly 15 hours and for $n = 1024$, $q = 12289$ and $\chi = \psi_{16}$ and leakage pattern $(1, 15)$ mod 16 in about 1 hour 17 minutes. The experiments were run using a MacBook Pro with 2.6 GHz Intel Core i5 processor, 16 GB 1600 MHz DDR3 memory, with a python script running 4 parallel processes and using Sage version 8.1. See Section 3.4. Indeed, the NTT notion itself is only applicable to certain specific rings, based on cyclotomic polynomials $\varPhi_m$ and modulus $q \equiv 1 \mod m$. We note that this stands in contrast to the non-leaky setting, where it is not clear how to leverage the algebraic structure of the ring to design improved attacks on RLWE. In addition, our experiments indicate that leaky search-RLWE remains hard for leakage parameter settings $(n' = 8, \alpha = 1)$.

A search-to-decision reduction. Assuming $2^{O(n^{\epsilon})}$ sub-exponential hardness of search-RLWE, fix some desired hardness level $2^{\Omega(n^{\epsilon'})}$, where $\epsilon' \leq \epsilon$. Let n^* be the minimum value in $\{4, 8, 16, 32, \ldots, n\}$ such that it takes $T_{n^*} \in 2^{\Omega(n^{\epsilon'})}$ time to solve the search version of leaky-RLWE, given positions $[\hat{s}^1_i]_{i \equiv \alpha \mod 2n^*}$.

Theorem 1.1 (Informal). *Assume $n^* > 4$, then one of the following must hold:*

(1) $D_{real,n^*,\{\alpha\}} \approx D_{sim,n^*,\{\alpha\}}$ *OR*
(2) $D_{real,n^*,\{\alpha,(n^*-1)\cdot\alpha\}} \approx D_{sim,n^*,\{\alpha,(n^*-1)\cdot\alpha\}}$ *OR*
(3) $D_{real,n^*,\{\alpha,(2n^*-1)\alpha\}} \approx D_{sim,n^*,\{\alpha,(2n^*-1)\alpha\}}$.

While at first glance it may seem that the conclusions (1), (2), (3) are redundant, in fact they are incomparable; Indeed, conclusion (1) does not imply (2) (resp. (3)), since the adversary in (2) (resp. (3)) is given additional leakage. Conversely, conclusion (2) (resp. (3)) does not imply (1), since the set of NTT coordinates that are indistinguishable from random is smaller in (2).

Furthermore, note that the assumption that $n^* > 4$ is validated by our experimental results, which show that leaky search-RLWE is easy for (the NewHope setting of parameters), $n = 1024$, $q = 12289$, error distribution $\chi = \varPsi_{16}$, and $n' = 4$.

We note that the search-to-decision reduction we present crucially relies on the fact that the leakage pattern is highly structured and our techniques do not seem to carry through to cases where arbitrary or random coordinates are leaked.

Resilience of NewHope to partial key exposure.

Theorem 1.2 (Informal). *Assuming that Leaky-DRLWE with leakage parameters $(8, \alpha = 1)$ and RLWE parameters $n = 1024, q = 12289$ and error distribution ζ[1] 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 238, 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, v is indistinguishable from a random variable that has min-entropy 158, conditioned on the transcript and leakage. Note that without leakage, the min-entropy is 256.

As mentioned above, setting $\alpha = 1$ is WLOG, and α can be any value in $\mathbb{Z}^*_{16}$. While the above may 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.

[1] ζ is a rounded Gaussian with standard deviation $\sqrt{8}$, as in the NewHope key exchange protocol.

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 6.4.

Choice of $n' = 8$ in Theorem 1.2. Our experimental results show that the search version of Leaky RLWE seems hard for parameters $(n', \alpha = 1)$, where $n' = 8$ and $\alpha \in \mathbb{Z}_{16}^*$, and is easy for parameters $(n', \alpha = 1)$, where $n' = 4$ (recall that setting $\alpha = 1$ is WLOG). Therefore, 8 is a good candidate for the value of n^* above. Moreover, our search to decision reduction tells us that if indeed $n^* = 8$, then either (1) $D_{real,8,1} \approx D_{sim,8,1}$ OR (2) $D_{real,8,\{1,7\}} \approx D_{sim,8,\{1,7\}}$ OR (3) $D_{real,8,\{1,15\}} \approx D_{sim,8,\{1,15\}}$. However, experimental results show (as discussed above) that we can break the search version of Leaky RLWE for distributions $D_{real,8,\{1,7\}}$ and $D_{real,8,\{1,15\}}$, which precludes (2) and (3). Thus, our experimental results support the conjecture that $D_{real,8,1} \approx D_{sim,8,1}$, for the NewHope parameter settings of $n = 1024$, $q = 12289$, and $\chi = \Psi_{16}$.

1.3 Technical Overview

Partial Key Exposure Attack on NTT Transform. Recall that the secret key is stored in NTT format, i.e. $\widehat{\boldsymbol{s}} := (\boldsymbol{s}(\omega^1), \boldsymbol{s}(\omega^3), \ldots, \boldsymbol{s}(\omega^{2n-1}))$. Note that coordinates of secret key in NTT format are indexed in by the set $\mathbb{Z}_{2n}^*$. We consider partial key exposure attacks in which we leak from $\widehat{\boldsymbol{s}}$ (1) all indices i such that $i \equiv 1 \bmod 8$ (2) all indices i such that $i \equiv 1 \bmod 16$ and for $i \equiv 7 \bmod 16$ (resp. $i \equiv 1 \bmod 16$ and for $i \equiv 15 \bmod 16$).

Given the above coordinates we reconstruct a polynomial $\boldsymbol{s}'$ of lower degree whose evaluation at the indices i matches with the leaked coordinates i.e. for all i in the set of leaked coordinates $\boldsymbol{s}'(\omega^i) = \boldsymbol{s}(\omega^i)$. This means that $\boldsymbol{s}'$ is then equal to the original secret key modulo another polynomial of degree smaller than n. In (1) leaking indices i such that $i \equiv 1 \bmod 8$, $\boldsymbol{s}' = \boldsymbol{s} \bmod (x^{n/4} - \omega^{n/4})$ and in (2) leaking indices i such that $i \equiv 1 \bmod 16$ (and indices such that $i \equiv 7 \bmod 16$) we obtain $\boldsymbol{s}' = \boldsymbol{s} \bmod (x^{n/8} - \omega^{n/8})$ (and another polynomial $\boldsymbol{s}'' = \boldsymbol{s}(x) \bmod (x^{n/8} - \omega^{7 \cdot n/8})$).

This means, in settings (1) (resp. (2)), each coordinate of the reconstructed polynomial provides a linear constraint on a *disjoint* set of coordinates of $\boldsymbol{s}$. In (1) (resp. (2)) there are $n/4$ (resp. $n/8$) independent systems of equations such that solving each system of equation will give us 4 (resp. 8) coordinates of the original RLWE secret $\boldsymbol{s}$. Since these systems are small and disjoint, they allow for attacks that are super-polynomial in the dimension. Specifically, for each system, we can find the most likely corresponding coordinates of the RLWE secret (under distribution $\chi = \Psi_{16}$), Unfortunately, simply choosing the most likely solution for each system as the final guessed key will not work, since the probability that the most likely solution is the correct one for *all* $n/4$ or $n/8$ systems is miniscule.

To solve this problem, we leverage the additional information provided by the RLWE instances. First, we extend the above attack to the error vector, $\boldsymbol{e}$. Note that in NTT transform notation the equation $\widehat{\boldsymbol{a}} \cdot \widehat{\boldsymbol{s}} + \widehat{\boldsymbol{e}} = \widehat{\boldsymbol{u}}$ holds component-wise and so given leakage on certain coordinates of $\widehat{\boldsymbol{s}}$, we can solve for the corresponding coordinates of $\widehat{\boldsymbol{e}}$. We also get to see multiple RLWE instances (which we write in matrix notation) as $(A^1, A^1\boldsymbol{s} + \boldsymbol{e}^1 = u^1), \ldots, (A^t, A^t\boldsymbol{s} + \boldsymbol{e}^t = u^t)$, where each RLWE instance will yield $n/4$ (or $n/8$) linear constraints on the coordinates of $\boldsymbol{e}^i$. Out of all the systems, we take only the likely solutions for which we have very high confidence that they are indeed correct. (E.g. for $n = 1024$, we choose confidence 0.98 for $n/4$ and 0.98 for $n/8$). For these systems, we fix the corresponding coordinates of the error and derive a noiseless system of n variables and 4 (resp. 8) equations. Once we have $n/4$ (resp. $n/8$) such systems, we end up with a final linear system of n variables and n equations, which we can then solve to recover $\boldsymbol{s}$. The attack works if all our guesses are correct, which will occur with probability 0.98^{256} (resp. 0.98^{128}). We also show that in some cases the number RLWE instances are needed in order to obtain a sufficient number of noiselesssystems is not too high. See Section 3 for more details on the attack and results.

Leaky R-LWE Search to Decision Reduction. Our technical contribution is an algorithm that takes a distinguishing adversary *which receives leakage on secret key and error* and uses it to recover large portions of the secret key. Let the RLWE secret be denoted by $\hat{\boldsymbol{s}} := \hat{\boldsymbol{s}}^1$. Assume WLOG that there exists an adversary obtains leakage $[\hat{s}_i^1]_{i \equiv 1 \mod 2n'}$ and distinguishes $\hat{\boldsymbol{u}} = \hat{\boldsymbol{a}} \cdot \hat{\boldsymbol{s}} + \hat{\boldsymbol{e}}$ from $\hat{\boldsymbol{u}}'$, where $\hat{u}_i = \hat{a}_i \cdot \hat{s}_i + \hat{e}_i$ for $i \equiv 1 \mod 2n'$ and otherwise is uniform random[2]. It is not hard to see, using techniques of [32], that this implies an attacker that learns a single index $j \in \mathbb{Z}_{2n}^*$, $j \not\equiv 1 \mod 2n'$, $j \equiv b \mod 2n'$ of the RLWE secret. We present an attack **Attack 1** that uses the above to learn *all* the values $[\hat{s}_i^1]_{i \equiv b^r \mod 2n'}$ for $r \in [n'/2]$. The main idea of attack is to learn all $[\hat{s}_i^1]_{i \equiv b \mod 2n'}$ in the first round, then apply an automorphism to shift the positions $i \equiv b^2 \mod n'$ into the positions $i \equiv b \mod 2n'$, resulting in a permuted RLWE secret, denoted $\hat{\boldsymbol{s}}^2$. Note that applying the automorphism causes the positions $\hat{s}_i^1$ such that $i \equiv b \mod n'$ to shift into the positions $i \equiv 1 \mod 2n'$. This means that we are now back where we started, and the reduction is now able to provide the required leakage (on $[\hat{s}_i^2]_{i \equiv 1 \mod 2n'}$) to the adversary and thus can learn the values of $[\hat{s}_i^2]_{i \equiv b \mod 2n'} = [\hat{s}_i^1]_{i \equiv b^2 \mod n'}$ in the second iteration, $[\hat{s}_i^3]_{i \equiv b \mod 2n'} = [\hat{s}_i^1]_{i \equiv b^3 \mod n'}$ in the third iteration, etc.

Assuming $2^{O(n^\epsilon)}$ sub-exponential hardness of RLWE, fix some desired hardness level $2^{\Omega(n^{\epsilon'})}$, where $\epsilon' \leq \epsilon$. Let n^* be the minimum value in $\{4, 8, 16, 32, \ldots, n\}$ such that it takes $T_{n^*} \in 2^{\Omega(n^{\epsilon'})}$ time to solve the search version of leaky-RLWE, given positions $[\hat{s}_i^1]_{i \equiv 1 \mod 2n^*}$ (i.e. given $1/n^*$-fraction of leakage) and takes time $T_{n^*/2} \notin 2^{\Omega(n^{\epsilon'})}$ time to solve the search version of leaky-RLWE given positions $[\hat{s}_i^1]_{i \equiv 1 \mod n^*}$ (i.e. given $2/n^*$-fraction of leakage). In particular (for sufficiently large n), $T_{n^*/2} < T_{n^*}/2$. Note that assuming that RLWE is at least $2^{\Omega(n^\epsilon)}$-hard, such an n^* must exist. Our theorem shows that for such n^*, a form of DRLWE with leakage holds.

Specifically, given $[\hat{s}_i^1]_{i \equiv 1 \mod 2n^*}$, we show that if there exists a distinguishing adversary, then Attack 1, runs in time at most $T_{n^*}/4$ (and a modified version of the attack takes time $T_{n^*}/2$), can be launched. Moreover, if $b \in \mathbb{Z}_{2n^*}^*$ is such that for some $r \in [n^*/2]$, $b^r \equiv n^* + 1 \mod 2n^*$, then we can combine with our knowledge of $[\hat{s}_i^1]_{i \equiv 1 \mod 2n^*}$ to obtain all values $[\hat{s}_i^1]_{i \equiv 1 \mod n^*}$. This means that we can then run the search attack for $2/n^*$-fraction of leakage to recover all of $\hat{\boldsymbol{s}}$ in time $T_{n^*/2}$. But by assumption $T_{n^*}/4(\text{ resp. } T_{n^*}/2) + T_{n^*/2} < T_{n^*}$, thus leading to contradiction.

The problem with the above approach is that given the structure of the group $\mathbb{Z}_{2n'}^*$, there will be some elements $b \in \mathbb{Z}_{2n^*}^*$ such that $b^2 = 1$. This means that the above algorithm can only learn $[\hat{s}_i^1]_{i \equiv b \mod 2n^*}$ and will not learn $[\hat{s}_i^1]_{i \equiv n^*+1 \mod 2n^*}$. In this case, we do not know how to rule out the possibility that given $[\hat{s}_i^1]_{i \equiv 1 \mod 2n^*}$, the positions $i \equiv b \mod 2n^*$ do not look random. But we show that if this is the case, then given leakage on $[\hat{s}_i^1]_{i \equiv 1 \mod n'}$, $[\hat{s}_i^1]_{i \equiv b \mod n'}$, all the other positions must be indistinguishable from random, since otherwise a variant of Attack 1 can be run.

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 Rec on their approximate inputs locally. The protocol ensures that after running 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 unpredictability 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

[2] Note that the problem is identical when the adversary obtains leakage $[\hat{s}_i^1]_{i \equiv \alpha \mod 2n'}$, for $\alpha \in \mathbb{Z}_{2n'}^*$ since, as we shall see next, an automorphism can be applied to shift all indeces i such that $i \equiv \alpha \mod 2n'$ to positions $i \equiv 1 \mod 2n'$.

protocol is split into vectors $\mathbf{x}_i \in \mathbb{Z}_q^4$, $i \in \{0, \dots n/4-1\}$ 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 $i \in \{n/8, \dots, n/4-1\}$ is indistinguishable from uniform random in $\mathbb{Z}_q^4$ and for $i \in \{0, \dots, n/8-1\}$, is indistinguishable from uniform random, given a single linear constraint. Specifically, for $i \in \{0, \dots, n/8-1\}$, 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 γ_i. The technically difficult part of the proof is showing that, with high probability over γ_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: $(\mathbf{x}, b') \to (\mathbf{x}'_i, b' \oplus 1)$ such that, $\mathsf{HelpRec}(\mathbf{x}_i, b) = (\mathbf{x}_i, b)$ $(= \mathbf{r})$ 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 $i \in \{0, \dots, n/8-1\}$ 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 $\mathsf{HelpRec}(\mathbf{x}_i, b) = (\mathbf{x}_i, b)$ $(= \mathbf{r})$ 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 defined explicitly in later section. 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. [9]. Partial key exposure attacks on RSA are based on a cryptanalytic method known as Coppersmith's method [17,16]. There has been a long sequence of improved partial key exposure attacks on RSA, see for example [8,26,41,42].

Leakage-resilient cryptography. The study of provably secure, leakage-resilient cryptography was introduced by the work of Dziembowski and Pietrzak in [25]. Pietrzak [39] also constructed a leakage-resilient stream-cipher. Brakerski et al. [14] 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 [22,29]. There are also work on leakage-resilient signature scheme [28,12,34].

Robustness of Lattice-based scheme. One of the first and important work is by Goldwasser et al. [27] 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 [40] is robust against an attacker which can measure large fraction of secret key without increasing the size of secret key. Dodis et al. [23] 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. [21] 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. [18] considered the leakage resilience of a RLWE-based public key encryption scheme.

Recently, Brakerski and Perlman [15] studied the robustness of RLWE problem, in cases where the secret polynomial $\boldsymbol{s}$ is not chosen uniform randomly but rather from some distribution with high entropy. They showed that the generalized version of the RLWE problem is at least as hard as solving worst-case lattice problems in the underlying ideal lattices. However, while analyzing distributions similar to the leakage patterns considered in this paper [3] called k-wise independent distributions, they notice that if k-wise independent set is *fixed* then the scheme may not be secure. This supports the attack methodology used in our work.

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 [20], Peikert [37], the NewHope protocol of Alkim et al. [4], the Frodo protocol of Bos et al. [10], and the Kyber protocol of Bos et al. [11]

2 Preliminaries

For a positive integer n, we denote by $[n]$ the set $\{0,\dots,n-1\}$. 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 ℓ_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 $\{0, 1/q, \dots, (q-1)/q\}$.

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 Λ (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 [19]. □

[3] [15] consider that the secret is sampled from a distribution where for indices $j \in T \subseteq [n]$ the coefficients s_j are chosen uniform randomly from R_q and $s_j = 0$ if $j \notin T$.

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 [35, 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 ζ_m of order m (i.e. a primitive m^{th} root of unity) to the rationals. The minimal polynomial of ζ_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 Δ_K of K measures the geometric sparsity of its ring of integers. The discriminant of the m^{th} cyclotomic number field K is

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

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 σ 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 σ since no confusion is likely to arise.

Lemma 2.3 ([33])**.** *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 ([33])**.** *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 [33].

Definition 2.6 (**Ring-LWE Distribution**)**.** *For a "secret" $s \in R_q^{\vee}$ (or just $R^{\vee}$) and a distribution χ over $K_{\mathbb{R}}$, a sample from the ring-*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-*LWE *problem, denoted R-$\mathsf{DLWE}_{q,\chi}$, 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. *[33, Theorem 2.22] Let K be the m^{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* SIVP *(or* SVP*) on ideal lattices in K to the problem of solving R-$\mathsf{DLWE}_{q,\chi}$ given only l samples, where χ is the Gaussian distribution D_{ξ} 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, ω a m^{th} root of unity in $\mathbb{Z}_q$ the NTT of polynomial $\boldsymbol{p} = \sum_{i=0}^{n-1} x^i \in R_q$ 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 NTT^{-1} is the inverse of function 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*

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

Lemma 2.11 ([24])**.** *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 Partial Key Exposure Attack on NTT

3.1 Reconstructing the secret given ($\boldsymbol{\alpha} \mod 8$) leakage.

Recall that the secret key $\boldsymbol{s}$ is represented as a degree $n-1$ polynomial $\boldsymbol{s}(x) = s_0 + s_1 \cdot x + \ldots + s_{n-1} \cdot x^{n-1}$, where $\boldsymbol{s}(x) \in \mathbb{Z}_q[x]/x^n + 1$, n is power of two and $q \equiv 1 \mod 2n$. Let ω be a $2n$-th primitive root in $\mathbb{Z}_q$, i.e. $\omega^{2n} \equiv 1 \mod q$. Then the NTT transform is obtained by evaluating $\boldsymbol{s}(x) \mod q$ at the powers $\omega^1, \omega^3, \ldots, \omega^{2n-1}$. Specifically, $\widehat{\boldsymbol{s}}(x) = \mathsf{NTT}(\boldsymbol{s}(x)) = \langle \boldsymbol{s}(\omega^1) \mod q, \boldsymbol{s}(\omega^3) \mod q, \ldots, \boldsymbol{s}(\omega^{2n-1}) \mod q \rangle$. For $n' \in \{1, 2, 4, 8, \ldots, n\}$ and $\alpha \in \mathbb{Z}^*_{2n'}$, let $\boldsymbol{s}^\alpha_u(x)$ be the degree $u = n/n'$ polynomial that is obtained by taking $\boldsymbol{s}(x)$ modulo $x^{n/n'} - (\omega^\alpha)^{n/n'}$. As discussed earlier, we may assume WLOG that $\alpha = 1$. Therefore, we abbreviate notation and write $\boldsymbol{s}_u$, instead of $\boldsymbol{s}^1_u$.

We consider attacks in which the adversary obtains as leakage all coordinates i of $\widehat{\boldsymbol{s}}(x)$ such that $i \equiv 1 \mod 2n'$ such that $n' \in \{1, 2, 4, 8, \ldots, n\}$.

For $i \in [n']$, the i-th coefficient of $\boldsymbol{s}_u(x)$, i.e. $\boldsymbol{s}_{u,i}$ is equal to

$$s_i + \omega^u \cdot s_{i+u} + \omega^{2 \cdot u} \cdot s_{i+2 \cdot u} + \ldots + \omega^{(n'-1) \cdot u} \cdot s_{i+(n'-1) \cdot u}$$

Note that the coefficients of $\boldsymbol{s}$ can be partitioned into u groups of n', forming independent linear systems, each with n' variables and one equation. Specifically, given only the leakage, the set of feasible secret keys is a cartesian product $\mathcal{S}_1 \times \cdots \times \mathcal{S}_u$, where for $i \in [u]$, the set $\mathcal{S}_i$ is the set of vectors $\{s_i, s_{i+u}, s_{i+2u}, \ldots, s_{i+(n'-1)u}\}$ that satisfy the i-th linear system:

$$\begin{bmatrix} 1 \ \omega^u \ \omega^{2 \cdot u} \ \cdots \ \omega^{(n'-1) \cdot u} \end{bmatrix} \cdot \begin{bmatrix} s_i \\ s_{i+u} \\ s_{i+2 \cdot u} \\ \vdots \\ s_{i+(n'-1) \cdot u} \end{bmatrix} = \begin{bmatrix} s_{u,i} \end{bmatrix}$$

Since the linear systems are independent, we can find the "most likely" secret key, given the leakage, by finding the "most likely" solution for each independent system. Since each system has only n' number of variables, there are at most $q^{n'}$ candidate solutions. For $n' = 4$, we can enumerate over all $q^4 = 12289^4$ possible vectors to find those that satisfy the constraint and then find the "most likely" solution (in fact, we use a meet-in-the-middle approach to reduce the number of candidate solutions, and speed up the attack). When the distribution over secret keys is Gaussian, the "most likely" solution is the one with the smallest norm. Since we are using a binomial distribution, we calculate the exact probability of each solution (using a table of values) under the binomial distribution and pick the one with highest probability.

Unfortunately, simply choosing the candidate secret $\boldsymbol{s}$ to be the one composed of the most likely solution of each system will almost never give the correct answer. Consider that the most likely solution is correct with probability 0.7 even in this case the success probability of recovering the full secret by correctly guessing 128 systems is $0.7^{128} = 1.48^{-18}\%$. . Moreover, the above attack has not leveraged the fact that, in addition to leakage on $\boldsymbol{s}$, we are also provided with RLWE instances! In the following, we describe an improved approach for guessing the secret key, that leverages the fact that we get to see multiple RLWE instances of the form $(\boldsymbol{a}, \boldsymbol{a} \cdot \boldsymbol{s} + \boldsymbol{e} = \boldsymbol{u})$.

First, we note that in NTT transform notation the equation $\widehat{\boldsymbol{a}} \cdot \widehat{\boldsymbol{s}} + \widehat{\boldsymbol{e}} = \widehat{\boldsymbol{u}}$ holds component-wise. Therefore, given leakage on certain coordinates of $\widehat{\boldsymbol{s}}$, we can solve for the corresponding coordinates of $\widehat{\boldsymbol{e}}$, assuming that the corresponding coordinates of $\widehat{\boldsymbol{a}}$ are invertible in $\mathbb{Z}_q$ (which occurs with high probability for random $\widehat{\boldsymbol{a}}$). We also get to see multiple RLWE instances (which we write in matrix notation) as $(A^1, A^1\boldsymbol{s} + \boldsymbol{e}^1 = u^1), \ldots, (A^t, A^t\boldsymbol{s} + \boldsymbol{e}^t = u^t)$. Thus, given leakage on coordinates of $\widehat{\boldsymbol{s}}$, we can learn all the corresponding coordinates of $\widehat{\boldsymbol{e}}^i$, for $i \in [t]$. Note that the previous method for finding most likely solutions for the systems of equations (which was described in terms of the RLWE secret $\boldsymbol{s}$), can work equally well for each $\boldsymbol{e}^t$, since it is sampled from the same distribution as $\boldsymbol{s}$.

Now, our goal will be to carefully choose which sets of variables (from all possible sets of variables in $\boldsymbol{e}^1, \ldots, \boldsymbol{e}^t$) to make a guess on so that the following are satisfied: (1) In total, we guess at least u number of n'-variable sets of coordinates from $\boldsymbol{e}^1, \ldots, \boldsymbol{e}^t$; (2) With high probability *all* our guesses are correct. To see why (1) and (2) allow us to recover the secret, observe that if our guess for the i-th variable set of some $\boldsymbol{e}^j$ is correct (denoted $\boldsymbol{e}^{j,i}$), we learn the following linear system of n' equations and n variables $(A^i_j \cdot \boldsymbol{s} = \boldsymbol{u}^i - \boldsymbol{e}^{j,i})$, where A^i_j is the submatrix of A_j consisting of n' rows corresponding to the i-th variable set of $\boldsymbol{e}^j$ and $\boldsymbol{u}^i$ is the vector of corresponding positions of $\boldsymbol{u}$. So assuming (1) and (2) hold, we can learn u *noiseless* systems of n' linear equations, each with $n = u \cdot n'$ number of variables. Ultimately, we now have a linear system of n variables and n equations, which we can then solve to obtain the candidate $\boldsymbol{s}$. We must now argue that (1) and (2) hold with high probability.

In order to ensure (2), we only guess the value of $\boldsymbol{e}^j_i$ when we have "high confidence" in the "most likely" solution. Specifically, for each (i, j), we want to know when the "most likely" solution to the system

$$\begin{bmatrix} 1 \ \omega^u \ \omega^{2\cdot u} \cdots \omega^{(n'-1)\cdot u} \end{bmatrix} \cdot \begin{bmatrix} e^j_i \\ e^j_{i+u} \\ e^j_{i+2\cdot u} \\ \vdots \\ e^j_{i+(n'-1)\cdot u} \end{bmatrix} = \begin{bmatrix} e^j_{u,i} \end{bmatrix}$$

has probability at least, say 0.98, of being the correct solution. To do this, we enumerate over all solutions and calculate the probability of the "most likely" solutions $\boldsymbol{e}^{*,j}_i := (e^{*,j}_i, e^{*,j}_{i+u}, \ldots, e^{*,j}_{i+(n'-1)u})$ as the ratio of the probability of $\boldsymbol{e}^{*,j}$ over the sum of the probabilities of all solutions. If the ratio is larger than, say 0.98, then we choose to guess this value of $\boldsymbol{e}^{*,j}_i$. Otherwise, we discard it. Thus, our probability of *all* guesses being correct is $0.98^u = 0.98^{n/n'}$. For $n = 1024$ and $n' = 4$, this means that we expect the attack to succeed with probability approx. 0.57%.

Moreover, while computing the exact probability can be relatively computationally intensive, we develop a heuristic that performs nearly as well and is much faster. Specifically, we transform finding the "most likely" solution to the system above to a CVP problem over a n'-dimensional lattice. We then calculate the probability of the solution under the binomial distribution and set some threshold th. If the probability of the solution is above the threshold we keep it, if not we discard it. Experimentally, we show that by setting the threshold correctly, we can still achieve confidence of approximately 0.98.

Our experiments also show that a fairly small number of LWE instances allows for (1) to hold as well. Specifically, for $n = 1024$, $q = 12289$, $\chi = \Psi_{16}$, $n' = 4$, we show that the "most likely" solutions for approx. 3% of the linear systems will have "high confidence" of at least 0.98. Thus, we expect around 33 RLWE instances to be sufficient in order to obtain 256 number of systems of 4 equations, for which each is correct with confidence at least 0.98.

Thus far we focused only on guessing sets of variables from the error terms of the RLWE instances; we extend our attack to guess sets of variables from the RLWE secret as well. Specifically, if a candidate solution for the i-th system, corresponding to the i-th set of u coordinates of the RLWE secret has "high confidence" we can fix those variables to the candidate solution and thus reduce the total number of variables in the final system as described in the following: Let $\boldsymbol{s}_i^* := (s_i^*, s_{i+u}^*, \ldots, s_{i+(n'-1)u}^*)$ denote a candidate solution to the i-th system that has high confidence. Now, consider each RLWE sample $(A^j, A^j\boldsymbol{s} + \boldsymbol{e}^j = u^j$. We denote by $A^{*,j}$ the submatrix obtained by deleting the columns $\{i, i+u, \ldots, i+(n'-1)u\}$ from A^j. Let $A^{j,\ell}$ denote the ℓ-th column of matrix A^j then we update the solution u^j to be $u^{*,j} := u^j - (A^{j,i} \cdot s_i^* + A^{j,i+u} \cdot s_{i+u}^* + \ldots + A^{j,i+(n'-1)u} \cdot s_{i+(n'-1)u}^*)$. If we obtain multiple high confidence candidate for sets of variables of $\boldsymbol{s}$, assume k of them, the above procedure can be done for each of them, reducing the total number of variables in the final system from n to $n - n' \cdot k$.

Confidence	Expected Number of RLWE Instance	Expected Success Probability
0.98	22	0.5
0.95	7	1.96×10^{-4}
0.90	4	1.9×10^{-10}

3.2 Reconstructing the secret given $(\alpha, \alpha \cdot 7 \mod 16)$ leakage

As noted in the previous section, let $\boldsymbol{s}_u^\alpha(x)$ be the degree $u = n/n'$ polynomial that is obtained by taking $\boldsymbol{s}(x)$ modulo $x^{n/n'} - (\omega^\alpha)^{n/n'}$. We consider two polynomial $\boldsymbol{s}_u^\alpha(x)$ and $\boldsymbol{s}_u^{\alpha \cdot 7}(x)$. We may assume WLOG, $\alpha = 1$. The i-th coefficient of $\boldsymbol{s}_u(x)$ and $\boldsymbol{s}_u^7(x)$ are as follows, respectively

$$s_i + \omega^u \cdot s_{i+u} + \omega^{2 \cdot u} \cdot s_{i+2 \cdot u} + \ldots + \omega^{(n'-1) \cdot u} \cdot s_{i+(n'-1) \cdot u}$$

$$s_i + \omega^{7 \cdot u} \cdot s_{i+u} + \omega^{7 \cdot 2 \cdot u} \cdot s_{i+2 \cdot u} + \ldots + \omega^{7 \cdot (n'-1) \cdot u} \cdot s_{i+(n'-1) \cdot u}$$

Similar to previous subsection we form the equation to solve the secret key as follows,

$$\begin{bmatrix} 1 & \omega^u & \omega^{2 \cdot u} & \cdots & \omega^{(n'-1) \cdot u} \\ 1 & \omega^{7 \cdot u} & \omega^{7 \cdot 2 \cdot u} & \cdots & \omega^{7 \cdot (n'-1) \cdot u} \end{bmatrix} \cdot \begin{bmatrix} s_i \\ s_{i+u} \\ s_{i+2 \cdot u} \\ \vdots \\ s_{i+(n'-1) \cdot u} \end{bmatrix} = \begin{bmatrix} s_{u,i} \\ s_{u,i}^7 \end{bmatrix}$$

For $n' = 8$, we should enumerate over $q^8 = 12289^8$ possible vectors to find the "most likely" (in order to solve the above equation we use meet-in-the-middle approach). The "most likely" key candidate is the one with smallest norm.

Similar to previous section our goal is to carefully choose the answers with "high confidence" such that (1) In total, we guess at least u number of n'-variable sets from $\boldsymbol{e}^1, \boldsymbol{e}^2, \ldots, \boldsymbol{e}^t 1$ (2) With high probability all our guess are correct. We choose the candidate which has probability of at least 0.95 of being correct solution. The total probability of success for this case is $0.95^u = 0.95^{n/n'}$. For $n = 1024$ and assuming $n' = 8$ we have success probability of $0.95^{128} = 0.14\%$.

As was mentioned in the previous subsection, we transform the computation of solutions with high confidence to a CVP problem over an n'-dimensional lattice. Experimentally, for $n = 1024$, $q = 12289$, $\chi = \Psi_{16}$, $n' = 8$, we show that approx. 0.56% of the solutions have "high confidence" of at least 0.95. We expect to need 178 RLWE instance to be sufficient in order to obtain 128 number of systems of 8 equations, for which the confidence is at least 0.95.

The following table summarizes the estimates obtained by solving the CVP problem for 128000 systems of size 8.

Confidence	Expected Number of RLWE Instance	Expected Success Probability
0.98	1778	7.5324%
0.95	178	0.1408%
0.9	18	1.3×10^{-6}%

3.3 Difficulty of Reconstructing the secret given ($\alpha \mod 16$) leakage

Unfortunately, our techniques do not seem to extend to 1/8-fraction of leakage, leading us to conjecture that search-RLWE with leakage is hard for these parameters. Similar to previous section, let $\boldsymbol{s}_u^\alpha(x)$ be the degree $u = n/n'$ polynomial that is obtained by taking $\boldsymbol{s}(x)$ modulo $x^{n/n'} - (\omega^\alpha)^{n/n'}$. We assume WLOG, $\alpha = 1$. The $i - th$ coefficient of $\boldsymbol{s}_u^\alpha(x)$ is equal to

$$s_i + \omega^u \cdot s_{i+u} + \omega^{2\cdot u} \cdot s_{i+2\cdot u} + \ldots + \omega^{(n'-1)\cdot u} \cdot s_{i+(n'-1)\cdot u}$$

Similar to the case ($\alpha \mod 8$), to find key candidates the following equation should be solved

$$\begin{bmatrix} 1 \; \omega^u \; \omega^{2\cdot u} \; \cdots \; \omega^{(n'-1)\cdot u} \end{bmatrix} \cdot \begin{bmatrix} s_i \\ s_{i+u} \\ s_{i+2\cdot u} \\ \vdots \\ s_{i+(n'-1)\cdot u} \end{bmatrix} = \begin{bmatrix} s_{u,i} \end{bmatrix}$$

For $n' = 8$, we can enumerate over all $q^8 = 12289^8$ possible vectors to find those that satisfy the constraint. In order to perform this enumeration efficiently, a meet-in-the-middle approach is used. Similar to the previous section we would like to guess the solution in cases in which we have "high confidence". For the case of $n' = 8$, however, we experimentally found that the probability of the most probable solution was always less than 0.12. This means that we cannot hope to obtain a sufficient number of noiseless linear constraints on the secret $\boldsymbol{s}$. In particular, with at most 0.12 confidence, we expect the probability of success of our attack to be at most $0.12^{n/n'} = 1.36 \times 10^{-116}$, which is clearly negligible.

3.4 Experimental Results

We wish to highlight that in agreement to our estimates we were able to successfully recover the entire RLWE secret for various dimensions as listed in Table 1. Specifically we were able to recover an entire secret key for $n = 1024$, $q = 12289$ and $\chi = \psi_{16}$ for leakage patterns $(1, 7)$ mod 16 in roughly 15 hours and for $n = 1024$, $q = 12289$ and $\chi = \psi_{16}$ and leakage pattern $(1, 15)$ mod 16 in about 1 hour 17 minutes.

The experiments were run using a MacBook Pro with 2.6 GHz Intel Core i5 processor, 16 GB 1600 MHz DDR3 memory, with a python script running 4 parallel processes and using Sage version 8.1

In the following table, n is the dimension of RLWE instance, $\mathcal{S}$ is the set of indices that we leak (e.g. 1mod16, N is the Number of RLWE Instance that were required to recover the key and p is the Expected Success Probability.

n	$\mathcal{S}$	Confidence	N	p
256	$1, 15$	0.95	125	19.3711%
512	$1, 7$	0.95	178	3.7524%
1024	$1, 7$	0.98	1929	7.5324%
1024	$1, 15$	0.95	170	0.1408%
1024	$1, 9$	0.98	22	0.5%

Table 1: Expected Success Probability of our Attack

4 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 $(p_0, \dots, p_{n-1})$. For $p \in R_q$ we denote $\widehat{\boldsymbol{p}} := \mathsf{NTT}(\boldsymbol{p}) := (\boldsymbol{p}(\omega^1), \boldsymbol{p}(\omega^3), \dots, \boldsymbol{p}(\omega^{2n-1}))$, where ω 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 ω^i. Note that $\widehat{\boldsymbol{p}}$ is indexed by the set $\mathbb{Z}^*_{2n}$.

Definition 4.1 (**Ring-LWE, Search with Leakage**). *The* search *version of the ring-*LWE *problem with leakage, denoted R-$\mathsf{SLWE}_{q,\psi,n',\mathcal{S}}$, is parameterized by $(n' \in \{1, 2, 4, 8, \dots n\}, \mathcal{S} \subseteq \mathbb{Z}^*_{2n'})$. 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 4.2 (**Ring-LWE, Decision with Leakage**). *The* decision *version of the ring-*LWE *problem with leakage, denoted R-$\mathsf{DLWE}_{q,\psi,n',\mathcal{S}}$, is parameterized by $(n' \in \{1, 2, 4, 8, \dots n\}, \mathcal{S} \subseteq \mathbb{Z}^*_{2n'})$. 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*

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

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 $[\widehat{e_i}]_{i \equiv \alpha \bmod 2n' \mid \forall \alpha \in S}$.

Also note that if decisional RLWE with leakage parameterized by $(n', \mathcal{S})$ as above is hard for randomly 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 randomly distributed elsewhere. This is because given an RLWE instance with leakage $\left(\widehat{\boldsymbol{a}}, \widehat{\boldsymbol{u}}, [\widehat{s_i}]_{i \equiv \alpha \bmod 2n' \mid \forall \alpha \in S}\right)$, 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', α).

We present a search to decision reduction in Section 5.

5 Search to Decision Reduction With Leakage

For a polynomial $\boldsymbol{v} \in R_q$, recall that $\hat{\boldsymbol{v}}$ denotes the NTT representation of $\boldsymbol{v}$, where $\hat{\boldsymbol{v}}$ is indexed by the set $\mathbb{Z}^*_{2n}$, so $\hat{\boldsymbol{v}} = \hat{v}_1, \hat{v}_3, \dots, \hat{v}_{2n-1}$, where $\widehat{v}_i := \boldsymbol{v}(\omega^i)$ for $i \in \mathbb{Z}^*_{2n}$ and ω is $2n$–th root of unity in $\mathbb{Z}_q$. We state the new definitions and theorems sometimes in terms of $\widehat{\boldsymbol{a}}, \widehat{\boldsymbol{s}}, \widehat{\boldsymbol{e}}$ instead of $\boldsymbol{a}, \boldsymbol{s}, \boldsymbol{e}$ since the leakage we consider is on the NTT transform which is used for efficient computations. Note that this is equivalent to considering $\boldsymbol{a}, \boldsymbol{s}, \boldsymbol{e}$ as NTT is efficiently invertible.

Let $\phi_{i\to j}$ be the automorphism that maps $\hat{\boldsymbol{v}}$ to $\hat{\boldsymbol{v}}'$ such that $\boldsymbol{v}(\omega^i) = \boldsymbol{v}'(\omega^j)$. $\phi_{i\to j}$ induces a permutation on the elements of $\hat{\boldsymbol{v}}$, denoted $\rho_{i\to j}$. Specifically, $\phi_{i\to j}(\hat{\boldsymbol{v}})$ maps $\hat{v}_\ell$ to $\hat{v}_{\rho_{i\to j}(\ell)}$ for $i, j, \ell \in \mathbb{Z}^*_{2n}$.

Fact 5.1. *If $i \equiv \alpha \mod 2n'$, $j \equiv \beta \mod 2n'$, and $\ell \equiv \gamma \mod 2n'$ then $\rho_{i\to j}(\ell) \equiv \alpha^{-1}\gamma\beta \mod 2n'$.*

The following theorem follows straightforwardly from [31,30].

Theorem 5.2 (Existence of Basic Attack). *If, for any $(n', \mathcal{S} \subseteq \mathbb{Z}^*_{2n'})$ adversary $\mathcal{A}$ running in time T distinguishes $D_{real,\mathcal{S},n'}$ from $D_{sim,\mathcal{S},n'}$ with probability $1/T$, then is some index j such that $j \neq \alpha' \mod n$ for all $a' \in \mathcal{S}$ and an attack "Basic Attack" that learns NTT coordinate $\hat{s}_j$ with probability $1 - 1/\mathsf{poly}(n)$ and takes time $\mathsf{poly}(n) \cdot T^2$.*

Attack 1: On input RLWE instance $(\hat{\boldsymbol{a}}, \hat{\boldsymbol{u}})$, index $j \in \mathbb{Z}^*_{2n}$, where $j \equiv b \mod 2n'$, leakage $[\hat{s}_i]_{i\equiv 1 \mod 2n'}$, and adversary $\mathcal{A}$ running in time T that distinguishes on index j with probability $1/T$:

1. Set $\hat{\boldsymbol{a}}^1 := \hat{\boldsymbol{a}}, \hat{\boldsymbol{u}}^1 := \hat{\boldsymbol{u}}$, $[\hat{s}^r_i := \hat{s}_i]_{i\equiv 1 \mod 2n'}$.
2. **Loop invariant: at the beginning of the outer loop, adversary always knows $[\hat{s}^r_i]_{i\equiv 1 \mod 2n'}$.**
3. For $r \in [n'/2]$, For each j' such that $j' \equiv j \mod 2n'$:
   (a) Run the Basic Attack with RLWE instance $(\hat{\boldsymbol{a}} := \phi_{j'\to j}(\hat{\boldsymbol{a}}^r), \hat{\boldsymbol{u}} := \phi_{j'\to j}(\hat{\boldsymbol{u}}^r))$, leakage set $[\hat{s}_i := \hat{s}^r_{\rho_{j'\to j}(i)}]_{i\equiv 1 \mod 2n'}$ to recover $\hat{s}^r_{j'}$. Note that all these values of $\hat{s}^r_{\rho_{j'\to j}}(i)$ are known: If $i \equiv 1 \mod 2n'$ then $\rho_{j'\to j}(i) \equiv 1 \mod 2n'$, since $j \equiv j' \mod 2n'$.
4. Note that at the end of the inner loop, (w.h.p.) all $\hat{s}^r_{j'}$ such that $j' \equiv b \mod 2n'$ are known.
5. Choose an $\ell \in \mathbb{Z}^*_{2n}$ such that $\ell \equiv b^2 \mod 2n'$. Set $\hat{\boldsymbol{a}}^{r+1} := \phi_{\ell\to j}(\hat{\boldsymbol{a}}^r)$ and $\hat{\boldsymbol{u}}^{r+1} := \phi_{\ell\to j}(\hat{\boldsymbol{u}}^r)$. Note that the adversary now knows $[\hat{s}^{r+1}_i]_{i\equiv 1 \mod 2n'}$, since all elements $\hat{s}^r_{i'}$ such that $i' \equiv b \mod 2n'$ are now in position $\hat{s}^{r+1}_i$ such that $i \equiv 1 \mod 2n'$.

At the end of the execution, the adversary learns all values s_i such that $i \equiv b^r \mod 2n'$ and $r \in [n'/2]$.

For parameter n', let $T_{n'}$ denote the time it takes to solve search-RLWE, under leakage attack parameterized by $(n', \alpha = 1)$.

Assuming $2^{O(n^\epsilon)}$ sub-exponential hardness of LWE, fix some ϵ'. Let n^* be the minimum element in the set $\mathcal{S}$, where $\mathcal{S} := \{n' \in \{2, 4, 8, \ldots, n\} \mid T_{n'} \in 2^{O(n^{\epsilon'})}\}$. Note that it must be the case that $T_{n^*} > 2 \cdot T_{n^*/2}$.

Recall that, 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 $p(n)$.

Theorem 5.3. *Assume $n^* > 4$, then one of the following must hold:*

- $D_{real,n^*,\{\alpha\}} \approx_{t(n),p(n)} D_{sim,n^*,\{\alpha\}}$ *OR*
- $D_{real,n^*,\{\alpha,(n^*-1)\cdot\alpha\}} \approx_{t(n),p(n)} D_{sim,n^*,\{\alpha,(n^*-1)\cdot\alpha\}}$ *OR*
- $D_{real,n^*,\{\alpha,(2n^*-1)\alpha\}} \approx_{t(n),p(n)} D_{sim,n^*,\{\alpha,(2n^*-1)\alpha\}}$.

where, $t(n) = \sqrt{T_{n^*}}/\mathsf{poly}(n) = p(n)$

Proof. As discussed above, due to the automorphisms, we can assume WLOG that $\alpha = 1$. Assume $D_{real,n^*,\{1\}} \not\approx_{\sqrt{T_{n^*}}/\mathsf{poly}(n),\mathsf{poly}(n)/\sqrt{T_{n^*}}} D_{sim,n^*,\{1\}}$. Then there must be an adversary A running in time $\sqrt{T_{n^*}}/\mathsf{poly}(n)$, that distinguishes on index $j \in \mathbb{Z}^*_{2n}$, where $j \equiv b \mod 2n'$ with probability at least $\mathsf{poly}(n)/\sqrt{T_{n^*}}$.

Case 1: b is such that $b^r \equiv n^*+1 \mod 2n^*$ for some $r \in [n^*/2]$. In this case, we can use Attack 1 to recover the positions i such that $i \equiv n^*+1 \mod 2n^*$ (w.h.p.) in time $\mathsf{poly}(n) \cdot T_{n^*}/4\mathsf{poly}(n)$. Now we can run the attack that takes as input $[\hat{s}_i]_{i \equiv 1 \mod n^*}$ and recovers all of $\hat{\boldsymbol{s}}$. By assumption, this attack runs in time $T_{n^*/2} < T_{n^*}/2$. Thus, we can to recover the whole $\hat{\boldsymbol{s}}$ in time $\mathsf{poly}(n) \cdot T_{n^*}/4\mathsf{poly}(n) + T_{n^*/2} < T_{n^*}$, which is a contradiction.

By properties of the group $\mathbb{Z}^*_{2n^*}$, where n^* is a power of two, for all $b \in \mathbb{Z}^*_{2n^*} \setminus \{n^*-1, 2n^*-1\}$, it is the case that $b^r \equiv n^*+1 \mod 2n^*$ for some $r \in [n^*/2]$. Thus, Case 1 holds for all $b \in \mathbb{Z}^*_{2n^*} \setminus \{n^*-1, 2n^*-1\}$.

Case 2: $b = n^*-1$. In this case, we can use Attack 1 to recover the positions i such that $i \equiv n^*-1 \mod 2n^*$ (w.h.p.) in time $\mathsf{poly}(n) \cdot T_{n^*}/4\mathsf{poly}(n)$. Assume $D_{real,n^*,\{1,(n^*-1)\}} \not\approx_{\sqrt{T_{n^*}}/\mathsf{poly}(n),\sqrt{T_{n^*}}/\mathsf{poly}(n)} D_{sim,n^*,\{1,(n^*-1)\}}$, then there must be some adversary $\mathcal{A}'$ that distinguishes on index $j' \in \mathbb{Z}^*_{2n}$, where $j' \equiv b' \in \mathbb{Z}^*_{2n^*} \setminus \{1, n^*-1\}$. We can combine this with the previous attack as follows:

Case 2(a): $b' \in \mathbb{Z}^*_{2n^*} \setminus \{1, n^*-1, 2n^*-1\}$. Due to essentially the same argument as before, we can (w.h.p.) learn all $[\hat{s}_i]_{i \equiv (b')^r \mod 2n^*}$ for $r \in [n^*/2]$ in time $\mathsf{poly}(n) \cdot T_{n^*}/2\mathsf{poly}(n)$ and then apply the same argument as above.

Specifically, given the initial leakage $[\hat{s}^1_i]_{i \equiv 1 \mod 2n^*}$, the attack will first learn $[\hat{s}^1_i]_{i \equiv n^*-1 \mod 2n^*}$, then learn $[\hat{s}^1_i]_{i \equiv b' \mod 2n^*}$, then, for some (j, j') such that $j \equiv b' \mod 2n^*$ and $j' \equiv 1 \mod 2n^*$, apply automorphism $\phi_{j \to j'}$ to get $\hat{\boldsymbol{s}}^2$, learn $[\hat{s}^2_i]_{i \equiv n^*-1 \mod 2n^*}$, then learn $[\hat{s}^2_i]_{i \equiv b' \mod 2n^*}$, etc. thus ultimately learning $[\hat{s}_i]_{i \equiv (b')^r \mod 2n^*}$ for $r \in [n^*/2]$. At this point, we will have $[\hat{s}_i]_{i \equiv 1 \mod n^*}$ and thus can learn all of $\hat{\boldsymbol{s}}$ in additional time $T_{n^*/2} < T_{n^*}/2$. Thus, in total the attack takes time $\mathsf{poly}(n) \cdot T_{n^*}/2\mathsf{poly}(n) + T_{n^*/2} < T_{n^*}$, leading to contradiction.

Case 2(b): $b' = 2n^*-1$. Due to essentially the same argument as before, we can (w.h.p.) recover the positions i such that $i \equiv 2n^*-1 \mod 2n^*$ in time $\mathsf{poly}(n) \cdot T_{n^*}/4\mathsf{poly}(n)$. The adversary now knows $[\hat{s}_i]_{i \equiv n^*-1 \mod n^*}$. We can thus can learn all of $\hat{\boldsymbol{s}}$ in additional time $T_{n^*/2} < T_{n^*}/2$. Thus, in total the attack takes time $\mathsf{poly}(n) \cdot T_{n^*}/4\mathsf{poly}(n) + T_{n^*/2} < T_{n^*}$, leading to contradiction.

Case 3: $b = 2n^*-1$. This essentially follows identically to Case 2.

□

6 Leakage Analysis of New Hope Key Exchange

6.1 New Hope Key Exchange scheme

It contains New Hope key exchange scheme and subroutines of $\mathsf{HelpRec}$ 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 $\mathcal{V}$ be the Voronoi cell of $\tilde{D}_4$. [4]

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 $\boldsymbol{e} \in \mathcal{V}$. 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 6.1 :

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

Algorithm 6.1 (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 $\boldsymbol{x} + \mathbb{Z}^4 : \boldsymbol{x} - k\boldsymbol{g} \in \mathscr{V} + \mathbb{Z}^4$

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

Lemma 6.2. *(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* $\mathsf{Decode}(k\boldsymbol{g} + \boldsymbol{e}) = k$.

Let us now present the algorithm CVP, which will be used as subroutine in reconciliation algorithms, as follows:

Algorithm 6.3 (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 $\boldsymbol{x} : \boldsymbol{x} - \boldsymbol{Bz} \in \mathscr{V}$
    $\boldsymbol{v}_0 \leftarrow \lfloor \boldsymbol{x} \rceil$
    $\boldsymbol{v}_1 \leftarrow \lfloor \boldsymbol{x} - \boldsymbol{g} \rceil$
    $k \leftarrow (\|\boldsymbol{x} - \boldsymbol{v}_0\| < 1)\ ?0 : 1$
    $(v_0, v_1, v_2, v_3)^t \leftarrow \boldsymbol{v}_k$
    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 6.4. *(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 6.5 (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 6.6. *(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 6.5 $k = k'$. Additionally, if $\boldsymbol{x}$ is uniform, then k is uniform independently of $\boldsymbol{r}$.*

We now present the complete NewHope key exchange protocol given in [3] as protocol 6.7.

Algorithm 6.7 (Protocol 2)**.** *Parameters:* $q = 12289$, $n = 1024$ *Error Distribution:* Ψ_{16}^n

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

6.2 Security with Auxiliary Inputs

In this section we consider a modification to Protocol 6.7 in which all binomial random variables are instead drawn from discrete Gaussians with corresponding standard deviation σ. We prove in Corollary 6.15 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 obtain our main result.

The proof of Corollary 6.15 has two components. In the first (computational) component (proof of Theorem 6.8), 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) component (proof of Theorem 6.9), we analyze the expected min-entropy of $v \leftarrow \mathsf{Rec}(\boldsymbol{v}'', \boldsymbol{r})$, conditioned on the adversary's view which now includes the reconciliation information $\boldsymbol{r} \leftarrow \mathsf{HelpRec}(\boldsymbol{v}'', b)$. These are then combined to obtain Corollary 6.15.

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

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

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.

Theorem 6.8. *If ring-LWE decision problem with leakage is hard as defined in Section 4 with parameters* $(n' = 8, \alpha \in \mathbb{Z}^*_{2n'})$*, then*

(1) The marginal distribution over $[\widehat{v}_i]_{i \equiv \alpha \mod 2n'}$*, is computationally indistinguishable from uniform random over* $\mathbb{Z}_q^{n/n'}$*.*

(2) Given the adversary's view, 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. (Proof of theorem 6.8):

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 6.1. $H_0 \approx H_1$

Claim 6.1 follows from the ring-LWE with leakage assumption defined in Section 4

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 6.2. $H_1 \approx H_2$

Claim 6.2 follows from the decision ring-LWE with leakage assumption defined in Section 4.

Hybrid H_3**:** This is same as hybrid H_2 except that we replace $\boldsymbol{v}'$ by a random vector from $\mathbb{Z}_q^n$, $\boldsymbol{v}''$, and for $i \equiv \alpha \mod 2n'$, replace $\widehat{e}''_i$ with $\widehat{e}'''_i = \widehat{v}''_i - \widehat{a}_i \cdot \widehat{s}'_i$ for $i \equiv \alpha \mod 2n'$.

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

Claim 6.3. $H_2 \approx H_3$

Claim 6.3 follows since the error coordinates $[\widehat{e}''_i]_{i \equiv \alpha \mod 2n'}$ are statistically close to uniform over Z_q, since there is a bijection between the vector $[\widehat{e}''_i]_{i \equiv \alpha \mod 2n'}$ and the polynomial $\boldsymbol{f} := \boldsymbol{e}'' \mod (x^{n/8} - (\omega^j)^{n/8})$. Moreover, $\boldsymbol{f}$ is statistically close to uniform random since it is sampled by drawing ring element $\boldsymbol{e}''$ from a discrete Gaussian of standard deviation σ and taking it modulo an ideal $\mathcal{I} = \langle q \rangle + \langle x^{n/8} - (\omega^j)^{n/8} \rangle$ with sufficiently high norm. Specifically, with parameter settings $\sigma = \sqrt{8}$ for error, the noise distribution has pdf proportional to

$$e^{-x^2/(2 \cdot \sigma^2)} = e^{-x^2/(2 \cdot \sqrt{8}^2)} = e^{-\pi x^2/(\sqrt{16 \cdot \pi}^2)} = e^{-\pi x^2/((4\sqrt{\pi})^2)} = e^{-\pi x^2/(\tilde{\sigma}^2)},$$

where $\tilde{\sigma} = 4\sqrt{\pi}$. Additionally, $\mathcal{I} = \langle q \rangle + \langle x^{n/8} - (\omega^j)^{n/8} \rangle$, which is the ideal corresponding to the leaked NTT coordinates, has norm $q^{n/8}$. Thus, $\boldsymbol{f}$ should be statistically close to random, since the smoothing parameter of $\mathcal{I}$ for $\epsilon = 2^{-2n}$ is $\eta_\epsilon(\mathcal{I}) \leq \frac{\sqrt{n}}{\lambda_1(\mathcal{I}^V}$. Since $\lambda_1(\mathcal{I}^V) \geq \sqrt{n} \cdot N(\mathcal{I}^V)^{1/n} = \sqrt{n} \cdot N(\mathcal{I})^{-1/n} = \sqrt{n} \cdot q^{-1/8}$ (see [38] for details), then we have $\eta_\epsilon(\mathcal{I}) \leq q^{1/8} \approx 3.245 < \tilde{\sigma}$.

It is clear by inspection that (1) and (2) of Theorem 6.8 hold in Hybrid 3. □

Switching from NTT to polynomial representation. We showed that in Hybrid H_3, 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

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

We take the right hand side of (1) to be a constant, denoted by γ_i. Let $\boldsymbol{c}_{\omega,\alpha} = [1 \ \ (\omega^\alpha)^{n/4} \ \ (\omega^\alpha)^{n/2} \ \ (\omega^\alpha)^{3n/4}]$. Thus the linear constraint corresponding to (1) 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. Therefore, 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 $\mathcal{D}_{\boldsymbol{\gamma}} = (\mathcal{D}_{\gamma_0}, \ldots, \mathcal{D}_{\gamma_{n/8-1}})$, 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 $\boldsymbol{c}_{\omega,\alpha} \cdot \mathbf{x}_i = \gamma_i$. Moreover, since there is a bijection between $[\widehat{v}''_i]_{i \equiv \alpha \bmod 2n'}$ and the values of the constraints $[\gamma_i]_{i \in \{0,\ldots,n/8-1\}}$, we have that if $[\widehat{v}''_i]_{i \equiv \alpha \bmod 2n'}$ is uniformly random, then $\boldsymbol{\gamma} = [\gamma_i]_{i \in \{0,\ldots,n/8-1\}}$ is also uniformly random.

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. This then fixes the values of $\boldsymbol{\gamma} = \gamma_1, \ldots, \gamma_{n/8}$. For each $i \in \{0, \ldots, n/8-1\}$, $\mathbf{x}_i$ is sampled independently from $\mathcal{D}_{\gamma_i}$ (defined in the preceding paragraph). Thus, we can analyze each block $\mathbf{x}_i$ independently to show that the average min-entropy of $\mathsf{Rec}(\mathbf{x}_i, \mathbf{r}_i)$, conditioned on $\mathbf{r}_i \leftarrow \mathsf{Rec}(\mathbf{x}_i; b_i)$ is close to 1. Due to independence, we can then sum the average min-entropies of each block to obtain the average min-entropy of v.

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 Rec for $i \in \{n/8, \ldots, n/4-1\}$ has (average) min-entropy exactly 1, conditioned on the leakage and transcript. Thus, it remains to show that for $i \in \{0, \ldots, n/8-1\}$, conditioned on the output of $\mathsf{HelpRec}$, the output of Rec has high average min-entropy.

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.

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

Theorem 6.9. *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

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

.

By definition of average min-entropy, the above implies that, for a single block, $\mathsf{Rec}(\mathbf{x}, \mathbf{r})$ has average min-entropy at least $-\log_2(1/2 + p)$, conditioned on $\gamma, \mathbf{r}$.

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:

$$\boldsymbol{c}_{\omega,\alpha} \cdot \mathbf{x} = \boldsymbol{c}_{\omega,\alpha} \cdot \mathbf{x}' \tag{2}$$

$$(\mathbf{r} =)\ \mathsf{HelpRec}(\mathbf{x}; b) = \mathsf{HelpRec}(\mathbf{x}'; b'), \tag{3}$$

$$\mathsf{Rec}(\mathbf{x}, \mathbf{r}) = 1 \oplus \mathsf{Rec}(\mathbf{x}', \mathbf{r}), \tag{4}$$

where $b' = b \oplus 1$.

Now the above conditions imply that:

$$\frac{1}{q} \cdot \sum_{(\gamma, \mathbf{r})} \Pr_{\mathcal{R}_\gamma}[\mathbf{r}] \cdot \Pr_{\substack{\mathbf{x} \sim \mathcal{S}_\gamma \\ b \sim \{0,1\}}} [\mathsf{HelpRec}(\mathbf{x}; b) \neq \mathsf{HelpRec}(\mathbf{x}'; b') \mid \mathsf{HelpRec}(\mathbf{x}; b) = \mathbf{r}] \leq p. \tag{5}$$

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 6.9, 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 (5).

We now turn to defining $\psi_{\boldsymbol{c}_{\omega,\alpha}}$ and proving that with probability at least $1-p$ over uniform $\mathbf{x}$, (2), (3) and (4) hold.

Defining $\psi_{\boldsymbol{c}_{\omega,\alpha}}$ so that (2) always holds. (2) 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 $vt_i \in [\frac{q}{2} \pm q^{1/4}] \cup \mathbb{Z}$. Experiment shows that the intersection of set $\ker(\boldsymbol{c}_{\omega,\alpha})$ and set $\mathbf{W}$ is nonempty given parameter setting of [5], namely fixing $q = 12289, n = 1024, \omega = 7$, $\ker(f_{\omega,j}) \cap \mathbf{W} \neq \varnothing$ for all $\alpha \in \mathbb{Z}_{16}^*$. **Note that this is the only part of the analysis that is not generic in terms of parameter settings. For more discussion, See Section 6.4.** 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 (2) holds with probability 1 over choice of $\mathbf{x}$.

If (3) holds then (4) 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 6.10. *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

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

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 $\mathsf{Rec}(\mathbf{x},\mathbf{r}) = 1 \oplus \mathsf{Rec}(\mathbf{x}+\mathbf{w},\mathbf{r})$. □

(3) 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 $\mathbf{g} \in \tilde{D}_4$, we have $\mathsf{HelpRec}(\mathbf{x};b) = \mathsf{HelpRec}(\mathbf{x}+q\mathbf{g};b')$ [5]. 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 $\mathsf{HelpRec}(\mathbf{x};b) = \mathsf{HelpRec}(\mathbf{x}+\mathbf{w};b')$ 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 6.3, 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 $\mathsf{CVP}_{\tilde{D}_4}$ algorithm, shown in Figure 6.3 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) $\boldsymbol{v}_1' \neq \boldsymbol{v}_1$
(c) $k' \neq 1-k$

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 6.11. *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, 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

$$\begin{aligned}
\mathrm{Prob}_{\mathbf{x},b'}[\mathbf{x} \in \mathcal{D}] &= \frac{1}{2}\mathrm{Prob}_{\mathbf{x},0}[\frac{2^r}{q}(\mathbf{x} + q\mathbf{g} \in \mathcal{D}')] + \frac{1}{2}\mathrm{Prob}_{\mathbf{x},1}[\frac{2^r}{q}(\mathbf{x} + q\mathbf{g} + \mathbf{g} \in \mathcal{D}')] && (6)\\
&= \frac{1}{2}\frac{\left|\frac{2^r}{2q}(2\mathbb{Z}_{2q}^4 + \mathbb{Z}_{2q}^4) \cap \mathcal{D}'\right|}{\left|\frac{2^r}{2q}(2\mathbb{Z}_{2q}^4 + \mathbb{Z}_{2q}^4)\right|} + \frac{1}{2}\frac{\left|\frac{2^r}{2q}(2\mathbb{Z}_{2q}^4) \cap \mathcal{D}'\right|}{\left|\frac{2^r}{2q}(2\mathbb{Z}_{2q}^4)\right|} && (7)\\
&= \frac{\left|\left(\frac{2^r}{2q}(2\mathbb{Z}_{2q}^4 + \mathbb{Z}_{2q}^4) \cup \frac{2^r}{2q}(2\mathbb{Z}_{2q}^4)\right) \cap \mathcal{D}'\right|}{\frac{2^r}{2q}(\mathbb{Z}_{2q}^4)} && (8)\\
&= \frac{\left|\frac{2^r}{2q}(\mathbb{Z}_{2q}^4) \cap \mathcal{D}'\right|}{\frac{2^r}{2q}(\mathbb{Z}_{2q}^4)} = \mathrm{Prob}_{\mathbf{z}}[\mathbf{z} \in \mathcal{D}'] && (9)
\end{aligned}$$

as desired. □

We omit to mention distribution of b' for simplicity unless confusion is likely to occur.

We next analyze probability of the three conditions (a), (b), (c) in Lemmas 6.12, 6.13 and 6.14.

Lemma 6.12 (Bounding the probability of (a))**.** *Given $\boldsymbol{v}_0, \boldsymbol{v}_0', \boldsymbol{v}_0, \boldsymbol{v}_0', k, k', \mathbf{z}, \boldsymbol{\beta}$ 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. When the event that $\boldsymbol{v}_0' \neq \boldsymbol{v}_0$ happens, it indicates existing a i, $\lfloor z_i \rceil \neq \lfloor z_i + \beta_i \rceil$. 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 6.11, we then derive that

$$\mathrm{Prob}_{\mathbf{x}}[\lfloor z_i \rceil = \lfloor z_i + \beta_i \rceil] \geq \frac{\left| \left[-1/2 + \frac{2^r}{q^{3/4}}, 1/2 - \frac{2^r}{q^{3/4}}\right) \cap \frac{2^r}{2q}\mathbb{Z}_{2q} \right|}{\left| [-1/2, 1/2) \cap \frac{2^r}{2q}\mathbb{Z}_{2q} \right|} \tag{10}$$

$$\geq \frac{\left| \left[\frac{2q}{2^r}(-1/2 + \frac{2^r}{q^{3/4}}), \frac{2q}{2^r}(1/2 - \frac{2^r}{q^{3/4}})\right) \cap \mathbb{Z}_{2q} \right|}{\left| [-\frac{q}{2^r}, \frac{q}{2^r}) \cap \mathbb{Z}_{2q} \right|} \tag{11}$$

$$= \frac{2\lfloor \frac{q}{2^r} - 2q^{1/4} \rfloor + 1}{2\lfloor \frac{q}{2^r} \rfloor + 1} \tag{12}$$

$$\geq \frac{\frac{q}{2^r} - 2q^{1/4} - 1}{\frac{q}{2^r}} \tag{13}$$

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 6.13 (Bounding the probability of (b))**.** *Given $\boldsymbol{v}_0, \boldsymbol{v}_0', \boldsymbol{v}_0, \boldsymbol{v}_0', k, k', \mathbf{z}, \boldsymbol{\beta}$ 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 6.12 by substituting $\mathbf{z}$ with $\mathbf{z} + \mathbf{g}$.

Lemma 6.14 (Bounding the probability of (c))**.** *Given $\boldsymbol{v}_0, \boldsymbol{v}_0', \boldsymbol{v}_0, \boldsymbol{v}_0', k, k', \mathbf{z}, \boldsymbol{\beta}$ as defined above, probability that $k' \neq 1 - k$ (denoted by $\mathrm{Prob}_{\mathbf{x}}[k' \neq 1 - k]$) 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 $\mathrm{Prob}_{\mathbf{x}}[k = 1, k' = 0]$ 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 6.11, $\mathrm{Prob}_{\mathbf{x}}[k = 0, k' = 1]$ 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 $\mathbf{z} \leftarrow_\$ \frac{2^r}{2q}\mathbb{Z}_{2q}^4 \cap [-1/2, 1/2)^4 \mod 2^r$. As $|z_i + \beta_i| \leq |z_i| + |\beta_i|$ by Triangle Inequality, we can upper-bound $\mathrm{Prob}_{\mathbf{x}}[k = 0, k' = 1]$ 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 $\mathbf{z} \leftarrow_\$ \frac{2^r}{2q}\mathbb{Z}_{2q}^4 \cap [-1/2, 1/2)^4 \mod 2^r$. Since $|\beta_0| + |\beta_1| + |\beta_2| + |\beta_3| \leq 4 \cdot \frac{2^r}{q^{3/4}}$, we can further upper-bound $\mathrm{Prob}_{\mathbf{x}}[k = 0, k' = 1]$ 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 $\mathbf{z} \leftarrow_{\$} \frac{2^r}{2q}\mathbb{Z}_{2q}^4 \cap [-1/2, 1/2)^4 \mod 2^r$.

Let $\varDelta = 4 \cdot \frac{2^r}{q^{3/4}}$. 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 $\frac{2^r}{2q}\mathbb{Z}_{2q}^4$ and satisfies the following two conditions:

$$1 - \varDelta < |z_0| + |z_1| + |z_2| + |z_3| < 1 \tag{14}$$
$$-1/2 \ \leq \ z_i < \ 1/2 \text{ , for } i = 0, 1, 2, 3 \tag{15}$$

divided by the cardinality of set where each element is in $\frac{2^r}{2q}\mathbb{Z}_{2q}^4$ and only satisfies the equation (15).

Similarly for *Case 2*, by Lemma 6.11, $\text{Prob}_{\mathbf{x}}[k = 1, k' = 0]$ 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 $\mathbf{z} \leftarrow_{\$} \frac{2^r}{2q}\mathbb{Z}_{2q}^4 \cap [-1/2, 1/2)^4 \mod 2^r$. 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:

$$1 \leq |z_0| + |z_1| + |z_2| + |z_3| < 1 + \varDelta \tag{16}$$
$$-1/2 \ \leq \ z_i < \ 1/2 \text{ , for } i = 0, 1, 2, 3 \tag{17}$$

by the cardinality of set that each element is in $\frac{2^r}{2q}\mathbb{Z}_{2q}^4$ and only satisfies the Equation 17.

Thus, by combining both cases, we have $\text{Prob}_{\mathbf{x}}[k' \neq 1 - k] = \text{Prob}_{\mathbf{x}}[k = 0, k' = 1] + \text{Prob}_{\mathbf{x}}[k = 1, k' = 0]$ 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:

$$1 - \varDelta < |z_0| + |z_1| + |z_2| + |z_3| < 1 + \varDelta \tag{18}$$
$$-1/2 \ \leq \ z_i < \ 1/2 \text{ , for } i = 0, 1, 2, 3 \tag{19}$$

by the cardinality of set where elements are in $\frac{2^r}{2q}\mathbb{Z}_{2q}^4$ and satisfies the the Equation 19.

Note that, disregarding the distribution of $\mathbf{z}$, (19) defines a unit hypercube $[-1/2, 1/2)^4$ centered at origin and (18) defines a hyper-object clipped by two hyperplanes in each octant. We denote by Vol_{cube} the hypercube volume. Let Vol_{clip} be the hypervolume where each points satisfies both (18) and (19), which is equivalent to say, Vol_{clip} is hypervolume of hypercube defined in (19) clipped by two hyperplanes in each octant, as defined in (18).

If $\mathbf{x}$ is sampled from $\mathbb{R}^4$, it is easy to see that probability $\text{Prob}_{\mathbf{x}}[k' \neq 1 - k]$ is upperbounded by the ratio of Vol_{clip} to Vol_{cube}.

For the rest of the proof, we first compute the ratio of Vol_{clip} to Vol_{cube} and then approximate the upperbound of $\text{Prob}_{\mathbf{x}}[k' \neq 1 - k]$ 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 (14) and (15) for adapting Theorem 2.2 where unit hypercube is defined as $[0, 1]^n$. Vol_{clip} and Vol_{cube} is i^{th} octant Let Vol_{clip}^i denote Vol_{clip} in the i^{th} octant, and Vol_{cube}^i denote Vol_{cube} in i^{th} octant. Thus, in the i^{th} octant, we have

$$2 - 2\varDelta < t_0 + t_1 + t_2 + t_3 < 2 + 2\varDelta \tag{20}$$
$$0 \leq t_i < 1, \text{ for } i = 0, 1, 2, 3, \tag{21}$$

where $t_i = 2z_i$.

Define two hyperspace as follows:

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

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

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 $\mathit{\Delta}$ with $4q^{1/4} \cdot \frac{2^r}{q}$, we obtain

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

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^{th} octant, such that if $\mathbf{z}$ satisfies the conditions (18) and (19), then $\mathbf{z}'$ satisfies the conditions (18) and (19), and if $\mathbf{z}$ satisfies the condition (19) but not satisfies (18), then $\mathbf{z}'$ satisfies the condition (19) but not satisfies (18). 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 ε, we begin by carving a hypercube $[\frac{1}{4} - \frac{1}{4}\mathit{\Delta}, \frac{1}{4} + \frac{1}{4}\mathit{\Delta}]^4$, which is contained in 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 $\frac{2^r}{2q} \cdot 2 \leq \varepsilon \cdot \frac{1}{2}\mathit{\Delta}$, we can guarantee that $\mathcal{P}(B) \cup -\mathcal{P}(B) \subseteq \varepsilon \cdot \mathrm{Vol}^1_{clip}$. Similarly, since 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 6.12, 6.13 and 6.14, 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 6.15. *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 $\hat{\mathbf{s}}, \hat{\mathbf{s}}', \hat{\mathbf{e}}, \hat{\mathbf{e}}', \hat{\mathbf{e}}''$, is indistinguishable from a distribution that has min-entropy $n/8 + n/8 \cdot (-\log_2(1/2 + p)) - k$.*

6.3 Instantiating the Parameters

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

$$\begin{aligned} p :=& 2 - 2\left(\frac{\frac{q}{2^r} - 2q^{1/4} - 1}{\frac{q}{2^r}}\right)^4 + \left(\frac{1 + \frac{1}{2q^{1/4}}}{1 - \frac{2^{r+1}}{q}}\right)^4 \cdot \left(\frac{2^{4r+10}}{q^3} - \frac{2^{3r+10}}{3q^{9/4}} + \frac{2^{r+5}}{3q^{3/4}}\right) && (22) \\ \approx& 0.10092952876519123 && (23) \end{aligned}$$

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 $128 + 128 \cdot (-\log_2(1/2 + 0.10092952876519123/2)) \approx 238$. 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 158.

6.4 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 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: 25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016. (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., Chang, Y.A., Cheng, C.M., Chou, L.P., Heninger, N., Lange, T., van Someren, N.: Factoring RSA keys from certified smart cards: Coppersmith in the wild. In Sako, K., Sarkar, P., eds.: ASIACRYPT 2013, Part II. Volume 8270 of LNCS., Springer, Heidelberg (December 2013) 341–360
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. 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
10. 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 16, ACM Press (October 2016) 1006–1018
11. 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
12. Boyle, E., Segev, G., Wichs, D.: Fully leakage-resilient signatures. Journal of Cryptology **26**(3) (July 2013) 513–558
13. Braithwaite, M.: Experimenting with post-quantum cryptography. https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html Accessed: 2018-10-09.
14. 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
15. Brakerski, Z., Perlman, R.: Order-LWE and the hardness of ring-LWE with entropic secrets. Cryptology ePrint Archive, Report 2018/494 (2018) https://eprint.iacr.org/2018/494.
16. 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
17. 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
18. 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.
19. Dadush, D., Regev, O.: Lecture note of fundamental domains, lattice density, and minkowski theorems (2018)
20. Ding, J.: A simple provably secure key exchange scheme based on the learning with errors problem. IACR Cryptology ePrint Archive **2012** (2012) 688
21. 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
22. 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
23. 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
24. 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
25. Dziembowski, S., Pietrzak, K.: Leakage-resilient cryptography. In: 49th FOCS, IEEE Computer Society Press (October 2008) 293–302
26. 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
27. 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
28. 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
29. 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
30. Lyubashevsky, V.: Search to decision reduction for the learning with errors over rings problem. In: 2011 IEEE Information Theory Workshop, ITW 2011, Paraty, Brazil, October 16-20, 2011. (2011) 410–414
31. Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. In Gilbert, H., ed.: EUROCRYPT 2010. Volume 6110 of LNCS., Springer, Heidelberg (May / June 2010) 1–23

32. 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
33. 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.
34. 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
35. Marichal, J.L., Mossinghoff, M.J.: Slices, slabs, and sections of the unit hypercube. arXiv preprint math/0607715 (2006)
36. Nemec, M., Sýs, M., Svenda, P., Klinec, D., Matyas, V.: The return of coppersmith's attack: Practical factorization of widely used RSA moduli. In Thuraisingham, B.M., Evans, D., Malkin, T., Xu, D., eds.: ACM CCS 17, ACM Press (October / November 2017) 1631–1648
37. 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
38. 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
39. Pietrzak, K.: A leakage-resilient mode of operation. In Joux, A., ed.: EUROCRYPT 2009. Volume 5479 of LNCS., Springer, Heidelberg (April 2009) 462–482
40. 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
41. 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
42. 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