

On the Non-Existence of Short Vectors in Random Module Lattices

Ngoc Khanh Nguyen^{1,2}

¹ IBM Research – Zurich, Switzerland

² Ruhr Universität Bochum, Germany
nkn@zurich.ibm.com

Abstract. Recently, Lyubashevsky & Seiler (Eurocrypt 2018) showed that small polynomials in the cyclotomic ring $\mathbb{Z}_q[X]/(X^n + 1)$, where n is a power of two, are invertible under special congruence conditions on prime modulus q . This result has been used to prove certain security properties of lattice-based constructions against unbounded adversaries. Unfortunately, due to the special conditions, working over the corresponding cyclotomic ring does not allow for efficient use of the Number Theoretic Transform (NTT) algorithm for fast multiplication of polynomials and hence, the schemes become less practical.

In this paper, we present how to overcome this limitation by analysing zeroes in the Chinese Remainder (or NTT) representation of small polynomials. As a result, we provide upper bounds on the probabilities related to the (non)-existence of a short vector in a random module lattice with no assumptions on the prime modulus. We apply our results, along with the generic framework by Kiltz et al. (Eurocrypt 2018), to a number of lattice-based Fiat-Shamir signatures so they can both enjoy tight security in the quantum random oracle model and support fast multiplication algorithms (at the cost of slightly larger public keys and signatures), such as the Bai-Galbraith signature scheme (CT-RSA 2014), Dilithium-QROM (Kiltz et al., Eurocrypt 2018) and qTESLA (Alkim et al., PQCrypto 2017). Our techniques can also be applied to prove that recent commitment schemes by Baum et al. (SCN 2018) are statistically binding with no additional assumptions on q .

Keywords: Lattice-based cryptography, Fiat-Shamir signatures, module lattices, lossy identification schemes, provable security.

1 Introduction

Cryptography based on the hardness of lattice problems, such as Module-SIS or Module-LWE [21, 16, 18], seems to be a very likely replacement for traditional cryptography after the eventual arrival of quantum computers. With the ongoing NIST PQC Standardization Process, we are closer to using quantum-resistant encryption schemes and digital signatures in real life. For additional efficiency, many practical lattice-based constructions work over *fully-splitting* polynomial

rings $R_q := \mathbb{Z}_q[X]/(f(X))$ where $f(X) = X^n + 1$ is a cyclotomic polynomial, n is a power of two and the prime q is selected so that $f(X)$ splits completely into n linear factors modulo q . With such a choice of parameters, multiplication in the polynomial ring can be performed very quickly using the Number Theoretic Transform (NTT), e.g. [10, 3, 24, 15]. Indeed, one obtains a speed-up of about a factor of 5 by working over rings where $X^n + 1$ splits completely versus just 2 factors (for primes of size between 2^{20} and 2^{29} [19]). Moreover, the structure of fully-splitting rings allows us to perform various operations in parallel as well as conveniently cache and sample polynomials which also significantly improves efficiency of the schemes.

Unfortunately, it is sometimes difficult to prove security of lattice-based constructions when working over fully-splitting polynomial rings [11, 8, 5]. Usually, the reason is that these security proofs rely on the assumption that polynomials of small norm are invertible. Recently, Lyubashevsky and Seiler [19] (generalising [17]) showed that when n is a power of two and under certain conditions on prime modulus q , small elements of R_q are indeed invertible. The result, however, is meaningful only when $X^n + 1$ does not split into many factors modulo q (e.g. at most 32 for $n = 512$). Consequently, we cannot apply the standard NTT algorithm in such polynomial rings unless we drop the invertibility assumption³.

In this paper, we present techniques to avoid the invertibility assumption in security proofs. This allows us to construct lattice-based primitives without any conditions on prime modulus q and consequently, we can work over fully-splitting rings and at the same time, use the NTT algorithm for fast multiplication of polynomials. We apply our results to the second-round candidates of the NIST PQC Standardization Process. Namely, we improve the efficiency of Dilithium-QROM [11] (which is the modified version of Dilithium [15] secure in the quantum random oracle model) as well as qTESLA [8]. We also briefly explain how our techniques can be applied to recent lattice-based commitment schemes [5].

1.1 Our Contribution

MAIN RESULTS. Our main technical result is an upper bound on the probability of existence of a short vector in a random module lattice (see Theorem 1.1, formally Corollary 3.9) and other related probabilities (Theorem 3.8 and Theorem 3.10). Informally, it states that the probability, over the uniformly random matrix \mathbf{A} , that there exists a pair of vectors $(\mathbf{z}_1, \mathbf{z}_2)$, which consists of small polynomials in R_q and $\mathbf{z}_1 \neq \mathbf{0}$, such that $\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = \mathbf{0}$ is small (for a suitable choice of parameters). In the context of Fiat-Shamir identification and signature schemes, \mathbf{A} represents a public key matrix and \mathbf{z}_1 (and sometimes \mathbf{z}_2 as well) represents a difference of two signatures/responses. Our upper bound depends on the tail function \mathcal{T} . For readability, we hide the concrete formula for \mathcal{T} here and we refer to the formal statement in Corollary 3.9.

³ Lyubashevsky and Seiler [19] showed, however, how to combine the FFT algorithm and Karatsuba multiplication in order to multiply in partially-splitting rings faster.

We recall that a similar result was presented by Kiltz et al. (e.g. Lemma 4.6 in [11]) but they only consider the case when $q \equiv 5 \pmod{8}$ so that invertibility properties can be applied [17, 19]. Here, we generalise their result on how to bound that probability without any assumptions on the prime modulus q .

Theorem 1.1 (Informal). *Denote $S_\alpha := \{y \in R_q : \|y\|_\infty \leq \alpha\}$ and let $\ell, k, \alpha_1, \alpha_2 \in \mathbb{N}$. Then*

$$\Pr_{\mathbf{A} \leftarrow R_q^{k \times \ell}} [\exists (\mathbf{z}_1, \mathbf{z}_2) \in S_{\alpha_1}^\ell \setminus \{\mathbf{0}\} \times S_{\alpha_2}^k : \mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = \mathbf{0}] \leq \frac{|S_{\alpha_1}|^\ell \cdot |S_{\alpha_2}|^k}{q^{nk}} + \mathcal{T}(q, \ell, k, \alpha_1, \alpha_2), \quad (1)$$

where $\mathcal{T}(q, \ell, k, \alpha_1, \alpha_2)$ is a function defined in Corollary 3.9.

Figure 1 shows values of the tail function \mathcal{T} for different prime moduli q . We observe that the more $f(x) = X^n + 1$ splits modulo q then the larger the value of \mathcal{T} . When $f(x)$ only splits into two factors, our upper bound is essentially equal to

$$\frac{|S_{\alpha_1}|^\ell \cdot |S_{\alpha_2}|^k}{q^{nk}}.$$

Indeed, in this case the value of \mathcal{T} is negligible and hence, we obtain an upper bound identical to Kiltz et al. On the other hand, if we want to work over fully-splitting polynomial rings in order to apply the Number Theoretic Transform algorithm, we would have to increase q as well as the dimensions (k, ℓ) of the matrix \mathbf{A} so that $\mathcal{T}(q, \ell, k, \alpha_1, \alpha_2)$ stays small. Unfortunately, this implies larger public key and signature size.

KEY TECHNIQUES. We provide an overview of the proof of Theorem 1.1. Let d be the divisor of n such that

$$X^n + 1 \equiv \prod_{i=1}^d f_i(X) \pmod{q}$$

for distinct polynomials $f_i(X)$ of degree n/d that are irreducible in $\mathbb{Z}_q[X]$. In other words, $X^n + 1$ splits into d irreducible polynomials modulo q . The proof sketch goes as follows.

Step 1: We apply the union bound:

$$\begin{aligned} \Pr_{\mathbf{A} \leftarrow R_q^{k \times \ell}} [\exists (\mathbf{z}_1, \mathbf{z}_2) \in S_{\alpha_1}^\ell \setminus \{\mathbf{0}\} \times S_{\alpha_2}^k : \mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = \mathbf{0}] \\ \leq \sum_{(\mathbf{z}_1, \mathbf{z}_2) \in S_{\alpha_1}^\ell \setminus \{\mathbf{0}\} \times S_{\alpha_2}^k} \Pr_{\mathbf{A} \leftarrow R_q^{k \times \ell}} [\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = \mathbf{0}]. \end{aligned} \quad (2)$$

Step 2: We identify the subset Z of $S_{\alpha_1}^\ell \setminus \{\mathbf{0}\} \times S_{\alpha_2}^k$ which satisfies:

$$(\mathbf{z}_1, \mathbf{z}_2) \in Z \iff \Pr_{\mathbf{A} \leftarrow R_q^{k \times \ell}} [\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = \mathbf{0}] > 0.$$

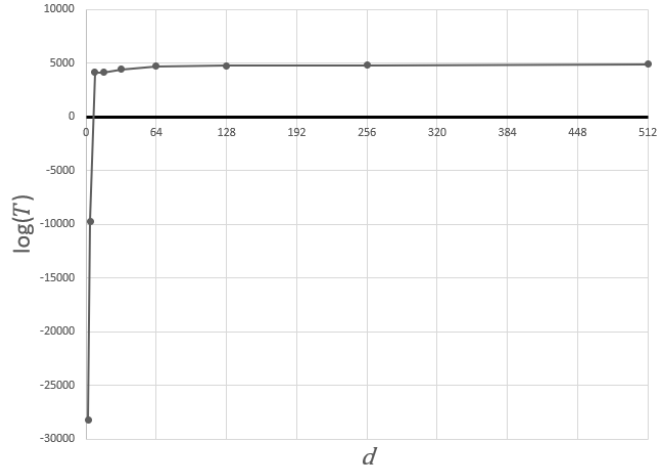


Fig. 1. Let $(n, q, \ell, k, \alpha_1, \alpha_2) = (512, \approx 2^{45}, 4, 4, 1.8 \cdot 10^6, 3.6 \cdot 10^6)$. The graph presents values of $\log(\mathcal{T}(q, \ell, k, \alpha_1, \alpha_2))$ depending on the number of irreducible polynomials d that $X^n + 1$ splits into modulo q . One notes that for prime moduli $q \approx 2^{45}$ such that $d \in \{2, 4\}$, the value of \mathcal{T} is sufficiently small, hence so is the right-hand side of Equation (1). On the other hand, values of \mathcal{T} rocket for $d \geq 8$ and therefore q or dimensions (k, ℓ) of the matrix \mathbf{A} must be increased in order to keep the upper bound in (1) small enough.

Hence, the probability in Equation (1) can be bounded by

$$\sum_{(\mathbf{z}_1, \mathbf{z}_2) \in Z} \Pr_{\mathbf{A} \leftarrow R_q^{k \times \ell}} [\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = \mathbf{0}].$$

Step 3: Next, we propose a partitioning of the set Z into subsets Z_0, Z_1, \dots, Z_d , i.e. $Z = \bigcup_{i=0}^d Z_i$. Then, we show that for each $(\mathbf{z}_1, \mathbf{z}_2) \in Z_i$, the probability

$$p_i := \Pr_{\mathbf{A} \leftarrow R_q^{k \times \ell}} [\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = \mathbf{0}]$$

is the same and we compute it. Thus, the probability in Equation (1) can now be bounded by:

$$\sum_{i=0}^d \sum_{(\mathbf{z}_1, \mathbf{z}_2) \in Z_i} p_i = \sum_{i=1}^d |Z_i| \cdot p_i$$

Step 4: We find an upper bound on $|Z_i|$.

ZERO FUNCTION. In this paper, we will consider zeroes in the “Chinese Remainder representation”⁴ of polynomials in R_q ⁵. Formally, we define the following **Zero**

⁴ Alternatively, we call it “FFT/NTT representation” in the fully-splitting case.

⁵ This technique has already been investigated in the literature for e.g. constructing provably secure variants of NTRUEncrypt [25].

function:

$$\text{Zero}(y) := \{i : y \equiv 0 \pmod{(f_i(X), q)}\} \text{ and } \text{Zero}(\mathbf{y}) := \bigcap_{j=1}^k \text{Zero}(y_j),$$

where $y \in R_q$ and $\mathbf{y} = (y_1, \dots, y_k) \in R_q^k$. Note that if y is invertible then $|\text{Zero}(y)| = 0$. Lyubashevsky and Seiler [19] proved that whenever a non-zero y has small Euclidean norm then $|\text{Zero}(y)| = 0$. Here, we extend it and provide a relationship between the Euclidean norm of y and the size of set $\text{Zero}(y)$ (see Lemma 3.2). In particular, the result implies that relatively small elements of R_q have only a few zeroes in the Chinese Remainder representation. This observation will be crucial for Steps 3 and 4.

ZERO ROWS. Consider the equation $\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = \mathbf{0}$ and let $j \in \text{Zero}(\mathbf{z}_1)$. If we look at this equation modulo $(f_j(X), q)$ then we just end up with $\mathbf{z}_2 = \mathbf{0}$, i.e. $j \in \text{Zero}(\mathbf{z}_2)$ and thus $j \in \text{Zero}(\mathbf{z}_1 \parallel \mathbf{z}_2)$ where \parallel denotes usual concatenation of vectors. Consequently, $\text{Zero}(\mathbf{z}_1) \subseteq \text{Zero}(\mathbf{z}_1 \parallel \mathbf{z}_2)$. Clearly, we have $\text{Zero}(\mathbf{z}_1 \parallel \mathbf{z}_2) \subseteq \text{Zero}(\mathbf{z}_1)$ and therefore these two sets are equal. This implies that the subset Z introduced in Step 2 can be identified as:

$$Z = \{(\mathbf{z}_1, \mathbf{z}_2) : \text{Zero}(\mathbf{z}_1) = \text{Zero}(\mathbf{z}_1 \parallel \mathbf{z}_2)\}.$$

Define $Z_i = \{(\mathbf{z}_1, \mathbf{z}_2) : \text{Zero}(\mathbf{z}_1) = \text{Zero}(\mathbf{z}_1 \parallel \mathbf{z}_2) \wedge |\text{Zero}(\mathbf{z}_1)| = i\} \subseteq Z$ (Step 3). Informally, we say that $(\mathbf{z}_1, \mathbf{z}_2) \in Z_i$ has i zero rows, since if we write down the components of \mathbf{z}_1 and \mathbf{z}_2 in the Chinese Remainder representation, in columns, then we get exactly i rows filled with zeroes.

For fixed $(\mathbf{z}_1, \mathbf{z}_2) \in Z_i$, we compute the probability p_i defined in Step 3 by counting the number of possible \mathbf{A} which satisfy $\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = \mathbf{0}$. This could be done by considering the equation modulo $(f_j(X), q)$ for all $j \notin \text{Zero}(\mathbf{z}_1)$. Indeed, for such j there is a simple way to count all $\mathbf{A} \in (\mathbb{Z}_q[X]/(f_j(x)))^{k \times \ell}$ which satisfy $\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = \mathbf{0}$ modulo $f_j(X)$. Concretely, one of the components of \mathbf{z}_1 , say z_u , is going to be invertible modulo $f_j(X)$ and therefore all entries of \mathbf{A} not related to z_u can be chosen arbitrarily. The rest, however, will be adjusted so that the equation holds. On the other hand, if $j \in \text{Zero}(\mathbf{z}_1) = \text{Zero}(\mathbf{z}_1 \parallel \mathbf{z}_2)$ then $\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2$ is simply equal to $\mathbf{0}$ modulo $(f_j(X), q)$ for any \mathbf{A} . By applying Chinese Remainder Theorem, we obtain the total number of possible $\mathbf{A} \in R_q^{k \times \ell}$ which satisfy the equation above.

The only thing left is to provide an upper bound on $|Z_i|$ (Step 4). Firstly, we observe that if $(\mathbf{z}_1, \mathbf{z}_2) \in Z_i$ then clearly $|\text{Zero}(z_j)| \geq i$ for $j = 1, \dots, \ell$ where $\mathbf{z}_1 = (z_1, \dots, z_\ell)$. Since each component of $\mathbf{z}_1 \in S_{\alpha_1}^\ell \setminus \{\mathbf{0}\}$ has infinity norm at most α_1 , and assuming this value is relatively small, we get that each component of \mathbf{z}_1 has only a few zeroes in the Chinese Remainder representation (Lemma 3.2). Hence, for some larger values of i , we simply get $Z_i = \emptyset$. The second observation is that if $(\mathbf{z}_1, \mathbf{z}_2) \in Z_i$ and $\mathbf{y}_1, \mathbf{y}_2$ are vectors of some ‘‘small’’ polynomials then $(\mathbf{z}_1 + \mathbf{y}_1, \mathbf{z}_2 + \mathbf{y}_2)$ is likely not to have exactly i zero rows. For example, suppose that

$$\text{Zero}(\mathbf{z}_1 + \mathbf{y}_1, \mathbf{z}_2 + \mathbf{y}_2) = \text{Zero}(\mathbf{z}_1 + \mathbf{y}'_1, \mathbf{z}_2 + \mathbf{y}'_2)$$

for some other small $\mathbf{y}'_1, \mathbf{y}'_2$. This implies that $(\mathbf{y}_1 - \mathbf{y}'_1, \mathbf{y}_2 - \mathbf{y}'_2)$ has at least i zero rows. In particular, each component of $\mathbf{y}_1 - \mathbf{y}'_1$, say \hat{y}_j , has at least i zeroes in the Chinese Remainder representation. However, we know that \hat{y}_j is a polynomial of small norm by the choice of \mathbf{y}_1 and \mathbf{y}'_1 . Therefore, \hat{y}_j has only a few zeroes (by the observation above or Lemma 3.2). By picking sufficiently small \mathbf{y}_1 and \mathbf{y}'_1 we can make sure that each component \hat{y}_j of $\mathbf{y}_1 - \mathbf{y}'_1$ has less than i zeroes. This would lead to a contradiction. In conclusion, our approach for bounding $|Z_i|$ is to, for each $(\mathbf{z}_1, \mathbf{z}_2) \in Z_i$, generate all pairs of form $(\mathbf{z}_1 + \mathbf{y}_1, \mathbf{z}_2 + \mathbf{y}_2) \notin Z_i$, for vectors of sufficiently small polynomials $\mathbf{y}_1, \mathbf{y}_2$, and applying the pigeonhole principle along with other simple counting arguments.

1.2 Applications

DIGITAL SIGNATURES. Kiltz et al. [11] presented a generic framework for constructing secure Fiat-Shamir signatures in the quantum random oracle model (QROM). As a concrete instantiation, they introduced a new signature scheme Dilithium-QROM, which is a modification of the original Dilithium scheme [15], and is tightly based on the hardness of Module-LWE problem in the QROM. However, in order to obtain security of Dilithium-QROM, Kiltz et al. choose the prime modulus q to be congruent to 5 modulo 8. This assumption assures that the underlying polynomial ring $\mathbb{Z}_q[X]/(X^n + 1)$ splits into two subrings modulo q and invertibility results can be applied [17, 19]. Unfortunately, polynomial multiplication algorithms in such rings are not efficient. We show how to apply our probability results to the security of Dilithium-QROM⁶ so that one can avoid such special assumptions on q (in particular, one could choose q so that R_q splits completely and NTT along with other optimisations can be applied). The only disadvantage is that, in order to keep the probabilities small, one should slightly increase the size of q and dimensions (k, ℓ) . Unfortunately, this results in having both considerably larger public keys and signatures.

General results by Kiltz et al. can also be applied to obtain a security proof in the QROM for a number of existing Fiat-Shamir signature schemes similar to Dilithium such as the Bai-Galbraith scheme [4] (see Section 4) or qTESLA [8]. So far, security of the latter scheme in the quantum random oracle model is proven assuming a certain non-standard conjecture. However, one can also obtain it by applying the framework by Kiltz et al. and using our probability upper bounds. Consequently, one gets a tightly secure version of qTESLA in the QROM without any non-standard conjecture. We recall that our results allow this signature scheme to work over fully-splitting rings so that the use of NTT for polynomial multiplication is possible. However, as in the case of Dilithium-QROM, we would end up with larger public key and signature size compared to the original qTESLA (see Table 2).

COMMITMENT SCHEMES. Recently, Baum et al. [5] presented efficient commitment schemes from Module-SIS and Module-LWE. However, both their new statistically

⁶ We present it in the full version of this paper [20].

binding commitment scheme and their improved construction from [7] rely on the general invertibility result from [19], i.e. special congruence conditions on the prime modulus q . Our probability upper bounds can be applied to prove the statistically binding property of these constructions, and consequently, one could now consider working in fully-splitting rings. As before, we observe that choosing primes q such that $X^n + 1$ splits into many factors modulo q results in having both larger commitment and proof size.

1.3 Related Works

The first asymptotically-efficient lattice-based signature scheme using the “Fiat-Shamir with Aborts” paradigm was presented in [13] which is based on the Ring-SIS problem. Later on, Lyubashevsky [14] improved the scheme by basing it on the combination of Ring-SIS and Ring-LWE. Since then, many substantial improvements have been proposed [10, 4, 15, 8]. In the meantime, lossy identification schemes were introduced and used to construct secure digital signatures in the quantum random oracle model [1, 27, 2, 11].

Invertibility of “small” polynomials⁷ is an important property in the context of (approximate) zero-knowledge proofs based on lattices. For example, one usually needs the difference set $\mathcal{C} - \mathcal{C}$ to contain only invertible polynomials for extraction purposes [26, 7] where \mathcal{C} is a challenge set. Lyubashevsky and Neven [17] proved that if q is congruent to 5 modulo 8 then the polynomial ring $R_q = \mathbb{Z}_q[X]/(X^n + 1)$ splits into two subrings and elements of small infinity norm are indeed invertible. This result was generalised by Lyubashevsky and Seiler [19]. Concretely, they showed that if $q \equiv 2k + 1 \pmod{4k}$ for some k then $X^n + 1$ splits into k irreducible polynomials modulo q and also small elements in R_q are invertible. These results have been recently applied in the context of computing probabilities related to the security of lattice-based signatures and commitment schemes, e.g. [11, 5].

2 Preliminaries

For $n \in \mathbb{N}$, let $[n] := \{1, \dots, n\}$. For a set S , $|S|$ is the cardinality of S , $\mathcal{P}(S)$ is the power set of S and $\mathcal{P}_i(S)$ is the set of all subsets of S of size i . If S is finite, we denote the sampling of a uniform random element x by $x \leftarrow S$, while we denote the sampling according to some distribution \mathfrak{D} by $x \leftarrow \mathfrak{D}$. By $\llbracket B \rrbracket$ we denote the bit that is 1 if the Boolean statement B is true, and 0 otherwise.

ALGORITHMS. Unless stated otherwise, we assume all our algorithms to be probabilistic. We denote by $y \leftarrow \mathbf{A}(x)$ the probabilistic computation of algorithm \mathbf{A} on input x . If \mathbf{A} is deterministic, we write $y := \mathbf{A}(x)$. The notation $y \in \mathbf{A}(x)$ is used to indicate all possible outcomes y of the probabilistic algorithm \mathbf{A} on input x . We can make any probabilistic \mathbf{A} deterministic by running it with fixed

⁷ What we mean by “small” is that the polynomial has small infinity or Euclidean norm.

randomness. We write $y := \mathbf{A}(x; r)$ to indicate that \mathbf{A} is run on input x with randomness r . The notation $\mathbf{A}(x) \Rightarrow y$ denotes the event that \mathbf{A} on input x returns y . Eventually, we write $\text{Time}(\mathbf{A})$ to denote the running time of \mathbf{A} .

2.1 Cyclotomic Rings

Let n be a power of two. Denote R and R_q respectively to be the rings $\mathbb{Z}[X]/(X^n + 1)$ and $\mathbb{Z}_q[X]/(X^n + 1)$, for a prime q . We also set d to be the divisor of n such that

$$X^n + 1 \equiv \prod_{i=1}^d f_i(X) \pmod{q}$$

for distinct polynomials $f_i(X)$ of degree n/d that are irreducible in $\mathbb{Z}_q[X]$. Alternatively, we say that $X^n + 1$ splits into d polynomials modulo q . If $d = n$ then $X^n + 1$ *fully splits*. By default, all the equalities and congruences between ring elements in this paper are modulo q .

Regular font letters denote elements in R or R_q and bold lower-case letters represent column vectors with coefficients in R or R_q . Bold upper-case letters denote matrices. By default, all vectors are column vectors.

MODULAR REDUCTIONS. For an even (resp. odd) positive integer α , we define $r' = r \bmod^\pm \alpha$ to be the unique element r' in the range $-\frac{\alpha}{2} < r' \leq \frac{\alpha}{2}$ (resp. $-\frac{\alpha-1}{2} \leq r' \leq \frac{\alpha-1}{2}$) such that $r' = r \bmod \alpha$. For any positive integer α , we define $r' = r \bmod^+ \alpha$ to be the unique element r' in the range $0 \leq r' < \alpha$ such that $r' = r \bmod \alpha$. When the exact representation is not important, we simply write $r \bmod \alpha$.

SIZES OF ELEMENTS. For an element $w \in \mathbb{Z}_q$, we write $\|w\|_\infty$ to mean $|w \bmod^\pm q|$. Define the ℓ_∞ and ℓ_2 norms for $w = w_0 + w_1X + \dots + w_{n-1}X^{n-1} \in R$ as follows:

$$\|w\|_\infty = \max_i \|w_i\|_\infty, \quad \|w\| = \sqrt{\|w_0\|_\infty^2 + \dots + \|w_{n-1}\|_\infty^2}.$$

Similarly, for $\mathbf{w} = (w_1, \dots, w_k) \in R^k$, we define

$$\|\mathbf{w}\|_\infty = \max_i \|w_i\|_\infty, \quad \|\mathbf{w}\| = \sqrt{\|w_1\|^2 + \dots + \|w_k\|^2}.$$

For a finite set $S \subseteq R^k$, however, we set

$$\|S\|_\infty = \max_{\mathbf{w} \in S} \|\mathbf{w}\|_\infty, \quad \|S\| = \max_{\mathbf{w} \in S} \|\mathbf{w}\|.$$

We write S_η to denote all elements $w \in R$ such that $\|w\|_\infty \leq \eta$.

EXTRACTING HIGH-ORDER AND LOW-ORDER BITS. To reduce the size of the public key, we need some algorithms that extract “higher-order” and “lower-order” bits of elements in \mathbb{Z}_q . The goal is that when given an arbitrary element $r \in \mathbb{Z}_q$ and another small element $z \in \mathbb{Z}_q$, we would like to be able to recover the higher order bits of $r + z$ without needing to store z . The algorithms are exactly as in [9, 11], and we repeat them for completeness in Figure 2. They are described as working on integers modulo q , but one can extend it to polynomials in R_q by simply being applied individually to each coefficient.

<u>Power2Round_q(r, δ)</u>	<u>Decompose_q(r, α)</u>
01 $r := r \bmod^+ q$	12 $r := r \bmod^+ q$
02 $r_0 := r \bmod^\pm 2^\delta$	13 $r_0 := r \bmod^\pm \alpha$
03 return $(r - r_0)/2^\delta$	14 if $r - r_0 = q - 1$
	15 then $r_1 := 0; r_0 := r_0 - 1$
<u>UseHint_q(h, r, α)</u>	16 else $r_1 := (r - r_0)/\alpha$
04 $m := (q - 1)/\alpha$	17 return (r_1, r_0)
05 $(r_1, r_0) := \text{Decompose}_q(r, \alpha)$	
06 if $h = 1$ and $r_0 > 0$ return $(r_1 + 1) \bmod^+ m$	<u>HighBits_q(r, α)</u>
07 if $h = 1$ and $r_0 \leq 0$ return $(r_1 - 1) \bmod^+ m$	18 $(r_1, r_0) := \text{Decompose}_q(r, \alpha)$
08 return r_1	19 return r_1
<u>MakeHint_q(z, r, α)</u>	<u>LowBits_q(r, α)</u>
09 $r_1 := \text{HighBits}_q(r, \alpha)$	20 $(r_1, r_0) := \text{Decompose}_q(r, \alpha)$
10 $v_1 := \text{HighBits}_q(r + z, \alpha)$	21 return r_0
11 return $\llbracket r_1 \neq v_1 \rrbracket$	

Fig. 2. Supporting algorithms for Dilithium and Dilithium-QROM [11].

Lemma 2.1. *Suppose that q and α are positive integers satisfying $q > 2\alpha$, $q \equiv 1 \pmod{\alpha}$ and α even. Let \mathbf{r} and \mathbf{z} be vectors of elements in R_q where $\|\mathbf{z}\|_\infty \leq \alpha/2$, and let \mathbf{h}, \mathbf{h}' be vectors of bits. Then the HighBits_q , MakeHint_q , and UseHint_q algorithms satisfy the following properties:*

1. $\text{UseHint}_q(\text{MakeHint}_q(\mathbf{z}, \mathbf{r}, \alpha), \mathbf{r}, \alpha) = \text{HighBits}_q(\mathbf{r} + \mathbf{z}, \alpha)$.
2. Let $\mathbf{v}_1 = \text{UseHint}_q(\mathbf{h}, \mathbf{r}, \alpha)$. Then $\|\mathbf{r} - \mathbf{v}_1 \cdot \alpha\|_\infty \leq \alpha + 1$.
3. For any \mathbf{h}, \mathbf{h}' , if $\text{UseHint}_q(\mathbf{h}, \mathbf{r}, \alpha) = \text{UseHint}_q(\mathbf{h}', \mathbf{r}, \alpha)$, then $\mathbf{h} = \mathbf{h}'$.

Lemma 2.2. *If $\|\mathbf{s}\|_\infty \leq \beta$ and $\|\text{LowBits}_q(\mathbf{r}, \alpha)\|_\infty < \alpha/2 - \beta$, then*

$$\text{HighBits}_q(\mathbf{r}, \alpha) = \text{HighBits}_q(\mathbf{r} + \mathbf{s}, \alpha).$$

IDEAL LATTICES. An integer lattice of dimension n is an additive subgroup of \mathbb{Z}^n . For simplicity, we only consider full-rank lattices. The determinant of a full-rank lattice Λ of dimension n is equal to the size of the quotient group \mathbb{Z}^n/Λ . We denote $\lambda_1(\Lambda) = \min_{\mathbf{w} \in \Lambda} \|\mathbf{w}\|$. We say that Λ is an *ideal lattice* in R if Λ is an ideal of R . There exists a lower bound on $\lambda_1(\Lambda)$ if Λ is an ideal lattice [19, 22]. Assuming that n is a power of two, we get a simplified bound.

Lemma 2.3 ([19], **Lemma 2.7**). *If Λ is an ideal lattice in R , then $\lambda_1(\Lambda) \geq \det(\Lambda)^{1/n}$.*

THE MLWE ASSUMPTION. For integers m, k , and a probability distribution $D : R_q \rightarrow [0, 1]$, we say that the advantage of algorithm A in solving the decisional $\text{MLWE}_{m,k,D}$ problem over the ring R_q is

$$\begin{aligned} \text{Adv}_{m,k,D}^{\text{MLWE}} := & \left| \Pr[A(\mathbf{A}, \mathbf{t}) \Rightarrow 1 \mid \mathbf{A} \leftarrow R_q^{m \times k}; \mathbf{t} \leftarrow R_q^m] \right. \\ & \left. - \Pr[A(\mathbf{A}, \mathbf{A}\mathbf{s}_1 + \mathbf{s}_2) \Rightarrow 1 \mid \mathbf{A} \leftarrow R_q^{m \times k}; \mathbf{s}_1 \leftarrow D^k; \mathbf{s}_2 \leftarrow D^m] \right|. \end{aligned}$$

The MLWE assumption states that the above advantage is negligible for all polynomial-time algorithms \mathbf{A} . It was introduced in [12], and is a generalization of the LWE assumption from [23]. The Ring-LWE assumption [18] is a special case of MLWE where $k = 1$. Analogously to LWE and Ring-LWE, it was shown in [12] that solving the MLWE problem for certain parameters is as hard as solving certain worst-case problems in certain algebraic lattices.

3 Zeroes in the Chinese Remainder Representation

In this section, we present general results about existence of solutions $(\mathbf{A}, \mathbf{t}) \in R_q^{k \times \ell} \times R^k$ to the equation $\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = \mathbf{c}\mathbf{t}$ (and other similar ones), for some $\mathbf{z}_1 \in R_q^\ell, \mathbf{z}_2 \in R^k, c \in R_q \setminus \{0\}$, and compute the probability of satisfying such equations for uniformly random \mathbf{A} and \mathbf{t} . The results are crucial for security analysis of Fiat-Shamir signature schemes. For instance, security of Dilithium-QROM [11] relies heavily on the assumption that c is invertible in R_q or \mathbf{z}_1 contains an invertible component. In such a case, the probability can be calculated straightforwardly. Hence, q is chosen so that $q \equiv 5 \pmod{8}$ because then, polynomials in R_q of small (infinity) norm are proved to be invertible [19, 17]. We avoid such assumptions and analyse “zeroes in the Chinese Remainder Representation” of $\mathbf{z}_1, \mathbf{z}_2$ and c in order to provide general upper bounds on the probabilities.

3.1 Zero Rows

We start by introducing the Zero function.

Definition 3.1. *Let $y \in R_q$. We define a set*

$$\text{Zero}(y) := \{i \in [d] : y \equiv 0 \pmod{f_i(X)}\}.$$

For a vector $\mathbf{y} = (y_1, \dots, y_k) \in R_q^k$, we set $\text{Zero}(\mathbf{y}) := \bigcap_{j=1}^k \text{Zero}(y_j)$ and similarly for multiple vectors $\mathbf{y}_1, \dots, \mathbf{y}_\ell$ over R_q , $\text{Zero}(\mathbf{y}_1, \dots, \mathbf{y}_\ell) := \bigcap_{j=1}^\ell \text{Zero}(\mathbf{y}_j)$.

Informally, we say that y has i zeroes in the Chinese Remainder Representation if $|\text{Zero}(y)| = i$. One observes that $\text{Zero}(y) = \emptyset$ if and only if y is invertible, by the Chinese Remainder Theorem. Also, $\text{Zero}(y) = [d] \iff y = 0$.

Lyubashevsky and Seiler [19] showed that if $\|y\| < q^{1/d}$ then y is invertible. Obviously, it is not very interesting if d is large (e.g. $d = n$). Here, we extend the result to consider the number of zeroes in the Chinese Remainder Representation.

Lemma 3.2. *Let $y \in R_q$ such that $0 < \|y\| < q^{m/d}$ for some $m \in [d]$. Then, $|\text{Zero}(y)| < m$.*

Proof. Suppose that $|\text{Zero}(y)| \geq m$ and pick any $i_1, \dots, i_m \in \text{Zero}(y)$. Define the following set:

$$A = \{z \in R : \forall j \in [m], z \equiv 0 \pmod{f_{i_j}(X)}\}.$$

Firstly, note that Λ is an additive group and $y \in \Lambda$. Moreover, for any $z \in \Lambda$, we have $z \cdot X \in \Lambda$ since each $f_{i_j}(X)$ is a factor of $X^n + 1$ modulo q . Therefore, Λ is an ideal of R , and hence an ideal lattice in the ring R . Consider the Chinese Remainder representation modulo q of all the elements in Λ . Note that they have 0 in the coefficients corresponding to $f_{i_j}(X)$ for $j \in \{1, \dots, m\}$ and arbitrary values everywhere else. This implies that $\det(\Lambda) = |\mathbb{Z}^n/\Lambda| = q^{nm/d}$. Hence, by Lemma 2.3 we have $\lambda_1(\Lambda) \geq q^{m/d}$. However, we know that $\|y\| > 0$, thus y is non-zero. Eventually, we obtain $\|y\| < q^{m/d} \leq \lambda_1(\Lambda) \leq \|y\|$ which leads to contradiction. \square

The lemma above implies that if a polynomial $y \in R_q$ is short enough, then it has only a few zeroes in the Chinese Remainder Representation (but is not necessarily invertible).

We now introduce the notion of `ZeroRows` which will be crucial in proving the main theorem.

Definition 3.3. Let $k \in \mathbb{N}$ and $A \subseteq R_q^k$ be a non-empty set. Then, we write $\text{ZeroRows}_i(A)$ to denote

$$\text{ZeroRows}_i(A) := \{\mathbf{a} \in A : |\text{Zero}(\mathbf{a})| = i\}.$$

We say that $\mathbf{a} \in \text{ZeroRows}_i(A)$ has i zero rows.

Name `ZeroRows` comes from the fact that if $\mathbf{a} = (a_1, \dots, a_k) \in \text{ZeroRows}_i(A)$ and if we write down the Chinese Remainder Representation of a_1, \dots, a_k as column vectors ⁸ then we get exactly i rows filled only with zeroes.

The next result gives an upper bound on $\text{ZeroRows}_i(S_\alpha^k)$ for fixed $i > 0, k$ and α . The key idea of the proof is as follows. For simplicity, consider $z' := z + X^j, z'' := z + X^\ell$ for some distinct $j, \ell \in [2n]$ and $z \in R_q$. To begin with, note that $\text{Zero}(z') \cap \text{Zero}(z'') = \emptyset$. Indeed, if there exists some $u \in \text{Zero}(z') \cap \text{Zero}(z'')$ then

$$z + X^\ell \equiv z'' \equiv 0 \equiv z' \equiv z + X^j \pmod{f_u(X)}.$$

Hence, we get a contradiction, since $X^j - X^\ell$ is invertible [6]. Therefore,

$$|\{z + X^j \in \text{ZeroRows}_i(S_\alpha) : j \in [2n]\}| \leq \lfloor d/i \rfloor.$$

This is because if size of the set is strictly larger than d/i then, by definition of $\text{ZeroRows}_i(S_\alpha)$ and the pigeonhole principle, we would have $\text{Zero}(z + X^j) \cap \text{Zero}(z + X^\ell) \neq \emptyset$ for some distinct j, ℓ . Thus, we end up with:

$$|\{z + X^j \notin \text{ZeroRows}_i(S_\alpha) : j \in [2n]\}| \geq 2n - \lfloor d/i \rfloor.$$

Our main strategy is that for each $\mathbf{z} \in \text{ZeroRows}_i(S_\alpha^k)$, we count all \mathbf{z}' of form $\mathbf{z} + \mathbf{y}$ (where \mathbf{y} is a somewhat small polynomial) such that $\mathbf{z}' \notin \text{ZeroRows}_i(S_\alpha^k)$ similarly as above, and eventually, obtain an upper bound on $|\text{ZeroRows}_i(S_\alpha^k)|$. The bound depends on the size of a set $W_i \subseteq R_q$, which satisfies the following

⁸ Namely, for each a_i we define a corresponding column vector $(a'_{i,1}, \dots, a'_{i,d})$, where $a'_{i,j}$ is the element of $\mathbb{Z}_q[X]/(f_j(X))$, such that $a_i \equiv a'_{i,j} \pmod{f_j(X)}$, for $j \in [d]$.

property: for any two distinct $u, v \in W_i$, $|\mathbf{Zero}(u - v)| < i$ ⁹. Later on, we show how to use our previous result, i.e. Lemma 3.2, to construct such sets.

Lemma 3.4. *Let $k, \alpha \in \mathbb{N}$, $i \in [d]$ and $W_i \subseteq R_q$ be a set of polynomials in R_q such that for any two distinct $u, v \in W_i$, $|\mathbf{Zero}(u - v)| < i$. Then,*

$$|\mathbf{ZeroRows}_i(S_\alpha^k)| \leq \frac{\binom{d}{i} \cdot |S_{\alpha + \|W_i\|_\infty}|^k}{|W_i|^k}.$$

Proof. Firstly, take any $\mathbf{z} = (z_1, \dots, z_k) \in S_\alpha^k$ and define

$$\mathbf{Bad}(z_1, \dots, z_k) := \{(z_1 + y_1, \dots, z_k + y_k) \in \mathbf{ZeroRows}_i(S_\alpha^k) : y_1, \dots, y_k \in W_i\}.$$

We claim that $|\mathbf{Bad}(z_1, \dots, z_k)| \leq \binom{d}{i}$. Indeed, suppose $|\mathbf{Bad}(z_1, \dots, z_k)| > \binom{d}{i}$ and define the function

$$F : \mathbf{Bad}(z_1, \dots, z_k) \rightarrow \mathcal{P}_i([d]), (z'_1, \dots, z'_k) \mapsto \mathbf{Zero}(z'_1, \dots, z'_k).$$

Note that F is well-defined by definition of \mathbf{Bad} . Also, $|\mathbf{Bad}(z_1, \dots, z_k)| > \binom{d}{i} = |\mathcal{P}_i([d])|$ implies that F is not injective. Hence,

$$F(z_1 + y_1, \dots, z_k + y_k) = I = F(z_1 + y'_1, \dots, z_k + y'_k)$$

for some set $I \in \mathcal{P}_i([d])$, $y_1, \dots, y_k, y'_1, \dots, y'_k \in W_i$ and $y_j \neq y'_j$ for some index j . Take any $u \in I$. Then, $z_j + y_j \equiv 0 \equiv z_j + y'_j \pmod{f_u(X)}$ and consequently, $y_j - y'_j \equiv 0 \pmod{f_u(X)}$. Since we picked arbitrary $u \in I$, we proved that $|\mathbf{Zero}(y_j - y'_j)| \geq i$. However, this leads to a contradiction by the definition of the set W_i .

Now, define a set

$$\mathbf{Good}(z_1, \dots, z_k) := \{(z_1 + y_1, \dots, z_k + y_k) \notin \mathbf{ZeroRows}_i(S_\alpha^k) : y_1, \dots, y_k \in W_i\}.$$

Clearly, $|\mathbf{Good}(z_1, \dots, z_k)| = |W_i|^k - |\mathbf{Bad}(z_1, \dots, z_k)| \geq |W_i|^k - \binom{d}{i}$. Consider the following set

$$S = \bigcup_{(z_1, \dots, z_k) \in \mathbf{ZeroRows}_i(S_\alpha^k)} \mathbf{Good}(z_1, \dots, z_k).$$

One observes that $S \subseteq S_{\alpha + \|W_i\|_\infty}^k \setminus \mathbf{ZeroRows}_i(S_\alpha^k)$ by definition of \mathbf{Good} , which gives us an upper bound on $|S|$. We are now interested in finding a lower bound for $|S|$. Let $(\hat{z}_1, \dots, \hat{z}_k)$ be an element of S and denote

$$\mathbf{COUNT}(\hat{z}_1, \dots, \hat{z}_k) := \{(z_1, \dots, z_k) \in \mathbf{ZeroRows}_i(S_\alpha^k) : (\hat{z}_1, \dots, \hat{z}_k) \in \mathbf{Good}(z_1, \dots, z_k)\}.$$

We claim that $|\mathbf{COUNT}(\hat{z}_1, \dots, \hat{z}_k)| \leq \binom{d}{i}$. Informally, this means that $(\hat{z}_1, \dots, \hat{z}_k)$ belongs to at most $\binom{d}{i}$ “good” sets (out of $|\mathbf{ZeroRows}_i(S_\alpha^k)|$). Just like before, assume that $|\mathbf{COUNT}(\hat{z}_1, \dots, \hat{z}_k)| > \binom{d}{i}$ and define a function

$$F : \mathbf{COUNT}(\hat{z}_1, \dots, \hat{z}_k) \rightarrow \mathcal{P}_i([d]), (z_1, \dots, z_k) \mapsto \mathbf{Zero}(z_1, \dots, z_k).$$

⁹ In the example above, W_1 is represented by the set $\{X^j : j \in [2n]\}$. Indeed, $|\mathbf{Zero}(X^j - X^k)| < 1$ for all distinct j, k .

Then,

$$F(z_1, \dots, z_k) = I = F(z'_1, \dots, z'_k)$$

for some set $I \in \mathcal{P}_i([d])$ and $z_1, \dots, z_k, z'_1, \dots, z'_k \in S_\alpha$ such that there exists an index j which satisfies $z_j \neq z'_j$. Since $(\hat{z}_1, \dots, \hat{z}_k) \in \text{Good}(z_1, \dots, z_k)$ and $(\hat{z}_1, \dots, \hat{z}_k) \in \text{Good}(z'_1, \dots, z'_k)$, we have that $z_j + y_j = \hat{z}_j = z'_j + y'_j$ for some distinct $y_j, y'_j \in W_i$. Take any $u \in I$ and note that $z_j \equiv 0 \equiv z'_j \pmod{f_u(X)}$. Therefore,

$$y_j \equiv \hat{z}_j - z_j \equiv \hat{z}_j - z'_j \equiv y'_j \pmod{f_u(X)}.$$

Hence, $|\text{Zero}(y_j - y'_j)| \geq i$. Similarly as before, we observe that this leads to a contradiction by the definition of W_i . Thus, $|\text{COUNT}(\hat{z}_1, \dots, \hat{z}_k)| \leq \binom{d}{i}$. This implies:

$$|S| \geq \frac{\sum_{\mathbf{z} \in \text{ZeroRows}_i(S_\alpha^k)} |\text{Good}(\mathbf{z})|}{\binom{d}{i}} \geq \frac{\sum_{\mathbf{z} \in \text{ZeroRows}_i(S_\alpha^k)} |W_i|^k - \binom{d}{i}}{\binom{d}{i}}$$

Combining the lower bound as well as the upper bound for $|S|$ we get:

$$\begin{aligned} |S_{\alpha + \|W_i\|_\infty}|^k - |\text{ZeroRows}_i(S_\alpha^k)| &\geq |S| \\ &\geq \frac{1}{\binom{d}{i}} |\text{ZeroRows}_i(S_\alpha^k)| \cdot |W_i|^k - |\text{ZeroRows}_i(S_\alpha^k)|. \end{aligned} \tag{3}$$

Therefore, $|\text{ZeroRows}_i(S_\alpha^k)| \leq \frac{\binom{d}{i} \cdot |S_{\alpha + \|W_i\|_\infty}|^k}{|W_i|^k}$. \square

We point out that the proof does not work for $i = 0$. In this case, we can use the obvious upper bound: $|\text{ZeroRows}_0(S_\alpha^k)| \leq |S_\alpha^k|$.

Consider again the equation $\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = \mathbf{c}\mathbf{t}$, where \mathbf{A} and \mathbf{t} are variables, and denote $\mathbf{A} = (a_{i,j})$ and $\mathbf{t} = (t_1, \dots, t_k)$. Clearly, we have $\text{Zero}(\mathbf{z}_1, c, \mathbf{z}_2) \subseteq \text{Zero}(\mathbf{z}_1, c)$. Suppose that $\text{Zero}(\mathbf{z}_1, c, \mathbf{z}_2) \neq \text{Zero}(\mathbf{z}_1, c)$. If we write $\mathbf{z}_1 = (z_1, \dots, z_\ell)$ and $\mathbf{z}_2 = (z'_1, \dots, z'_k)$, then there exist some i, j such that $i \in \text{Zero}(\mathbf{z}_1, c)$ and $i \notin \text{Zero}(\mathbf{z}_1, c, z'_j)$. Note that

$$\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = \mathbf{c}\mathbf{t} \implies a_{j,1}z_1 + \dots + a_{j,\ell}z_\ell + z'_j = ct_j.$$

However,

$$0 \neq z'_j \equiv a_{j,1}z_1 + \dots + a_{j,\ell}z_\ell + z'_j \equiv ct_j \equiv 0 \pmod{f_i(X)},$$

which leads to a contradiction. Therefore, if $\text{Zero}(\mathbf{z}_1, c, \mathbf{z}_2) \neq \text{Zero}(\mathbf{z}_1, c)$ then we end up with no solutions. This motivates us to extend the ZeroRows function as follows.

Definition 3.5. Let $k \in \mathbb{N}$ and $A \subseteq R_q^k, B \subseteq R_q^\ell$ be non-empty sets. Then, we define $\text{ZeroRows}_i(A; B)$ to be

$$\text{ZeroRows}_i(A; B) := \{(\mathbf{a}, \mathbf{b}) \in A \times B : \text{Zero}(\mathbf{a}, \mathbf{b}) = \text{Zero}(\mathbf{a}) \wedge |\text{Zero}(\mathbf{a})| = i\}.$$

Sometimes, we write $\text{ZeroRows}_i(A_1, A_2; B)$ to denote $\text{ZeroRows}_i(\bar{A}; B)$, where $\bar{A} = A_1 \times A_2$.

Using the same techniques as before, one can prove a similar result to Lemma 3.4 which is related to the modified ZeroRows function.

Lemma 3.6. *Let $k, \ell, \alpha_1, \alpha_2 \in \mathbb{N}$, $i \in [d]$ and $W_i \subseteq R_q$ be a set of polynomials in R_q such that for any two distinct $u, v \in W_i$, $|\mathbf{Zero}(u - v)| < i$. Take any set $\mathcal{D} \subseteq R_q \setminus \{\mathbf{0}\}$ and define e to be the largest integer which satisfies $\|\mathcal{D}\| \geq q^{e/d}$. Then,*

$$|\mathbf{ZeroRows}_i(S_{\alpha_1}^\ell, \mathcal{D}; S_{\alpha_2}^k)| \leq \frac{\binom{e}{i} \cdot |S_{\alpha_1 + \|W_i\|_\infty}^\ell| \cdot |S_{\alpha_2 + \|W_i\|_\infty}^k| \cdot |\mathcal{D}|}{|W_i|^{\ell+k}}.$$

Proof. Since we follow the same strategy as in the proof of Lemma 3.4, we only provide a proof sketch. To begin with, take any $\mathbf{z}_1 = (z_1, \dots, z_\ell) \in S_{\alpha_1}^\ell$, $c \in \mathcal{D}$, $\mathbf{z}_2 = (z'_1, \dots, z'_k) \in S_{\alpha_2}^k$ and define

$$\mathbf{Bad}(\mathbf{z}_1, c, \mathbf{z}_2) := \{(\mathbf{z}_1 + \mathbf{y}, c, \mathbf{z}_2 + \mathbf{y}') \in \mathbf{ZeroRows}_i(S_{\alpha_1}^\ell, \mathcal{D}; S_{\alpha_2}^k) : \mathbf{y} \in W_i^\ell, \mathbf{y}' \in W_i^k\}.$$

We point out that c stays still. Using the same technique as before, one can prove that $|\mathbf{Bad}(\mathbf{z}_1, c, \mathbf{z}_2)| \leq \binom{e}{i}$. Informally, this is because we only consider all subsets of $\mathbf{Zero}(c)$ (instead of $[d]$ like last time) of size i and c has at most e zeroes in the Chinese Remainder Representation (Lemma 3.2).

Now, we define a set

$$\mathbf{Good}(\mathbf{z}_1, c, \mathbf{z}_2) := \{(\mathbf{z}_1 + \mathbf{y}, c, \mathbf{z}_2 + \mathbf{y}') \notin \mathbf{ZeroRows}_i(S_{\alpha_1}^\ell, \mathcal{D}; S_{\alpha_2}^k) : \mathbf{y} \in W_i^\ell, \mathbf{y}' \in W_i^k\}.$$

As before, we have $|\mathbf{Good}(\mathbf{z}_1, c, \mathbf{z}_2)| = |W_i|^{\ell+k} - |\mathbf{Bad}(\mathbf{z}_1, c, \mathbf{z}_2)| \geq |W_i|^{\ell+k} - \binom{e}{i}$. Consider the following set

$$S = \bigcup_{(\mathbf{z}_1, c, \mathbf{z}_2) \in \mathbf{ZeroRows}_i(S_{\alpha_1}^\ell, \mathcal{D}; S_{\alpha_2}^k)} \mathbf{Good}(\mathbf{z}_1, c, \mathbf{z}_2).$$

We have that

$$S \subseteq S_{\alpha_1 + \|W_i\|_\infty}^\ell \times \mathcal{D} \times S_{\alpha_2 + \|W_i\|_\infty}^k \setminus \mathbf{ZeroRows}_i(S_{\alpha_1}^\ell, \mathcal{D}; S_{\alpha_2}^k)$$

by definition of \mathbf{Good} . Let $(\mathbf{z}'_1, c, \mathbf{z}'_2)$ be an element of S and denote

$$\mathbf{COUNT}(\mathbf{z}'_1, c, \mathbf{z}'_2) := \{(\mathbf{z}_1, c, \mathbf{z}_2) \in \mathbf{ZeroRows}_i(S_{\alpha_1}^\ell, \mathcal{D}; S_{\alpha_2}^k) : (\mathbf{z}'_1, c, \mathbf{z}'_2) \in \mathbf{Good}(\mathbf{z}_1, c, \mathbf{z}_2)\}.$$

Similarly as before, we can show that $|\mathbf{COUNT}(\hat{z}_1, \dots, \hat{z}_k)| \leq \binom{e}{i}$. Hence, we get:

$$\begin{aligned} |S| &\geq \frac{\sum_{(\mathbf{z}_1, c, \mathbf{z}_2) \in \mathbf{ZeroRows}_i(S_{\alpha_1}^\ell, \mathcal{D}; S_{\alpha_2}^k)} |\mathbf{Good}(\mathbf{z}_1, c, \mathbf{z}_2)|}{\binom{e}{i}} \\ &\geq \frac{\sum_{(\mathbf{z}_1, c, \mathbf{z}_2) \in \mathbf{ZeroRows}_i(S_{\alpha_1}^\ell, \mathcal{D}; S_{\alpha_2}^k)} (|W_i|^{\ell+k} - \binom{e}{i})}{\binom{e}{i}} \end{aligned} \quad (4)$$

Combining the lower bound as well as upper bound for $|S|$ we get:

$$|S_{\alpha_1 + \|W_i\|_\infty}^\ell| \cdot |\mathcal{D}| \cdot |S_{\alpha_2 + \|W_i\|_\infty}^k| - |\mathbf{ZeroRows}_i(S_{\alpha_1}^\ell, \mathcal{D}; S_{\alpha_2}^k)| \geq |S|,$$

and

$$|S| \geq \frac{1}{\binom{e}{i}} |\text{ZeroRows}_i(S_{\alpha_1}^\ell, \mathcal{D}; S_{\alpha_2}^k)| \cdot |W_i|^{\ell+k} - |\text{ZeroRows}_i(S_{\alpha_1}^\ell, \mathcal{D}; S_{\alpha_2}^k)|.$$

Therefore, $|\text{ZeroRows}_i(S_{\alpha_1}^\ell, \mathcal{D}; S_{\alpha_2}^k)| \leq \frac{\binom{e}{i} \cdot |S_{\alpha_1 + \|W_i\|_\infty}^\ell \cdot |S_{\alpha_2 + \|W_i\|_\infty}|^k \cdot |\mathcal{D}|}{|W_i|^{\ell+k}}$. \square

Again, we note that the lemma does not hold for $i = 0$. In this case, we use a simple bound: $|\text{ZeroRows}_0(S_{\alpha_1}^\ell, \mathcal{D}; S_{\alpha_2}^k)| \leq |S_{\alpha_1}^\ell| \cdot |S_{\alpha_2}^k| \cdot |\mathcal{D}|$.

In Lemma 3.6 we have an additional condition $0 \notin \mathcal{D}$. This is because otherwise we cannot define the integer e . Recall that e represents the maximal number of zeroes in the Chinese Remainder Representation that an element in \mathcal{D} can have. Hence, in case $\mathcal{D} = \{0\}$, we can simply set $e = d$ and follow the strategy as in Lemma 3.6. Thus, we end up with the following corollary.

Corollary 3.7. *Let $k, \ell, \alpha_1, \alpha_2 \in \mathbb{N}$, $i \in [d]$ and $W_i \subseteq R_q$ be a set of polynomials in R_q such that for any two distinct $u, v \in W_i$, $|\text{Zero}(u - v)| < i$. Then,*

$$|\text{ZeroRows}_i(S_{\alpha_1}^\ell; S_{\alpha_2}^k)| \leq \frac{\binom{d}{i} \cdot |S_{\alpha_1 + \|W_i\|_\infty}^\ell \cdot |S_{\alpha_2 + \|W_i\|_\infty}|^k}{|W_i|^{\ell+k}}.$$

3.2 Computing Probabilities

We state and prove the main results of our paper. The first one provides an upper bound on the probability (over \mathbf{A} and \mathbf{t}) of existence of $(\mathbf{z}_1, \mathbf{z}_2, c)$ which satisfy $\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = c\mathbf{t}$. This can be applied to the security analysis of the Bai-Galbraith scheme [4] or qTESLA [2, 8]. The second one, however, considers a slightly different equation: $\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = c\mathbf{t}_1 \cdot 2^\delta$ where $\mathbf{t}_1 = \text{Power2Round}_q(\mathbf{t}, \delta)$ for some δ , and can be applied to the security analysis of Dilithium-QROM [11].

Theorem 3.8. *Let $\alpha_1, \alpha_2 \in \mathbb{N}$ and $\mathcal{D} \subseteq R_q \setminus \{0\}$. Also, for $i = 1, \dots, d$, define $W_i \subseteq R_q$ to be a set of polynomials such that for any two distinct $u, v \in W_i$, $|\text{Zero}(u - v)| < i$. Then*

$$\begin{aligned} \Pr_{\mathbf{A} \leftarrow R_q^{k \times \ell}, \mathbf{t} \leftarrow R_q^k} [\exists (\mathbf{z}_1, \mathbf{z}_2, c) \in S_{\alpha_1}^\ell \times S_{\alpha_2}^k \times \mathcal{D} : \mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = c\mathbf{t}] \leq \\ \frac{|S_{\alpha_1}^\ell| \cdot |S_{\alpha_2}^k| \cdot |\mathcal{D}|}{q^{nk}} + \sum_{i=1}^e \frac{\binom{e}{i} \cdot |S_{\alpha_1 + \|W_i\|_\infty}^\ell \cdot |S_{\alpha_2 + \|W_i\|_\infty}|^k \cdot |\mathcal{D}|}{|W_i|^{\ell+k} \cdot q^{nk(1-i/d)}} \end{aligned} \quad (5)$$

where e is the largest integer such that $|\mathcal{D}| \geq q^{e/d}$.

Proof. Fix $\mathbf{z}_1 = (z_1, \dots, z_\ell)$, $\mathbf{z}_2 = (z'_1, \dots, z'_k)$ and c . We first prove that

$$\text{Zero}(\mathbf{z}_1, c) \neq \text{Zero}(\mathbf{z}_1, c, \mathbf{z}_2) \implies \Pr_{\mathbf{A} \leftarrow R_q^{k \times \ell}, \mathbf{t} \leftarrow R_q^k} [\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = c\mathbf{t}] = 0.$$

Suppose that $\text{Zero}(\mathbf{z}_1, c) \neq \text{Zero}(\mathbf{z}_1, c, \mathbf{z}_2)$. Then, there exists some $i \in [d]$ such that $i \in \text{Zero}(\mathbf{z}_1, c)$ and $i \notin \text{Zero}(\mathbf{z}_1, c, \mathbf{z}_2)$. This implies that there is some $j \in [k]$

so that $i \notin \text{Zero}(\mathbf{z}_1, c, z'_j)$ (otherwise $i \in \text{Zero}(\mathbf{z}_1, c, \mathbf{z}_2)$). In particular, we have $z'_j \not\equiv 0 \pmod{f_i(X)}$. Denote $\mathbf{A} = (a_{i,j})$ and $\mathbf{t} = (t_1, \dots, t_k)$ and note that

$$\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = c\mathbf{t} \implies a_{j,1}z_1 + \dots + a_{j,\ell}z_\ell + z'_j = ct_j.$$

However,

$$0 \not\equiv z'_j \equiv a_{j,1}z_1 + \dots + a_{j,\ell}z_\ell + z'_j \equiv ct_j \equiv 0 \pmod{f_i(X)},$$

contradiction.

Hence, there are no \mathbf{A}, \mathbf{t} which satisfy $\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = c\mathbf{t}$. Thus, we only consider $(\mathbf{z}_1, c, \mathbf{z}_2)$ such that $\text{Zero}(\mathbf{z}_1, c) = \text{Zero}(\mathbf{z}_1, c, \mathbf{z}_2)$, alternatively $(\mathbf{z}_1, c, \mathbf{z}_2) \in \text{ZeroRows}_i(S_{\alpha_1}^\ell, \mathcal{D}; S_{\alpha_2}^k)$ for some $i \leq e$. We claim that

$$\Pr_{\mathbf{A} \leftarrow R^{k \times \ell}, \mathbf{t} \leftarrow R_q^k}[\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = c\mathbf{t}] = 1/q^{nk(1-i/d)}.$$

Note that we can write:

$$\Pr_{\mathbf{A} \leftarrow R^{k \times \ell}, \mathbf{t} \leftarrow R_q^k}[\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = c\mathbf{t}] = \prod_{i=1}^k \Pr_{a_{i,1}, \dots, a_{i,\ell}, t_i \leftarrow R_q} [a_{i,1}z_1 + \dots + a_{i,\ell}z_\ell + z'_i = c \cdot t_i].$$

Let us fix an index i and define

$$A = \{(a_1, \dots, a_\ell, t) \in R_q^{\ell+1} : \sum_{j=1}^{\ell} a_j z_j + z'_i = c \cdot t\}.$$

We want to show that $|A| = q^{n(\ell+i/d)}$. Take any $u \in [d]$ and consider the set

$$A_u = \{(a_1, \dots, a_\ell, t) \in (\mathbb{Z}_q[X]/(f_u(X)))^{\ell+1} : a_1 z_1 + \dots + a_\ell z_\ell + z'_i \equiv c \cdot t \pmod{f_u(X)}\}.$$

If $u \in \text{Zero}(\mathbf{z}_1, c, \mathbf{z}_2)$ then any a_1, \dots, a_ℓ, t satisfy the equation, because

$$z_1 \equiv \dots \equiv z_\ell \equiv z'_i \equiv c \equiv 0 \pmod{f_u(X)}.$$

Hence, $|A_u| = q^{(\ell+1) \cdot n/d}$. If $u \notin \text{Zero}(\mathbf{z}_1, c, \mathbf{z}_2)$ then one of z_1, \dots, z_ℓ, c is invertible modulo $(f_u(X), q)$, without loss of generality say z_j . Then, $a_1, \dots, a_{j-1}, a_{j+1}, \dots, a_\ell, c$ can be chosen arbitrarily and a_j is picked such that the equation is satisfied. Therefore, $|A_u| = q^{\ell \cdot n/d}$. Now, by the Chinese Remainder Theorem we have that

$$|A| = \prod_{u=1}^d |A_u| = q^{i \cdot (\ell+1) \cdot n/d + (d-i) \cdot \ell \cdot n/d} = q^{n(\ell+i/d)}.$$

Hence,

$$\Pr_{a_{i,1}, \dots, a_{i,\ell}, t_i \leftarrow R_q} [a_{i,1}z_1 + \dots + a_{i,\ell}z_\ell + z'_i = c \cdot t_i] = \frac{|A|}{q^{(\ell+1) \cdot n}} = 1/q^{n(1-i/d)}.$$

Eventually, we obtain $\Pr_{\mathbf{A} \leftarrow R^{k \times \ell}, \mathbf{t} \leftarrow R_q^k}[\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = c\mathbf{t}] = 1/q^{nk(1-i/d)}$.

Now, we combine the observations above and Lemma 3.6. For clarity, set $Z_i = \text{ZeroRows}_i(S_{\alpha_1}^\ell, \mathcal{D}; S_{\alpha_2}^k)$. Then,

$$\begin{aligned}
& \Pr_{\mathbf{A} \leftarrow R^{k \times \ell}, \mathbf{t} \leftarrow R_q^k} [\exists (\mathbf{z}_1, \mathbf{z}_2, c) \in S_{\alpha_1}^\ell \times S_{\alpha_2}^k \times \mathcal{D} : \mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = c\mathbf{t}] \\
& \leq \sum_{\mathbf{z}_1 \in S_{\alpha_1}^\ell, c \in \mathcal{D}, \mathbf{z}_2 \in S_{\alpha_2}^k} \Pr_{\mathbf{A} \leftarrow R^{k \times \ell}, \mathbf{t} \leftarrow R_q^k} [\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = c\mathbf{t}] \\
& \leq \sum_{i=0}^e \sum_{(\mathbf{z}_1, c, \mathbf{z}_2) \in Z_i} \Pr_{\mathbf{A} \leftarrow R^{k \times \ell}, \mathbf{t} \leftarrow R_q^k} [\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = c\mathbf{t}] \\
& \leq \sum_{i=0}^e \sum_{(\mathbf{z}_1, c, \mathbf{z}_2) \in Z_i} 1/q^{nk(1-i/d)} \\
& \leq \sum_{i=0}^e |Z_i|/q^{nk(1-i/d)} \\
& \leq \frac{|S_{\alpha_1}|^\ell \cdot |S_{\alpha_2}|^k \cdot |\mathcal{D}|}{q^{nk}} + \sum_{i=1}^e \frac{\binom{e}{i} \cdot |S_{\alpha_1 + \|W_i\|_\infty}|^\ell \cdot |S_{\alpha_2 + \|W_i\|_\infty}|^k \cdot |\mathcal{D}|}{|W_i|^{\ell+k} \cdot q^{nk(1-i/d)}}.
\end{aligned} \tag{6}$$

□

We can obtain a very similar result for $\mathcal{D} = \{0\}$ using Corollary 3.7. We just need to pick e to be the integer, such that any non-zero $(\mathbf{z}_1, \mathbf{z}_2) \in S_{\alpha_1}^\ell \times S_{\alpha_2}^k$ has at most e zero rows. Since each component of \mathbf{z}_1 has norm at most $\alpha_1\sqrt{n}$, we could choose the maximal e so that $\alpha_1\sqrt{n} \geq q^{e/d}$. We omit the proof since it is very similar to the one for Theorem 3.8.

Corollary 3.9. *Let $\alpha_1, \alpha_2 \in \mathbb{N}$. Also, for $i = 1, \dots, d$, define $W_i \subseteq R_q$ to be a set of polynomials such that for any two distinct $u, v \in W_i$, $|\text{Zero}(u - v)| < i$. Then*

$$\begin{aligned}
& \Pr_{\mathbf{A} \leftarrow R_q^{k \times \ell}} [\exists (\mathbf{z}_1, \mathbf{z}_2) \in S_{\alpha_1}^\ell \setminus \{\mathbf{0}\} \times S_{\alpha_2}^k : \mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = \mathbf{0}] \leq \\
& \frac{|S_{\alpha_1}|^\ell \cdot |S_{\alpha_2}|^k}{q^{nk}} + \sum_{i=1}^e \frac{\binom{d}{i} \cdot |S_{\alpha_1 + \|W_i\|_\infty}|^\ell \cdot |S_{\alpha_2 + \|W_i\|_\infty}|^k}{|W_i|^{\ell+k} \cdot q^{nk(1-i/d)}},
\end{aligned} \tag{7}$$

where e is the largest integer such that $\alpha_1\sqrt{n} \geq q^{e/d}$.

The next theorem considers a modified equation $\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = c\mathbf{t}_1 \cdot 2^\delta$ where $\mathbf{t}_1 = \text{Power2Round}_q(\mathbf{t}, \delta)$ for some $\delta \in \mathbb{N}$. However, we need to take a slightly different approach in order to provide a reasonable upper bound for the probability due to the appearance of Power2Round_q function.

Theorem 3.10. *Let $\alpha_1, \alpha_2, \delta \in \mathbb{N}$ and $\mathcal{D} \subseteq R_q \setminus \{\mathbf{0}\}$. Also, for $i = 1, \dots, d$, define $W_i \subseteq R_q$ to be a set of polynomials such that for any two distinct $u, v \in W_i$,*

$|\text{Zero}(u - v)| < i$. Then

$$\begin{aligned} \Pr_{\mathbf{A} \leftarrow R_q^{k \times \ell}, \mathbf{t} \leftarrow R_q^k} [\exists(\mathbf{z}_1, \mathbf{z}_2, c) \in S_{\alpha_1}^\ell \times S_{\alpha_2}^k \times \mathcal{D} : \mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = c\mathbf{t}_1 \cdot 2^\delta] \leq \\ \leq |D| \cdot |S_{\alpha_2}|^k \cdot \left(\left(\frac{2^\delta}{q^{(1-e_1/d)}} \right)^{nk} + \frac{|S_{\alpha_1}|^\ell}{q^{nk}} + \sum_{i=1}^{e_2} \frac{\binom{d}{i} \cdot |S_{\alpha_1 + \|W_i\|_\infty}|^\ell}{|W_i|^\ell \cdot q^{nk(1-i/d)}} \right) \end{aligned} \quad (8)$$

where $\mathbf{t}_1 = \text{Power2Round}_q(\mathbf{t}, \delta)$ and e_1 (resp. e_2) is the largest integer such that $\|D\| \geq q^{e_1/d}$ (resp. $\alpha_1 \sqrt{N} \geq q^{e_2/d}$).

Proof. Case 1. suppose that $\mathbf{z}_1 = 0$. Then, the probability becomes:

$$\Pr_{\mathbf{t} \leftarrow R_q^k} [\exists(\mathbf{z}_2, c) \in S_{\alpha_2}^k \times \mathcal{D} : \mathbf{z}_2 = c\mathbf{t}_1 \cdot 2^\delta].$$

Fix $\mathbf{z}_2 = (z_1, \dots, z_k)$, c and denote $\mathbf{t} = (t_1, \dots, t_k)$. Consider the following probability:

$$\Pr_{\mathbf{t} \leftarrow R_q^k} [\mathbf{z}_2 = c\mathbf{t}] = \prod_{j=1}^k \Pr[z_j = ct_j].$$

By definition of e_1 , we have $|\text{Zero}(c)| \leq e_1$ by Lemma 3.2. Take arbitrary $j \in [k]$. We compute the maximal number of polynomials t_j satisfying $z_j = ct_j$. Define a set

$$T_u = \{t \in \mathbb{Z}_q[X]/(f_u(X)) : z_j \equiv ct \pmod{f_u(X)}\}.$$

Clearly, $|T_u| \leq q^{n/d}$. Let $u \notin \text{Zero}(c)$. Then, c is invertible modulo $(f_u(X), q)$. Therefore, $|T_u| = 1$. By the Chinese Remainder Theorem, the number of polynomials t_j satisfying $z_j = ct_j$ is at most

$$\prod_{u=1}^k |T_u| \leq q^{|\text{Zero}(c)| \cdot n/d} \leq q^{e_1 \cdot n/d}.$$

Hence, we end up with

$$\Pr[z_j = ct_j] \leq \frac{q^{e_1 \cdot n/d}}{q^n} = \frac{1}{q^{n(1-e_1/d)}}.$$

Thus:

$$\Pr_{\mathbf{t} \leftarrow R_q^k} [\mathbf{z}_2 = c\mathbf{t}] = \prod_{j=1}^k \Pr[z_j = ct_j] \leq \frac{1}{q^{nk(1-e_1/d)}}.$$

For $\mathbf{t} \in R_q^k$, the most frequent value of each coefficient of \mathbf{t}_1 occurs at most 2^δ times. Hence,

$$\Pr_{\mathbf{t} \leftarrow R_q^k} [\mathbf{z}_2 = c\mathbf{t}_1 \cdot 2^\delta] \leq \left(\frac{2^\delta}{q^{(1-e_1/d)}} \right)^{nk}.$$

Eventually, by the union bound we obtain:

$$\Pr_{\mathbf{t} \leftarrow R_q^k} [\exists (\mathbf{z}_2, c) \in S_{\alpha_2}^k \times \mathcal{D} : \mathbf{z}_2 = c\mathbf{t}_1 \cdot 2^\delta] \leq \sum_{\mathbf{z}_2 \in S_{\alpha_2}^k, c \in \mathcal{D}} \left(\frac{2^\delta}{q^{(1-e_1/d)}} \right)^{nk},$$

and the sum is equal to $|\mathcal{D}| \cdot |S_{\alpha_2}|^k \cdot \left(\frac{2^\delta}{q^{(1-e_1/d)}} \right)^{nk}$.

Case 2. Suppose that $\mathbf{z} = (z_1, \dots, z_\ell) \neq \mathbf{0}$ and fix $\mathbf{z}_2 = (z'_1, \dots, z'_k)$ and c . Also, denote $\mathbf{A} = (a_{i,j})$, $\mathbf{t} = (t_1, \dots, t_k)$ and $t'_i = \text{Power2Round}_q(t_i, \delta)$ for $i \in [k]$. Then,

$$\Pr_{\mathbf{A} \leftarrow R^{k \times \ell}, \mathbf{t} \leftarrow R_q^k} [\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = c\mathbf{t}_1 \cdot 2^\delta] = \prod_{i=1}^k \Pr_{a_{i,1}, \dots, a_{i,\ell}, t_i \leftarrow R_q} \left[\sum_{j=1}^{\ell} a_{i,j} z_j + z'_i = c \cdot t'_i \cdot 2^\delta \right].$$

Let us fix an index i and consider the set

$$A_t = \{(a_1, \dots, a_\ell) \in R_q^\ell : \sum_{j=1}^{\ell} a_j z_j + z'_i = c \cdot t' \cdot 2^\delta\},$$

where $t' = \text{Power2Round}_q(t)$. We want to prove that $|A_t| \leq q^{n(\ell-1+m/d)}$, where $m = |\text{Zero}(z_1, \dots, z_\ell)|$. Define

$$A_t^u = \{(a_1, \dots, a_\ell) \in (\mathbb{Z}_q[X]/(f_u(X)))^\ell : \sum_{j=1}^{\ell} a_j z_j \equiv c \cdot t' \cdot 2^\delta - z'_i \pmod{f_u(X)}\}.$$

Clearly, we have $|A_t^u| \leq q^{\ell \cdot n/d}$. Consider $u \notin \text{Zero}(z_1, \dots, z_\ell)$. This means that z_w is invertible modulo $(f_u(X), q)$ for some $w \in [\ell]$. Hence, we can pick any possible values for $a_1, \dots, a_{w-1}, a_{w+1}, \dots, a_\ell$ and then adjust a_w so that it satisfies the equation. Note that for fixed $a_1, \dots, a_{w-1}, a_{w+1}, \dots, a_\ell$, there is exactly one such a_w . Thus, $|A_t^u| = q^{(\ell-1) \cdot n/d}$. By the Chinese Remainder Theorem, we get

$$|A_t| = \prod_{u=1}^d |A_t^u| \leq q^{m \cdot n\ell/d} \cdot q^{(d-m) \cdot (\ell-1)n/d} = q^{n(\ell-1+m/d)}.$$

Since we consider uniform distribution for $a_{i,1}, \dots, a_{i,\ell}, t_i$, we can conclude that:

$$\Pr_{a_{i,1}, \dots, a_{i,\ell}, t_i \leftarrow R_q} \left[\sum_{j=1}^{\ell} a_{i,j} z_j + z'_i = c \cdot t'_i \cdot 2^\delta \right] = \frac{\sum_{t_i \in R_q} |A_{t_i}|}{q^{\ell \cdot n} \cdot q^n} \leq \frac{q^{n(\ell-1+m/d)}}{q^{\ell \cdot n}} = 1/q^{n(1-m/d)}.$$

Therefore, $\Pr_{\mathbf{A} \leftarrow R^{k \times \ell}, \mathbf{t} \leftarrow R_q^k} [\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = c\mathbf{t}_1 \cdot 2^\delta] \leq 1/q^{nk(1-m/d)}$.

Now we can apply the union bound. First of all, note that if $i > e_2$ then $\text{ZeroRows}_i(S_{\alpha_1}^\ell \setminus \{\mathbf{0}\}) = \emptyset$ by Lemma 3.2. Hence,

$$S_{\alpha_1}^\ell \setminus \{\mathbf{0}\} = \bigcup_{i=0}^d \text{ZeroRows}_i(S_{\alpha_1}^\ell \setminus \{\mathbf{0}\}) = \bigcup_{i=0}^{e_2} \text{ZeroRows}_i(S_{\alpha_1}^\ell \setminus \{\mathbf{0}\}).$$

For simplicity, denote $Z_i = \text{ZeroRows}_i(S_{\alpha_1}^\ell \setminus \{\mathbf{0}\})$. Then,

$$\begin{aligned}
& \Pr[\exists(\mathbf{z}_1, \mathbf{z}_2, c) \in S_{\alpha_1}^\ell \times S_{\alpha_2}^k \times \mathcal{D} : \mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = c\mathbf{t}_1 \cdot 2^\delta] \\
& \leq \sum_{\mathbf{z}_1 \in S_{\alpha_1}^\ell \setminus \{\mathbf{0}\}, \mathbf{z}_2 \in S_{\alpha_2}^k, c \in \mathcal{D}} \Pr[\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = c\mathbf{t}_1 \cdot 2^\delta] \\
& \leq \sum_{\mathbf{z}_2 \in S_{\alpha_2}^k, c \in \mathcal{D}} \sum_{i=0}^{e_2} \sum_{\mathbf{z}_1 \in Z_i} \Pr[\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 = c\mathbf{t}_1 \cdot 2^\delta] \\
& \leq \sum_{\mathbf{z}_2 \in S_{\alpha_2}^k, c \in \mathcal{D}} \sum_{i=0}^{e_2} \sum_{\mathbf{z}_1 \in Z_i} 1/q^{nk(1-i/d)} \\
& \leq \sum_{\mathbf{z}_2 \in S_{\alpha_2}^k, c \in \mathcal{D}} \sum_{i=0}^{e_2} |Z_i|/q^{nk(1-i/d)}.
\end{aligned} \tag{9}$$

By Lemma 3.4, $|Z_i| \leq \frac{\binom{d}{i} \cdot |S_{\alpha_1 + \|W_i\|_\infty}^\ell|}{|W_i|^\ell}$. Also, we have $|Z_0| \leq |S_{\alpha_1}|^\ell$. Therefore, we can bound the probability above by:

$$|\mathcal{D}| \cdot |S_{\alpha_2}^k| \cdot (|S_{\alpha_1}|^\ell / q^{nk} + \sum_{i=1}^{e_2} \frac{\binom{d}{i} \cdot |S_{\alpha_1 + \|W_i\|_\infty}^\ell|}{|W_i|^\ell \cdot q^{nk(1-i/d)}}). \tag{10}$$

The theorem now follows from combining the two cases. \square

3.3 Constructing W_i

All the probability results presented in the previous subsection depend on the sizes of sets W_i . Recall that a set W_i satisfies a condition that for any two distinct $u, v \in W_i$, we have $|\text{Zero}(u - v)| < i$. Based on the upper bounds obtained above, we would like to construct large sets W_i but with small infinity norm $\|W_i\|_\infty$.

Let us start by constructing W_1 . We choose

$$W_1 := \{X^i : i \in [2n]\}.$$

Clearly, $X^i - X^j \in R_q$ is invertible, for $i \neq j$, so $|\text{Zero}(X^i - X^j)| = 0 < 1$. Also, $|W_1| = 2n$ and $\|W_1\|_\infty = 1$.

Now, let us fix $i \geq 2$. The main idea is to set W_i to be a subset of $S = \{u \in R_q : \|u\| < \frac{1}{2}q^{i/d}\}$, i.e. $\|W_i\| < \frac{1}{2}q^{i/d}$. Note that if we pick two distinct $u, v \in S$, then $0 < \|u - v\| < q^{i/d}$ by the triangle inequality. Hence, by Lemma 3.2 we get that $|\text{Zero}(u - v)| < i$. Therefore, any subset of S will satisfy the condition for W_i ¹⁰.

If $t := \lfloor \frac{q^{i/d}}{2} \rfloor$ is smaller than \sqrt{n} then we set

$$W_i := \left\{ \sum_{j=1}^t \epsilon_j \cdot X^{\alpha_j} \in R_q : \epsilon_1, \dots, \epsilon_t \in \{-1, 0, 1\}, \{\alpha_1, \dots, \alpha_t\} \in \mathcal{P}_{t^2}([n]) \right\}.$$

¹⁰ Note that this technique can also be used for W_1 as long as $q^{1/d}$ is large enough.

Then, $\|W_i\|_\infty = 1$, $\|W_i\| = t < \frac{1}{2}q^{i/d}$ and

$$|W_i| = \sum_{j=0}^{t^2} \binom{n}{j} \cdot 2^j.$$

Suppose that $t \geq \sqrt{n}$. In this case, we provide two constructions of W_i and in the experiments we choose the one that minimises the overall probability.

1. Set $W_i := S$. Then, $\|W_i\|_\infty = \lfloor \frac{1}{2}q^{i/d} \rfloor$ and $|W_i| \geq V_n(\frac{1}{2}q^{i/d} - \sqrt{n})$ ¹¹ where $V_N(r)$ is the volume of an n -dimensional ball of radius r .
2. Set $W_i := S_{\lfloor t/\sqrt{n} \rfloor}$. Clearly, we have the following properties: $W_i \subseteq S$, $\|W_i\|_\infty = \lfloor t/\sqrt{n} \rfloor$ and $|W_i| = (2 \lfloor t/\sqrt{n} \rfloor + 1)^n$.

4 Applications to the Bai-Galbraith Scheme

We present a slightly modified version of Bai-Galbraith scheme [4] whose security is based on MLWE in the quantum random oracle model. First, we construct the corresponding lossy identification protocol¹². Results from the previous section will be used to prove security properties of this ID scheme. Then, using the main result of [11], we obtain the secure signature scheme in the QROM. Note that identical techniques can be applied to other closely related signature schemes, such as qTESLA [2, 8] or the original scheme [4]. We focus on the modified scheme because it is actually a simpler version of Dilithium-QROM. Since the highly-optimised version of Dilithium-QROM can be somewhat overwhelming to readers who are not already comfortable with such constructions, we consider its simplified version here.

4.1 The Identification Protocol

The algorithms for identification protocol $\text{ID} = (\text{IGen}, \text{P}_1, \text{P}_2, \text{V})$ are described in Figure 3 with the concrete parameters $\text{par} = (q, d, n, k, \ell, \gamma, \gamma', \eta, \beta)$ given later in Table 1 and Table 2.

We want the challenge space in these ID and signature schemes to be a subset of the ring R , have size a little larger than 2^{256} , and consist of polynomials with small norms. In this paper, we set the dimension n of the ring R to be equal to 512. Hence, let us define the following challenge set:

$$\text{ChSet} := \{c \in R \mid \|c\|_\infty = 1 \text{ and } \|c\| = \sqrt{46}\}. \quad (11)$$

Hence, ChSet consists of elements in R with $-1/0/1$ coefficients that have exactly 46 non-zero coefficients. The size of this set is $\binom{n}{46} \cdot 2^{46}$, which for $n = 512$ is greater than 2^{265} .

¹¹ This can be proven similarly as in [5] by putting a box of side-length 1 centered on every integer point and checking that the ball is completely covered by these boxes.

¹² For readers not familiar with definitions of lossy and canonical identification schemes, we provide all necessary background in [20].

KEY GENERATION. The key generation starts with choosing a random 256-bit seed ρ and expanding into a matrix $\mathbf{A} \in R_q^{k \times \ell}$ by an extendable output function **Sam**, i.e. a function on bit strings in which the output can be extended to any desired length, modeled as a random oracle. The secret keys $(\mathbf{s}_1, \mathbf{s}_2) \in S_\eta^\ell \times S_\eta^k$ have uniformly random coefficients between $-\eta$ and η (inclusively). The value $\mathbf{t} = \mathbf{A}\mathbf{s}_1 + \mathbf{s}_2$ is then computed. The public key needed for verification is (ρ, \mathbf{t}) and the secret key is $(\rho, \mathbf{s}_1, \mathbf{s}_2)$.

PROTOCOL EXECUTION. The prover starts the identification protocol by reconstructing \mathbf{A} from the random seed ρ . The next step has the prover sample $\mathbf{y} \leftarrow S_{\gamma'-1}^\ell$ and then compute $\mathbf{w} = \mathbf{A}\mathbf{y}$. He then writes $\mathbf{w} = 2\gamma \cdot \mathbf{w}_1 + \mathbf{w}_0$, with \mathbf{w}_0 between $-\gamma$ and γ (inclusively), and then sends \mathbf{w}_1 to the verifier.

The set **ChSet** is defined as in Equation (11), and $\mathbf{ZSet} = S_{\gamma'-\beta-1}^\ell \times \{0, 1\}^k$. The set of commitments **WSet** is defined as $\mathbf{WSet} = \{\mathbf{w}_1 : \exists \mathbf{y} \in S_{\gamma'-1}^\ell \text{ s.t. } \mathbf{w}_1 = \text{HighBits}_q(\mathbf{A}\mathbf{y}, 2\gamma)\}$.

The verifier generates a random challenge $c \leftarrow \mathbf{ChSet}$ and sends it to the prover. The prover computes $\mathbf{z} = \mathbf{y} + c\mathbf{s}$. If $\mathbf{z} \notin S_{\gamma'-\beta-1}^\ell$, then the prover sets his response to \perp . He also replies with \perp if $\text{LowBits}_q(\mathbf{w} - c\mathbf{s}_2, 2\gamma) \notin S_{\gamma-\beta-1}^k$. Eventually, the verifier checks whether $\|\mathbf{z}\|_\infty < \gamma' - \beta$ and that $\mathbf{A}\mathbf{z} = c\mathbf{t}$.

4.2 Security Analysis

We omit proofs of correctness and non-abort honest verifier zero-knowledge properties since they have already been analysed in the previous works [4, 9, 11, 2]. Instead, we focus on lossiness, min entropy and computational unique response. We recall that sets W_i are introduced in Section 3.3.

Lemma 4.1. *If $\beta \geq \max_{s \in S_\eta, c \in \mathbf{ChSet}} \|cs\|_\infty$, then ID is perfectly naHVZK and has correctness error $\nu \approx 1 - \exp(-\beta n \cdot (k/\gamma + \ell/\gamma'))$.*

<u>I</u> Gen(par)	<u>P</u> ₁ (sk)
01 $\rho \leftarrow \{0, 1\}^{256}$	08 $\mathbf{A} \leftarrow R_q^{k \times \ell} := \text{Sam}(\rho)$
02 $\mathbf{A} \leftarrow R_q^{k \times \ell} := \text{Sam}(\rho)$	09 $\mathbf{y} \leftarrow S_{\gamma'-1}^\ell$
03 $(\mathbf{s}_1, \mathbf{s}_2) \leftarrow S_\eta^\ell \times S_\eta^k$	10 $\mathbf{w} := \mathbf{A}\mathbf{y}$
04 $\mathbf{t} := \mathbf{A}\mathbf{s}_1 + \mathbf{s}_2$	11 $\mathbf{w}_1 := \text{HighBits}_q(\mathbf{w}, 2\gamma)$
05 $pk = (\rho, \mathbf{t})$	12 return ($W = \mathbf{w}_1, St = (\mathbf{w}, \mathbf{y})$)
06 $sk = (\rho, \mathbf{s}_1, \mathbf{s}_2)$	
07 return (pk, sk)	<u>P</u> ₂ (sk, $W = \mathbf{w}_1, c, St = (\mathbf{w}, \mathbf{y})$)
	13 $\mathbf{z} := \mathbf{y} + c\mathbf{s}_1$
	14 if $\ \mathbf{z}\ _\infty \geq \gamma' - \beta$ or $\ \text{LowBits}_q(\mathbf{w} - c\mathbf{s}_2, 2\gamma)\ _\infty \geq \gamma - \beta$
	15 then $\mathbf{z} := \perp$
	16 else return $Z = \mathbf{z}$
<u>V</u> (pk, $W = \mathbf{w}_1, c, Z = \mathbf{z}$)	
17 return $\llbracket \ \mathbf{z}\ _\infty < \gamma' - \beta \rrbracket$ and $\llbracket \mathbf{w}_1 = \text{HighBits}_q(\mathbf{A}\mathbf{z} - c\mathbf{t}, 2\gamma) \rrbracket$	

Fig. 3. Modified Bai-Galbraith identification protocol.

LOSSYNESS. Let us consider the scheme in which the public key is generated uniformly at random (Figure 4), rather than as in IGen of Figure 3. It is enough to show that even if the prover is computationally unbounded, he only has approximately a $1/|\text{ChSet}|$ probability of making the verifier accept during each run of the identification scheme.

LossyGen(par) 01 $\rho \leftarrow \{0, 1\}^{256}; \mathbf{A} \leftarrow R_q^{k \times \ell} := \text{Sam}(\rho)$ 02 $\mathbf{t} \leftarrow R_q^k$ 03 return $pk = (\rho, \mathbf{t})$

Fig. 4. The lossy instance generator LossyGen.

Since the output of LossyGen is uniformly random over $R_q^{k \times \ell} \times R_q^k$ and the output of IGen in Figure 3 is $(\mathbf{A}, \mathbf{A}\mathbf{s}_1 + \mathbf{s}_2)$ where $\mathbf{A} \leftarrow R_q^{k \times \ell}$ and $(\mathbf{s}_1, \mathbf{s}_2) \leftarrow S_\eta^\ell \times S_\eta^k$, we get that

$$\text{Adv}_{\text{ID}}^{\text{LOSS}}(\mathbf{A}) = \text{Adv}_{k, \ell, D}^{\text{MLWE}}(\mathbf{A}),$$

where D is the uniform distribution over S_η .

Lemma 4.2. *Let e_ℓ be the largest integer which satisfies $q^{e_\ell/d} \leq 2\sqrt{46}$. Then, ID has ε_{Is} -lossy soundness, where*

$$\varepsilon_{\text{Is}} \leq \frac{1}{|\text{ChSet}|} + \frac{|S_{2(\gamma' - \beta - 1)}|^\ell \cdot |S_{4\gamma + 2}|^k \cdot |\text{ChSet}|^2}{q^{nk}} + \sum_{i=1}^{e_\ell} \frac{\binom{e_\ell}{i} \cdot |S_{2(\gamma' - \beta - 1) + \|W_i\|_\infty}|^\ell \cdot |S_{4\gamma + 2 + \|W_i\|_\infty}|^k \cdot |\text{ChSet}|^2}{|W_i|^{\ell + k} \cdot q^{nk(1 - i/d)}}. \quad (12)$$

Proof. Consider an unbounded adversary \mathbf{C} that is executed in game LOSSY-IMP of Figure 5.

GAME LOSSY-IMP: 01 $pk_{\text{Is}} := (\rho, \mathbf{t}) \leftarrow \text{LossyGen}(\text{par})$ 02 $(\mathbf{w}_1, St) \leftarrow \mathbf{C}(pk_{\text{Is}})$ 03 $c \leftarrow \text{ChSet}$ 04 $\mathbf{z} \leftarrow \mathbf{C}(St, c)$ 05 return $\llbracket \mathbf{w}_1 = \text{HighBits}_q(\mathbf{A}\mathbf{z} - ct, 2\gamma) \rrbracket$ and $\llbracket \ \mathbf{z}\ _\infty < \gamma' - \beta \rrbracket$

Fig. 5. The lossy impersonation game LOSSY-IMP.

Assume that for some \mathbf{w}_1 , there exist two $c \neq c' \in \text{ChSet}$ and two \mathbf{z}, \mathbf{z}' that lead to C winning, i.e. $\|\mathbf{z}\|_\infty, \|\mathbf{z}'\|_\infty < \gamma' - \beta$ and

$$\begin{aligned}\mathbf{w}_1 &= \text{HighBits}_q(\mathbf{A}\mathbf{z} - \mathbf{t}c, 2\gamma), \\ \mathbf{w}_1 &= \text{HighBits}_q(\mathbf{A}\mathbf{z}' - \mathbf{t}c', 2\gamma).\end{aligned}$$

By Lemma 2.1, we know that this implies

$$\begin{aligned}\|\mathbf{A}\mathbf{z} - \mathbf{t}c - \mathbf{w}_1 \cdot 2\gamma\|_\infty &\leq 2\gamma + 1, \\ \|\mathbf{A}\mathbf{z}' - \mathbf{t}c' - \mathbf{w}_1 \cdot 2\gamma\|_\infty &\leq 2\gamma + 1.\end{aligned}$$

By the triangle inequality, we have that

$$\|\mathbf{A}(\mathbf{z} - \mathbf{z}') - \mathbf{t} \cdot (c - c')\|_\infty \leq 4\gamma + 2,$$

which can be rewritten as

$$\mathbf{A}(\mathbf{z} - \mathbf{z}') + \mathbf{u} = \mathbf{t} \cdot (c - c') \quad (13)$$

for some \mathbf{u} such that $\|\mathbf{u}\|_\infty \leq 4\gamma + 2$ (and $\|\mathbf{z} - \mathbf{z}'\|_\infty \leq 2(\gamma' - \beta - 1)$).

If $\mathbf{A} \leftarrow R_q^{k \times \ell}$ and $\mathbf{t} \leftarrow R_q^k$, then, by Theorem 3.8, we have that Equation (13) is satisfied with probability less than

$$\frac{|S_{2(\gamma' - \beta - 1)}|^\ell \cdot |S_{4\gamma + 2}|^k \cdot |\mathcal{D}|}{q^{nk}} + \sum_{i=1}^{e_\ell} \frac{\binom{e_\ell}{i} \cdot |S_{2(\gamma' - \beta - 1) + \|W_i\|_\infty}|^\ell \cdot |S_{4\gamma + 2 + \|W_i\|_\infty}|^k \cdot |\mathcal{D}|}{|W_i|^{\ell + k} \cdot q^{nk(1 - i/d)}},$$

where $\mathcal{D} := \{c - c' : c, c' \in \text{ChSet}\} \setminus \{0\}$ and sets W_i 's are defined in Section 3.3.

Thus, except with the above probability, for every \mathbf{w}_1 , there is at most one possible c that allows C to win. In other words, except with the above probability, C has at most a $1/|\text{ChSet}|$ chance of winning. \square

Note that we do not make any assumptions on the prime q . However, small d (e.g. $d = 2$ for $q \equiv 3$ or $5 \pmod{8}$) implies small e_ℓ . As a consequence, the smaller d we choose, then the probability above also decreases.

MIN-ENTROPY. Now, we prove that the \mathbf{w}_1 sent by the honest prover in the first step is extremely likely to be distinct for every run of the protocol.

Lemma 4.3. *Let e_m be the largest integer which satisfies $q^{e_m/d} \leq 2\gamma' \sqrt{n}$. Then the identification scheme ID in Figure 3 has*

$$\alpha > \log \left(\min \left\{ \frac{1}{M}, (2\gamma' - 1)^{n^\ell} \right\} \right)$$

bits of min-entropy, where

$$M := \frac{|S_{2\gamma'}|^\ell \cdot |S_{2\gamma}|^k}{q^{nk}} + \sum_{i=1}^{e_m} \frac{\binom{d}{i} \cdot |S_{2\gamma' + \|W_i\|_\infty}|^\ell \cdot |S_{2\gamma + \|W_i\|_\infty}|^k}{|W_i|^{\ell + k} \cdot q^{nk(1 - i/d)}}.$$

Proof. We claim that

$$\begin{aligned} & \Pr_{\mathbf{A} \leftarrow R_q^{k \times \ell}} [\exists \mathbf{y} \neq \mathbf{y}' \in S_{\gamma'-1}^\ell \text{ s.t. } \text{HighBits}_q(\mathbf{A}\mathbf{y}, 2\gamma) = \text{HighBits}_q(\mathbf{A}\mathbf{y}', 2\gamma)] \\ & \leq \frac{|S_{2\gamma'}|^\ell \cdot |S_{2\gamma}|^k}{q^{nk}} + \sum_{i=1}^{e_m} \frac{\binom{d}{i} \cdot |S_{2\gamma'+\|W_i\|_\infty}|^\ell \cdot |S_{2\gamma+\|W_i\|_\infty}|^k}{|W_i|^{\ell+k} \cdot q^{nk(1-i/d)}}. \end{aligned} \quad (14)$$

Indeed, if we write

$$\text{Decompose}_q(\mathbf{A}\mathbf{y}, 2\gamma) = (\mathbf{w}_1, \mathbf{w}_0) \text{ and } \text{Decompose}_q(\mathbf{A}\mathbf{y}', 2\gamma) = (\mathbf{w}'_1, \mathbf{w}'_0),$$

then $\text{HighBits}_q(\mathbf{A}\mathbf{y}, 2\gamma) = \text{HighBits}_q(\mathbf{A}\mathbf{y}', 2\gamma)$ implies that $\mathbf{A}\mathbf{y} = \mathbf{w}_1 \cdot 2\gamma + \mathbf{w}_0$ and $\mathbf{A}\mathbf{y}' = \mathbf{w}'_1 \cdot 2\gamma + \mathbf{w}'_0$ with $\mathbf{w}_1 = \mathbf{w}'_1$ and $\|\mathbf{w}_0\|_\infty, \|\mathbf{w}'_0\|_\infty \leq \gamma$. Hence,

$$\mathbf{A}(\mathbf{y} - \mathbf{y}') - (\mathbf{w}_0 - \mathbf{w}'_0) = \mathbf{0} \quad (15)$$

where

$$\|\mathbf{y} - \mathbf{y}'\|_\infty < 2\gamma', \|\mathbf{w}_0 - \mathbf{w}'_0\|_\infty \leq 2\gamma.$$

Corollary 3.9 shows that the probability over the choice of $\mathbf{A} \leftarrow R_q^{k \times \ell}$, that there exist two non-zero elements of norm less than 2γ and $2\gamma'$, respectively, which satisfy Equation (15) is at most

$$\frac{|S_{2\gamma'}|^\ell \cdot |S_{2\gamma}|^k}{q^{nk}} + \sum_{i=1}^{e_m} \frac{\binom{d}{i} \cdot |S_{2\gamma'+\|W_i\|_\infty}|^\ell \cdot |S_{2\gamma+\|W_i\|_\infty}|^k}{|W_i|^{\ell+k} \cdot q^{nk(1-i/d)}} = M.$$

This proves Equation (14).

Now, we know that with probability at least $1-M$ over the choice of $\mathbf{A} \leftarrow R_q^{k \times \ell}$, each $W = \text{HighBits}_q(\mathbf{A}\mathbf{y}, 2\gamma)$ has exactly a $\frac{1}{|S_{\gamma'-1}^\ell|} = (2\gamma' - 1)^{-n\ell}$ probability of being output. Thus, the claim in the lemma follows directly from the definition. \square

COMPUTATIONAL UNIQUE RESPONSE. Here, we show the Computational Unique Response (CUR) property required for strong-unforgeability of the signature scheme.

Lemma 4.4. *Let e_c be the largest integer such that $q^{e_c/d} \leq 2(\gamma' - \beta)\sqrt{n}$. Then*

$$\text{Adv}_{\text{ID}}^{\text{CUR}}(\mathbf{A}) \leq \frac{|S_{2(\gamma'-\beta)}|^\ell \cdot |S_{4\gamma+2}|^k}{q^{nk}} + \sum_{i=1}^{e_c} \frac{\binom{d}{i} \cdot |S_{2(\gamma'-\beta)+\|W_i\|_\infty}|^\ell \cdot |S_{4\gamma+2+\|W_i\|_\infty}|^k}{|W_i|^{\ell+k} \cdot q^{nk(1-i/d)}}$$

for all (even unbounded) adversaries \mathbf{A} .

Proof. Let $(W, c, Z) = (\mathbf{w}_1, c, \mathbf{z})$ be any valid transcript and suppose \mathbf{A} is able to generate a valid $Z' = \mathbf{z}' \neq Z$ such that $\mathbb{V}(pk = (\mathbf{A}, \mathbf{t}), \mathbf{w}_1, c, \mathbf{z}') = 1$. Thus, we have

$$\mathbf{w}_1 = \text{UseHint}_q(\mathbf{h}, \mathbf{A}\mathbf{z} - ct, 2\gamma) \text{ and } \mathbf{w}_1 = \text{UseHint}_q(\mathbf{h}', \mathbf{A}\mathbf{z}' - ct, 2\gamma).$$

q	d	γ
$2^{44} - 17043$	2	592493
$2^{44} - 8583$	4	593431
$2^{44} - 13743$	8	305156
$2^{44} - 7583$	16	282832
$2^{44} - 1599$	32	285978
$2^{45} - 36991$	64	364254
$2^{45} - 58111$	128	353952
$2^{45} - 511$	256	360620
$2^{45} - 23551$	512	359769

Table 1. Prime moduli q for each possible value of d . We used the main result of [19] for finding q . For each case, we also provide values γ such that $2\gamma|q - 1$. Just like in [11], we set $\gamma' = \gamma$.

The above two equations imply (by Lemma 2.1) that

$$\|\mathbf{A}\mathbf{z} - \mathbf{c}\mathbf{t} - \mathbf{w}_1 \cdot 2\gamma\|_\infty \leq 2\gamma + 1 \text{ and } \|\mathbf{A}\mathbf{z}' - \mathbf{c}\mathbf{t} - \mathbf{w}_1 \cdot 2\gamma\|_\infty \leq 2\gamma + 1.$$

By the triangle inequality, we have

$$\mathbf{A}(\mathbf{z} - \mathbf{z}') + \mathbf{u} = \mathbf{0}$$

for some \mathbf{u} such that $\|\mathbf{u}\| \leq 4\gamma + 2$ and $\|\mathbf{z} - \mathbf{z}'\| < 2(\gamma' - \beta)$. Hence, by Corollary 3.9, the probability over the choice of $\mathbf{A} \leftarrow R_q^{k \times \ell}$, that there exist such \mathbf{v}, \mathbf{u} is at most

$$\frac{|S_{2(\gamma' - \beta)}|^\ell \cdot |S_{4\gamma + 2}|^k}{q^{nk}} + \sum_{i=1}^{e_c} \frac{\binom{d}{i} \cdot |S_{2(\gamma' - \beta) + \|W_i\|_\infty}|^\ell \cdot |S_{4\gamma + 2 + \|W_i\|_\infty}|^k}{|W_i|^{\ell + k} \cdot q^{nk(1 - i/d)}}.$$

□

4.3 Concrete Parameteres

In this subsection, we instantiate the modified Bai-Galbraith mBG signature scheme obtained by the Fiat-Shamir transformation from ID with concrete parameters (Table 1 and Table 2). We consider nine different instantiations of mBG for all possible $d \in \{2^i : i \in [9]\}$.

For each value of d , we have selected parameters (e.g. prime modulus q and γ) such that the ID scheme satisfies the following security properties: (i) $\varepsilon_{zk} = 0$, (ii) the scheme has more than 2845 bits of min-entropy, i.e. $\alpha > 2845$, (iii) $\varepsilon_{\text{IS}} \leq 2^{-264}$, (iv) $\text{Adv}_{\text{ID}}^{\text{CUR}}(\mathbf{C}) \leq 2^{-288}$. Following the steps in [11], one can prove security of the modified Bai-Galbraith scheme in the quantum random oracle model (see [20]).

We compare the nine different instantiations of the modified Bai-Galbraith scheme (Table 2) with respect to recommended parameters in Table 2. Firstly,

d	2	4	8	16	32	64	128	256	512
n	512	512	512	512	512	512	512	512	512
(k, ℓ) (dimensions of \mathbf{A})	(4, 4)	(4, 4)	(5, 5)	(5, 5)	(5, 5)	(5, 5)	(5, 5)	(5, 5)	(5, 5)
# of ± 1 's in $c \in \text{ChSet}$	46	46	46	46	46	46	46	46	46
η (max. coeff. of $\mathbf{s}_1, \mathbf{s}_2$)	5	5	2	2	2	2	2	2	2
$\beta (= \eta \cdot (\# \text{ of } 1\text{'s in } c))$	230	230	92	92	92	92	92	92	92
e_ℓ (lossyness)	0	0	0	1	2	5	10	21	42
e_c (CUR)	1	2	4	8	17	34	68	136	272
e_m (min-entropy)	1	2	4	8	17	34	68	136	272
$\log(\varepsilon_{\text{Is}})$	-264	-264	-264	-264	-264	-264	-264	-264	-264
$\log(\text{Adv}_{\text{ID}}^{\text{CUR}}(\mathbf{A}))$	-1326	-1317	-592	-924	-288	-799	-986	-766	-677
α	3373	3363	3149	3481	2845	3356	3543	3324	3235
pk size (kilobytes)	11.29	11.29	14.11	14.11	14.11	14.43	14.43	14.43	14.43
sig size (kilobytes)	5.69	5.69	6.76	6.76	6.76	6.76	6.76	6.76	6.76
Exp. Repeats $\frac{1}{1-\nu}$	4.94	4.93	4.68	5.29	5.19	3.64	3.78	3.69	3.70
BKZ block-size to break LWE	480	480	600	600	600	585	585	585	585
Best known classical bit-cost	140	140	175	175	175	171	171	171	171
Best known quantum bit-cost	127	127	159	159	159	155	155	155	155

Table 2. Parameters for the modified Bai-Galbraith scheme. Recall that ν is the maximum coefficient of secret keys $\mathbf{s}_1, \mathbf{s}_2$ and $\beta = \nu \cdot (\# \text{ of } \pm 1\text{'s in } c \in \text{ChSet})$. On the other hand, variables $e_\ell, e_c, e_m, \alpha, \varepsilon_{\text{Is}}, \text{Adv}_{\text{ID}}^{\text{CUR}}(\mathbf{A}), \nu$ are defined in Section 4.2.

observe that for $d \leq 4$, we pick $q \approx 2^{44}$. In this case, we end up with public key and signature size 11.29kB and 5.69kB respectively.

The situation changes for $d = 8$. Interestingly, if one keeps the same parameters as for $d = 4$ then one still gets $\varepsilon_{\text{Is}} \leq 2^{-264}$, hence the lossyness property is still preserved. The problem is, however, that the advantage $\text{Adv}_{\text{ID}}^{\text{CUR}}(\mathbf{A})$ gets extremely big. Concretely, for parameters above we have $\log(\text{Adv}_{\text{ID}}^{\text{CUR}}(\mathbf{A})) \approx 3483$. We found out that one of the compounds in the sum is actually dominating (see Lemma 4.4). Namely, we get:

$$\log\left(\frac{\binom{8}{1} \cdot |S_{2(\gamma'-\beta)+\|W_1\|_\infty}|^\ell \cdot |S_{4\gamma+2+\|W_1\|_\infty}|^k}{|W_1|^{\ell+k} \cdot q^{nk(1-1/8)}}\right) \approx 3483.$$

We believe the reason for it being so large is because for $d = 8$, $i = 1$ and $q \approx 2^{44}$ we have $t := \left\lfloor \frac{q^{i/d}}{2\sqrt{n}} \right\rfloor = 1$ (introduced in Section 3.3). Hence, W_1 has only 3^{512} elements. As a consequence, the value above is still big. Thus, a natural way to solve this issue would be to increase q . Unfortunately, in order to keep the MLWE problem hard, this would imply increasing the size of secret keys, i.e. η . Hence, β would also get bigger, so in order to keep the repetition rate $1/(1-\nu)$ small, we would have to increase the value of γ (and γ'). In this case, probabilities related to the security of ID, e.g. $\varepsilon_{\text{is}}, \log(\text{Adv}_{\text{ID}}^{\text{CUR}}(\mathbf{A}))$, would get considerably bigger, so one would need to consider larger q again and eventually, we would end up in a vicious circle. We avoid that by increasing dimensions $(k, \ell) = (5, 5)$ of the matrix \mathbf{A} . Unfortunately, this comes at a price of larger public key (14.11kB) and signature (6.76kB) sizes. In order to minimise such costs, we decrease the size of secret keys $\eta = 2$ and thus, we select smaller values for γ . As before, we choose $q \approx 2^{44}$. We pick almost identical parameters for $d = 16$ and $d = 32$.

Next, we consider $d \geq 64$. If we choose the parameters as for $d = 32$ then the lossiness probability ε_{is} is no longer small and therefore, we need to increase the $q \approx 2^{45}$. We observe that the new parameters still provide much more than 128 bits of security for MLWE. The public key gets slightly larger (14.43kB) and the signature size stays the same as before.

In order to maintain security of the Bai-Galbraith scheme in the quantum random oracle model for bigger d (i.e. $d \geq 256$), we need to increase both dimensions (k, ℓ) of the matrix \mathbf{A} as well as the prime modulus q . This results in having 3.13kB larger public key and 1.07kB signature sizes than for $d = 2$. We remark that security parameters were chosen such that the expected number of repetitions of the protocol $1/(1-\nu)$ is at most six. Indeed, admitting small repetition rate as well as supporting the use of the Number Theoretic Transform, efficient caching and polynomial sampling assures us that the protocol can be performed very efficiently.

Acknowledgments

The author would like to thank Vadim Lyubashevsky for fruitful discussions and anonymous reviewers for their useful comments. This work was supported by the SNSF ERC Transfer Grant CRETP2-166734 FELICITY.

References

1. Abdalla, M., Fouque, P.A., Lyubashevsky, V., Tibouchi, M.: Tightly-secure signatures from lossy identification schemes. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 572–590. Springer, Heidelberg (Apr 2012)
2. Alkim, E., Bindel, N., Buchmann, J.A., Dagdelen, Ö., Eaton, E., Gutoski, G., Krämer, J., Pawlega, F.: Revisiting TESLA in the quantum random oracle model. In: Post-Quantum Cryptography - 8th International Workshop, PQCrypto 2017, Utrecht, The Netherlands, June 26-28, 2017, Proceedings. pp. 143–162 (2017)

3. Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P.: Post-quantum key exchange - A new hope. In: Holz, T., Savage, S. (eds.) USENIX Security 2016. pp. 327–343. USENIX Association (Aug 2016)
4. Bai, S., Galbraith, S.D.: An improved compression technique for signatures based on learning with errors. In: Benaloh, J. (ed.) CT-RSA 2014. LNCS, vol. 8366, pp. 28–47. Springer, Heidelberg (Feb 2014)
5. Baum, C., Damgård, I., Lyubashevsky, V., Oechsner, S., Peikert, C.: More efficient commitments from structured lattice assumptions. In: Catalano, D., De Prisco, R. (eds.) SCN 18. LNCS, vol. 11035, pp. 368–385. Springer, Heidelberg (Sep 2018)
6. Benhamouda, F., Camenisch, J., Krenn, S., Lyubashevsky, V., Neven, G.: Better zero-knowledge proofs for lattice encryption and their application to group signatures. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014, Part I. LNCS, vol. 8873, pp. 551–572. Springer, Heidelberg (Dec 2014)
7. Benhamouda, F., Krenn, S., Lyubashevsky, V., Pietrzak, K.: Efficient zero-knowledge proofs for commitments from learning with errors over rings. In: Pernul, G., Ryan, P.Y.A., Weippl, E.R. (eds.) ESORICS 2015, Part I. LNCS, vol. 9326, pp. 305–325. Springer, Heidelberg (Sep 2015)
8. Bindel, N., Akleylek, S., Alkim, E., Barreto, P.S.L.M., Buchmann, J., Eaton, E., Gutoski, G., Kramer, J., Longa, P., Polat, H., Ricardini, J.E., Zanon, G.: qtesla. Tech. rep., National Institute of Standards and Technology (2017), available at <https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions>
9. Ducas, L., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., Stehlé, D.: CRYSTALS - Dilithium: Digital signatures from module lattices. IACR Cryptology ePrint Archive 2017, 633 (2017), to appear in TCHES 2018
10. Güneysu, T., Lyubashevsky, V., Pöppelmann, T.: Practical lattice-based cryptography: A signature scheme for embedded systems. In: Prouff, E., Schaumont, P. (eds.) CHES 2012. LNCS, vol. 7428, pp. 530–547. Springer, Heidelberg (Sep 2012)
11. Kiltz, E., Lyubashevsky, V., Schaffner, C.: A concrete treatment of Fiat-Shamir signatures in the quantum random-oracle model. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018, Part III. LNCS, vol. 10822, pp. 552–586. Springer, Heidelberg (Apr / May 2018)
12. Langlois, A., Stehlé, D.: Worst-case to average-case reductions for module lattices. Des. Codes Cryptography 75(3), 565–599 (2015)
13. Lyubashevsky, V.: Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 598–616. Springer, Heidelberg (Dec 2009)
14. Lyubashevsky, V.: Lattice signatures without trapdoors. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 738–755. Springer, Heidelberg (Apr 2012)
15. Lyubashevsky, V., Ducas, L., Kiltz, E., Lepoint, T., Schwabe, P., Seiler, G., Stehlé, D.: Crystals-dilithium. Tech. rep., National Institute of Standards and Technology (2017), available at <https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions>
16. Lyubashevsky, V., Micciancio, D.: Generalized compact Knapsacks are collision resistant. In: Bugliesi, M., Preneel, B., Sassone, V., Wegener, I. (eds.) ICALP 2006, Part II. LNCS, vol. 4052, pp. 144–155. Springer, Heidelberg (Jul 2006)
17. Lyubashevsky, V., Neven, G.: One-shot verifiable encryption from lattices. In: Coron, J., Nielsen, J.B. (eds.) EUROCRYPT 2017, Part I. LNCS, vol. 10210, pp. 293–323. Springer, Heidelberg (Apr / May 2017)

18. Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 1–23. Springer, Heidelberg (May / Jun 2010)
19. Lyubashevsky, V., Seiler, G.: Short, invertible elements in partially splitting cyclotomic rings and applications to lattice-based zero-knowledge proofs. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018, Part I. LNCS, vol. 10820, pp. 204–224. Springer, Heidelberg (Apr / May 2018)
20. Nguyen, N.K.: On the non-existence of short vectors in random module lattices. Cryptology ePrint Archive, Report 2019/973 (2019), <https://eprint.iacr.org/2019/973>
21. Peikert, C., Rosen, A.: Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In: Halevi, S., Rabin, T. (eds.) TCC 2006. LNCS, vol. 3876, pp. 145–166. Springer, Heidelberg (Mar 2006)
22. Peikert, C., Rosen, A.: Lattices that admit logarithmic worst-case to average-case connection factors. In: Johnson, D.S., Feige, U. (eds.) 39th ACM STOC. pp. 478–487. ACM Press (Jun 2007)
23. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: Gabow, H.N., Fagin, R. (eds.) 37th ACM STOC. pp. 84–93. ACM Press (May 2005)
24. Schwabe, P., Avanzi, R., Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Seiler, G., Stehlé, D.: Crystals-kyber. Tech. rep., National Institute of Standards and Technology (2017), available at <https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions>
25. Stehlé, D., Steinfeld, R.: Making NTRUEncrypt and NTRUSign as secure as standard worst-case problems over ideal lattices. Cryptology ePrint Archive, Report 2013/004 (2013), <http://eprint.iacr.org/2013/004>
26. Stehlé, D., Steinfeld, R., Tanaka, K., Xagawa, K.: Efficient public key encryption based on ideal lattices. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 617–635. Springer, Heidelberg (Dec 2009)
27. Unruh, D.: Post-quantum security of Fiat-Shamir. In: Takagi, T., Peyrin, T. (eds.) ASIACRYPT 2017, Part I. LNCS, vol. 10624, pp. 65–95. Springer, Heidelberg (Dec 2017)