Research Article

Gabrielle De Micheli*, Nadia Heninger, and Barak Shani

Characterizing overstretched NTRU attacks

<https://doi.org/10.1515/jmc-2015-0055>

Received Feb 05, 2020; accepted Feb 12, 2020

Abstract: Overstretched NTRU is a variant of NTRU with a large modulus. Recent lattice subfield and subring attacks have broken suggested parameters for several schemes. There are a number of conflicting claims in the literature over which attack has the best performance. These claims are typically based on experiments more than analysis. In this paper, we argue that comparisons should focus on the lattice dimension used in the attack. We give evidence, both analytically and experimentally, that the subring attack finds shorter vectors and thus is expected to succeed with a smaller dimension lattice than the subfield attack for the same problem parameters, and also to succeed with a smaller modulus when the lattice dimension is fixed.

Keywords: Overstretched NTRU, subfield attack, subring attack

2010 Mathematics Subject Classification: Primary 11T71

1 Introduction

NTRU is a public key cryptosystem [11] that serves as a basis for many cryptographic protocols (e.g. [9, 10, 14]) and is believed to remain secure in the presence of quantum computers. See the survey [23] for a complete description of the NTRU cryptosystem and its applications. In this paper, we consider the *overstretched* NTRU variant in the cyclotomic field $K = \mathbb{Q}[x]/(x^n + 1)$, with n a power of 2. Let $R = \mathbb{Z}[x]/(x^n + 1)$ be the ring of integers in K , and let $R_q = \mathbb{Z}_q[x]/(x^n + 1)$ for some integer q that is super-polynomial in n . The private key consists of two polynomials $\mathbf{f}, \mathbf{g} \in R_q$, with $\mathbf{f}$ invertible. The public key $\mathbf{h}$ is defined by $\mathbf{h} := \mathbf{g}\mathbf{f}^{-1}$. The coefficients of $\mathbf{f}$ and $\mathbf{g}$ are chosen to be small from a given distribution, most commonly the uniform distribution over $\{-1, 0, 1\}$. The (general) NTRU key recovery problem is to recover $\mathbf{a}, \mathbf{b} \in R_q$ with “sufficiently small” coefficients such that $\mathbf{h} = \mathbf{b}\mathbf{a}^{-1}$.

Cryptanalyses of NTRU. Coppersmith and Shamir [5] presented a lattice attack on NTRU. The lattice has dimension $2n$, and in the context of this paper the attack works over the full field K . Later variants of this attack decrease the lattice dimension, resulting in feasible computations for larger parameters. The first cryptanalyses of overstretched NTRU were given independently by Albrecht et al. [1] and Cheon et al. [4]. These works present *subfield attacks* that exploit subfields in K . Their main result is that if q is exponentially large, the dimension can be much smaller and the attack runs in polynomial time.

Kirchner and Fouque [12] presented a *subring attack* against overstretched NTRU. This attack allows more flexibility in choosing different (larger) dimensions. Moreover, they proved that despite the larger dimension, the “full field” attack does not perform worse than the subfield and subring attacks.

Experimentally, the subring and subfield attacks are significantly faster than the full field attack. [12] compare to the experiments in [1] and conclude that if one wishes to minimize the ratio between n and q then the subring attack “performs better” than the subfield attack. Subsequent work by Duong et al. [8] conclude that

*Corresponding Author: Gabrielle De Micheli: University of Pennsylvania, United States of America; Email: gmicheli@seas.upenn.edu

Nadia Heninger: University of Pennsylvania, United States of America; Email: nadiah@seas.upenn.edu

Barak Shani: University of Pennsylvania, United States of America; Email: baraksh@seas.upenn.edu

for different choices of subfields, the subfield attack is not worse than the subring attack. These comparisons are mainly experimental and not analytic.

However, these works directly compare lattices of different dimensions and observe that the attack succeeds on a smaller modulus q for a given degree n using larger-dimension lattices. The benefit of this comparison is questionable, as it follows from [12] that the full field, which has the largest dimension, is expected to achieve the lowest ratio between n and q among all these lattice attacks. Furthermore, the point of the subfield and subring attacks is to decrease the dimension, so increasing the dimension is in opposition to the goal of the attack construction. While lattice dimension is not the only parameter that affects the running time or approximation factor of lattice basis reduction algorithms, in all of our experiments, as in the reported experiments of previous works, lattice dimension seems to play a crucial role in the actual running time.

Our results. The main goal of our work is to resolve the conflicting claims in previous work. We formally analyze the relative performance, focusing on the lattice dimension and use experiments to validate our analysis. Our focus on the lattice dimension follows our claim that this is the correct metric for comparison.

1. We formally justify the projection technique of May [17] and May and Silverman [18], which is key to the subring attack. We formalize its necessary conditions, and explain its relation to standard assumptions on NTRU. This analysis fills a theoretical gap in prior work on the subring attack.
2. We show that the subring lattice is expected to contain shorter vectors than the subfield lattice, which resolves the incompatible claims in prior work. In short, if this is the case, for fixed n and q , the subring attack can use projection to discard more equations and obtain a lower dimension lattice. Thus, for a given degree n and fixed lattice dimension, the subring attack is expected to succeed on a smaller modulus q .

Main Result (Informal). *Consider the NTRU problem with polynomial degree n . Let L be a subfield of K such that $[K : L] = r$, and let $n' = n/r$. Then, for sufficiently large n , we have the following.*

1. *For a lattice dimension $2n'$, the subring lattice is expected to contain shorter vectors than the subfield lattice, and to solve the NTRU problem for smaller modulus. The ratio of the Euclidean norm of the respective vectors is approximately $\sqrt{2r/(r+1)}$. If these are the shortest vectors, then the ratio of the smallest feasible moduli for each attack approaches 2 as r increases.*
2. *For a modulus q , if we decrease the lattice dimension below $2n'$ using projection, the subring attack is expected to solve the NTRU problem with a smaller dimension lattice and a smaller block size for the BKZ algorithm than the subfield attack, by finding a non-zero integral multiple of the desired vectors.*

Our analysis does not show that these desired vectors are the shortest vectors in the corresponding lattices. Thus, our bounds may not be tight. We present experimental evidence suggesting that these bounds are conservative. Our result focuses on the structure of the lattices more than actual implementations of the attacks. In particular, we fix the subfield index and analyze the asymptotics of the length of short vectors in the lattices. Implementations of the attacks would try to optimize the choice of the subfield with respect to the degree of the field. An analysis of such an optimization seems challenging.

2 Preliminaries

We denote the ring representation of an element by $\mathbf{a} \in R$, and the vector representation by $a \in \mathbb{Z}_q^n$. The Euclidean norm $\|\mathbf{f}\|$ is the norm of the corresponding vector consisting of the polynomial coefficients, i.e. $\|f\|$. We use $[x]_q$ to denote $x \bmod q$.

A *number field* is a finite field extension of $\mathbb{Q}$. Its degree is $[K : \mathbb{Q}]$. The ring of integers $\mathcal{O}$ of a number field K is the set of algebraic integers contained in K . For any field K and subfield L of K , we define $r = [K : L]$ to be the index of the subfield we consider. If $n' = [L : \mathbb{Q}]$ and $n = [K : \mathbb{Q}]$, then $r = n/n'$.

Let ζ_m be a primitive m^{th} root of unity. Let the m^{th} *cyclotomic field* be $K = \mathbb{Q}(\zeta_m)$, and m a power of 2. The m^{th} *cyclotomic polynomial* is $x^n + 1$, where $n = \phi(m)$ and ϕ is Euler's phi function, and $K \cong \mathbb{Q}[x]/(x^n + 1)$.

Let K be a number field and L a subfield of K . Consider the map $m_a : x \mapsto ax$, for an element $a \in K$ and $x \in L$. The trace of $a \in K$, denoted $\text{Tr}_{K/L}(a)$, is the trace of m_a . The relative norm of $a \in K$, denoted $N_{K/L}(a)$, is the determinant of m_a . The trace is additive and the norm is multiplicative. In particular, if K is a Galois extension of $\mathbb{Q}$ and we define $G = \text{Gal}(K/L)$, then $\text{Tr}_{K/L}(a) = \sum_{\sigma \in G} \sigma(a)$ and $N_{K/L}(a) = \prod_{\sigma \in G} \sigma(a)$. The embeddings $\sigma \in G$ permute or conjugate the coefficients of $x \in K$ in the canonical embedding. Hence, $\forall \sigma \in G$, $\|\sigma(x)\| = \|x\|$. Let K be a number field and L a subfield of index r . When we enumerate the embeddings, we set $\sigma_1 = \text{Id}$. To prevent confusion, while we use canonical embeddings, the norms are taken with respect to the coefficients.

A *lattice* is a discrete additive subgroup of $\mathbb{R}^n$. We will represent an n -dimensional lattice as an $n \times n$ matrix where the rows are given by the basis vectors b_i , and write $\mathcal{L}(B)$ for the lattice generated by basis matrix B .

3 Characterization of NTRU attacks

We give a short presentation of the different attacks on NTRU. A comprehensive characterization of the attacks appears in the full version of this paper [6].

3.1 The full field attack

Coppersmith and Shamir [5] considered the following $2n \times 2n$ matrix

$$A_{full} = \begin{pmatrix} \mathbf{I}_n & \mathcal{M}_{\mathbf{h}} \\ 0 & q\mathbf{I}_n \end{pmatrix},$$

where $\mathbf{I}_n$ is the n -dimensional identity matrix and $\mathcal{M}_{\mathbf{h}}$ represents multiplication in R by the public key $\mathbf{h}$. The lattice generated by A_{full} , which we call $\mathcal{L}(A_{full})$, contains the vector $(f, g) = (f_0, \dots, f_{n-1}, g_0, \dots, g_{n-1})$, because $(f_0, \dots, f_{n-1})\mathcal{M}_{\mathbf{h}} \pmod{q} \equiv (g_0, \dots, g_{n-1})$. The vector (f, g) has relatively small Euclidean norm, and is most likely a vector of the smallest non-zero length in the lattice $\mathcal{L}(A_{full})$. Thus, the NTRU problem can be reduced to computing short vectors in $\mathcal{L}(A_{full})$.

Coppersmith and Shamir [5] note that one can derive useful information to recover the secret key even when a multiple of $(\mathbf{f}, \mathbf{g})$ is found, for multiples of relatively small norm (yet larger than $(\mathbf{f}, \mathbf{g})$). See [5] for more details. In fact, one can focus on finding a small multiple of $\mathbf{f}$, since given $\alpha\mathbf{f}$, a small multiple of $\mathbf{g}$ can be found by computing $\alpha\mathbf{f}\mathbf{h} = \alpha\mathbf{g}$. The different attacks exploit this fact, and aim to recover (a small multiple of) $N_{K/L}(\mathbf{f})$, for a subfield $L \subseteq K$, which can be shown to have a relatively small Euclidean norm.

In the following descriptions, we use the term “ f part” for the part of the vector corresponding to the identity matrix, and “ g part” for the part corresponding to multiplication by $\mathbf{h}$ (or by $N_{K/L}(\mathbf{h})$ in the subfield lattice).

The subfield attacks [1, 4] The *norm* attack [1] uses the lattice generated by the rows of the $2n' \times 2n'$ matrix

$$A_{subfield} = \begin{pmatrix} \mathbf{I}_{n'} & \mathcal{M}'_{N_{K/L}(\mathbf{h})} \\ 0 & q\mathbf{I}_{n'} \end{pmatrix},$$

where n' is the degree of the subfield L and $\mathcal{M}'_{N_{K/L}(\mathbf{h})}$ is an $n' \times n'$ matrix representing multiplication by $N_{K/L}(\mathbf{h})$ in L . This lattice contains the short vector $(N_{K/L}(\mathbf{f}), N_{K/L}(\mathbf{g})) = (\prod_{\sigma \in G} \sigma(\mathbf{f}), \prod_{\sigma \in G} \sigma(\mathbf{g}))$.

In the *trace* attack [4] one replaces $\mathcal{M}_{N_{K/L}(\mathbf{h})}$ with $\mathcal{M}_{\text{Tr}_{K/L}(\mathbf{h})}$, the matrix representing multiplication by $\text{Tr}_{K/L}(\mathbf{h})$ in L . We focus on the norm attack because it performs slightly better when the polynomials are *balanced* (that is, the polynomials $\mathbf{f}$ and $\mathbf{g}$ have approximately the same number of non-zero coefficients).

The subring attack [12] The subring attack can be divided into two steps. First, consider the the following $(n' + n) \times (n' + n)$ matrix

$$A_{subring} = \begin{pmatrix} \mathbf{I}_{n'} & \mathcal{M}'_{\mathbf{h}} \\ 0 & q\mathbf{I}_n \end{pmatrix},$$

where $\mathcal{M}'_{\mathbf{h}}$ is an $n' \times n$ matrix representing multiplication by $\mathbf{h}$ in L . This lattice contains the short vector $(N_{K/L}(\mathbf{f}), N_{K/L}(\mathbf{f})\mathbf{h}) = (\mathbf{f} \prod_{\sigma \in G \setminus \{\text{Id}\}} \sigma(\mathbf{f}), \mathbf{g} \prod_{\sigma \in G \setminus \{\text{Id}\}} \sigma(\mathbf{f}))$.

The dimension $n' + n$ is larger than $2n'$, the subfield attack lattice dimension. The second step “projects” the lattice, i.e., deletes columns of $\mathcal{M}'_{\mathbf{h}}$, to reduce the dimension. We denote the projected vector $(N_{K/L}(\mathbf{f}), \overline{N_{K/L}(\mathbf{f})\mathbf{h}})$. For rigorous analysis, columns should be chosen independently. This approach offers more flexibility than the subfield attack by allowing one to choose dimensions greater than $2n'$.

Previous comparison of the attacks. The size of the modulus q causes a tension between applications and security. Many applications, such as fully homomorphic encryption, need a relatively large modulus, but NTRU with a very large modulus can be broken in polynomial time, even with the Coppersmith-Shamir attack. Hence, it is important to analyze the relation between q and n when studying the security of cryptosystems that are based on overstretched NTRU.

In [1], the experimental results focus on finding the minimal modulus q for which the NTRU problem can be solved with the subfield attack on a fixed n using the LLL algorithm. The subsequent work [8, 12] followed this approach and directly compared to these experiments, both claiming to achieve “better results”. Moreover, [12, Theorem 9] shows that under some conditions, working over a subfield of smaller index (including the full field) will not give worse results despite the increase in dimension (however, see our experimental results for the full field compared to the other attacks in Table 2).

We claim that the lattice dimension, which strongly influences the attacks’ running time, should be central to the attack comparisons. This point has been overlooked in prior work, and thus it is not clear whether the different experiments remain comparable. Table 1 gives a series of experimental “improvements” that decrease q by modifying the dimension. We give results from previous papers and from our own experiments. We ran the subfield and the subring attack using our implementations of these attacks and used the projection technique to reduce the dimension of the lattice. Except for the case $\log(n) = 12$, these comparisons are inconclusive when dimension is taken into account. For a detailed comparison, see the full version of this paper [6].

Table 1: Experimental comparisons between the subfield and subring attacks.

	Attack	$\log n$	$\log q$	$\log r$	Dimension
	Subfield [1]	11	165	4	256
	Subring [12]	11	115	4	638
	Subfield [1]	11	95	3	512
	Subring [12]	11	81	3	856
	Subfield (our exp.)	11	81	2	856
	Subfield [8]	11	72	2	1024
	Subring [12]	12	157	4	686
	Subring/Subfield (our exp.) (failed)	12	157	3	686

4 Main results

Our main contribution is a full characterization of the various attacks on overstretched NTRU. In Section 4.1, we give a detailed analysis of the applicability of the projection technique to NTRU lattices. Having fully proven the subring attack, we compare it to the subfield attack in Section 4.2.

4.1 The projection technique

The key to the projection technique is that the system of equations corresponding to $\mathbf{f} \cdot \mathbf{h} = \mathbf{g}$ is assumed to be overdetermined, so one can discard some of the equations. We formalize this assumption, relate it to standard assumptions on NTRU and derive concrete results. Some of these details are missing in [12, Section 3.2].

In the following, let $\mathcal{L}(A)$ be the lattice generated by any of the above attack matrices A , $\mathcal{L}'$ be the projected lattice of dimension $n' + d$, and $\mathcal{M}$ the upper right quadrant of A . The *discrepancy* $\mathcal{D}(\Gamma)$ [7, 13] measures how equidistributed a sequence of points $\Gamma = \{\gamma_1, \dots, \gamma_n\}$ in the interval $[0, 1]$ is. Formally defined, $\mathcal{D}(\Gamma) = \sup_{J \subseteq [0,1]} \left| \frac{T(J,n)}{n} - |J| \right|$, where the supremum is taken over all subintervals J of $[0, 1]$, $|J|$ is the length of J , and $T(J, n)$ is the number of points γ_i in J for $1 \leq i \leq n$. Let $\mathcal{T}$ be a sequence of elements in $\mathbb{Z}^n$ with the dot product. $\mathcal{T}$ is Δ -homogenously distributed modulo q if for any $a \in \mathbb{Z}^n$ with at least one coordinate coprime to q , the discrepancy of $\{[a \cdot t]_q / q\}_{t \in \mathcal{T}}$ is at most Δ . We would like to consider the columns of $\mathcal{M}$ as a set of elements in $\mathcal{T}$. However, this sequence is not Δ -homogenously distributed modulo q for small Δ : for example when $\mathcal{M} = \mathcal{M}_{\mathbf{h}}$, $\mathbf{h} \cdot \mathbf{f} = \mathbf{g}$ does not distribute homogenously. We define the following weaker notion.

Definition 1 (Weak homogenous distribution). *Let $u \in \mathcal{O}$, $B > 0$, and $\mathcal{T}$ be a sequence of elements in $\mathbb{Z}^n$. Then $\mathcal{T}$ is (B, u) -weakly Δ -homogenously distributed modulo q if for any $a \notin \mathcal{O}u$ such that $\|a\| < B$, with at least one coordinate coprime to q , the discrepancy of the sequence $\{[a \cdot t]_q / q\}_{t \in \mathcal{T}}$ is at most Δ .*

Theorem 1. *For $\mathbf{f}, \mathbf{g} \in R_q$ let $\mathbf{h} = \mathbf{g}/\mathbf{f}$. Suppose the columns of $\mathcal{M}_{\mathbf{h}}$ are $(B, \mathbf{f})$ -weakly Δ -homogenously distributed modulo q . Let $\mathcal{L}'$ be an $(n + d)$ -dimensional lattice as above. Then with probability at least $1 - (2B - 1)^n((2B + 1)/q + \Delta)^d$ over the columns of $\mathcal{M}_{\mathbf{h}}$, any vector $(x, y) \in \mathcal{L}'$ s.t. $\|(x, y)\| < B$ satisfies $(x, [x\mathbf{h}]_q) = (\alpha\mathbf{f}, \alpha\mathbf{g})$ for some $\alpha \in \mathcal{O}$. The result follows for the $(n' + d)$ -dimensional subring lattice $\mathcal{L}'$ with the assumption taken over $\mathcal{O}_L := \mathcal{O} \cap L$.*

Proof. Suppose $0 \neq (x, y) \in \mathcal{L}'$ and $x \notin \mathcal{O}\mathbf{f}$. Let $(x\mathbf{h})_i$ denote the i th coefficient of $[x\mathbf{h}]_q$, $0 \leq i < n$. Suppose that $\|(x, y)\| < B$, so $|x_i| < B$ and $|(x\mathbf{h})_i| < B$. Let $P = \Pr[|(x\mathbf{h})_i| < B]$ for some i . By the assumption on $\mathbf{h}$, $P < \frac{2B+1}{q} + \Delta$. The $d \leq n$ rightmost columns in $\mathcal{L}'$ correspond to coefficients of multiplication by $\mathbf{h}$, so $\Pr[|(x\mathbf{h})_i| < B \text{ for all the corresponding columns in } \mathcal{L}'] = P^d < ((2B + 1)/q + \Delta)^d$, for d independently chosen columns. There are $(2B - 1)^n$ different possibilities for x such that $|x_i| < B$, with $0 \leq i < n$. Hence, the probability over the chosen columns of $\mathcal{M}_{\mathbf{h}}$ in $\mathcal{L}'$ that there exists a lattice point $\|(x, y)\| < B$ with $x \notin \mathcal{O}\mathbf{f}$ is at most $(2B - 1)^n P^d < (2B - 1)^n ((2B + 1)/q + \Delta)^d$. $\square$

Theorem 1 considers $\mathcal{M}_{\mathbf{h}}$, and thus also $\mathcal{M}'_{\mathbf{h}}$, as these are the cases of interest in [12, 17] respectively. However, it can be generalized to the other matrices $\mathcal{M}$ described above. In general, it is not known that the columns of $\mathcal{M}_{\mathbf{h}}$ are $(B, \mathbf{f})$ -weakly homogenously distributed for sufficiently small B . Understanding the distribution of $\mathbf{h}$ is extremely important as it underlies the security of NTRU. In general, $\mathbf{h}$ is not uniformly distributed in R_q , as can be seen from a simple information-theoretic argument. Hence, understanding the distribution of $\mathbf{f}^{-1}$ is important in order to understand the distribution of $\mathbf{h}$. Banks and Shparlinski [2] studied how “well spread” the coefficients of $\mathbf{f}^{-1}$ are, that is, whether they “look and behave like random polynomials”. We remark that the desired property on $\mathbf{h}$ may follow from the behaviour of $\mathbf{f}^{-1}$, but this property is not well formed.

Moreover, it is standard to assume that $\mathbf{h} = \mathbf{g}/\mathbf{f}$ is indistinguishable from random in R_q , see [14]. We remark that this assumption has a strong relation with the weakly homogenous distribution of $\mathcal{M}_{\mathbf{h}}$. Indeed, if the latter is not true, then one can pick a set of small polynomials a and analyze the distribution of $\{[a \cdot t]_q / q\}_{t \in \mathcal{M}_{\mathbf{h}}}$ to distinguish it from a random $\mathbf{h}$. Thus, under the indistinguishability assumption, this set of polynomials has to be negligibly small.

We ran experiments with ternary $\mathbf{f}, \mathbf{g}$ and verified that the coefficients of $[\mathbf{f}^{-1}]_q$ equidistribute in $\mathbb{Z}_q$ and that $\mathcal{M}_{\mathbf{h}}$ is $(B, \mathbf{f})$ -weakly homogenously distributed for sufficiently small B . For the rest of the paper, we rely on the following assumption.

Assumption 1. *The set of columns $\mathcal{M}_{\mathbf{h}}$ is $(B, \mathbf{f})$ -weakly $O(q^{-1})$ -homogenously distributed modulo q for $B \ll q$.*

Corollary 1. Let $\mathbf{f}, \mathbf{g} \in R_q$ and $\mathbf{h} = \mathbf{g}/\mathbf{f}$ be NTRU private and public keys. Let $\mathcal{L}'$ be the projected NTRU lattice of dimension $n + d$, where $d \geq (n \log(2B + 1) + 1) / \log(q/(2B + 1))$. Under Assumption 1, any vector $(x, y) \in \mathcal{L}'$ s.t. $\|(x, y)\| < B$ satisfies $(x, [xh]_q) = (\alpha f, \alpha g)$ for some $\alpha \in \mathcal{O}$ with probability at least $1/2 + O(q^{-1})$ over the chosen columns of $\mathcal{M}_{\mathbf{h}}$. The result follows for the $(n' + d)$ -dimensional subring lattice $\mathcal{L}'$ with the assumption taken over $\mathcal{O}_L := \mathcal{O} \cap L$.

Proof. Using notation from Theorem 1, the probability that there exists a lattice point $\|(x, y)\| < B$ with $x \notin \mathcal{O}f$ is at most $\frac{(2B+1)^{n+d}}{q^d} + O(q^{-1}) = \frac{2^{(n+d)(\log(2B+1))}}{2^{d \log(q)}} + O(q^{-1})$. Setting $d \geq (n \log(2B + 1) + 1) / \log(q/(2B + 1))$ gives the result. $\square$

Setting d as required in Corollary 1, observe that the dimension of $\mathcal{L}'$ is $n + d \geq (n \log(q) + 1) / (\log(q/(2B + 1)))$. This is similar to the subring lattice in [12, Theorem 6]. Thus, Corollary 1 completes the missing details on the validity of the subring attack and, along with [12, Theorem 6], gives a complete analysis of the subring attack under Assumption 1. We formalize this result in the following theorem. Now, β denotes the block size in the BKZ [21] algorithm.

Theorem 2 (Adapted from Theorem 6 in [12]). Let $\mathbf{f}, \mathbf{g} \in R_q$ and $\mathbf{h} = \mathbf{g}/\mathbf{f}$ be NTRU private and public keys satisfying Assumption 1. Let $B = \|\mathbf{v}\|$ where $\mathbf{v} = (\mathbf{f}, \mathbf{g})$ in the full field, $\mathbf{v} = (N_{K/L}(\mathbf{f}), N_{K/L}(\mathbf{g}))$ in the subfield and $\mathbf{v} = (N_{K/L}(\mathbf{f}), N_{K/L}(\mathbf{f}\mathbf{h}))$ in the subring. Then for $\frac{\beta}{\log \beta} = \frac{2n' \log q}{\log(q/B)^2}$ one can find a multiple $\alpha \mathbf{v}$ for a non-zero $\alpha \in \mathcal{O}$ with probability at least $1/2 + O(q^{-1})$ over the chosen columns of $\mathcal{M}$.

4.2 Comparing $\|N_{K/L}(\mathbf{g})\|$ and $\|N_{K/L}(\mathbf{f}\mathbf{h})\|$

In Section 3, we showed that a small vector in the subfield lattice is the vector $(N_{K/L}(\mathbf{f}), N_{K/L}(\mathbf{g}))$, while in the subring lattice the vector $(N_{K/L}(\mathbf{f}), N_{K/L}(\mathbf{f}\mathbf{h}))$ is small. The f part of these vectors is the same. Our interest is therefore in the g part. Moreover, we know that $N_{K/L}(\mathbf{g})$ n' -dimension vector and $N_{K/L}(\mathbf{f}\mathbf{h})$ is n -dimensional vector. We show that these two elements have the same Euclidean norm. It then follows that on average the coefficients of $N_{K/L}(\mathbf{g})$ are larger than the coefficients of $N_{K/L}(\mathbf{f}\mathbf{h})$. When we truncate the latter to n' coordinates, its norm becomes smaller than the norm of $N_{K/L}(\mathbf{g})$. Using an assumption on the distribution of the coefficients of $N_{K/L}(\mathbf{g})$, we quantify the difference in size. More precisely, Theorem 3 shows, with no further assumptions, that when $[K : L] = 2$, the average size of the coefficients of $N_{K/L}(\mathbf{g})$ is expected to be $\sqrt{2}$ times the average size of the coefficients of $N_{K/L}(\mathbf{f}\mathbf{h})$. In Theorem 4, we generalize this result for any subfield such that $[K : L] = r$, and prove that the expected ratio of the average magnitude of the coefficients is $\sqrt{r}$ under Assumption 2 below. Our main results are given in Corollaries 2 and 3.

Claim 1. Let f, g be two polynomials with coefficients chosen uniformly at random from the same set. Let $f = (u_1, \dots, u_m)$ and $g = (w_1, \dots, w_n)$. Then, $E[\|f\|^2] = E[\|g\|^2]$ if and only if the expectation of the square of the coefficients satisfies $E[u_i^2] = \frac{n}{m} E[w_i^2]$.

In light of this result, our aim is to show that the ratio between $\|N_{K/L}(\mathbf{g})\|$ and $\|N_{K/L}(\mathbf{f}\mathbf{h})\|$ tends to 1 as n increases. Then, we can conclude that the subring lattice of dimension $2n'$ is expected to contain shorter vectors than the subfield lattice of the same dimension. We use random walks to model the coefficients of a product of two polynomials. A first case is for polynomials whose coefficients are drawn independently and uniformly from the set $\{-1, 0, 1\}$. A one-dimensional random walk over $\mathbb{Z}$ starts at 0 and at each step moves either +1 or -1 with equal probability. Let a_i , for $i = 1, \dots, n$, denote independent random variables with value either +1 or -1 with uniform probability, and let $w_0 = 0$ and $w_n = \sum_{i=1}^n a_i$. The series $\{w_n\}$ defines a random walk over $\mathbb{Z}$. The expected distance after n steps is on the order of $\sqrt{n}$. As n increases, the distribution of the series w_n approaches the normal distribution. A second case is for polynomials whose coefficients are drawn from a Gaussian distribution: in a Gaussian random walk, we let a_i follow the Gaussian distribution with standard deviation σ and mean zero. The expected distance after n steps is then on the order of $\sigma\sqrt{n}$. For further background, see [15]. We now consider the specific case of subfield $L \subseteq K$ of index 2.

Theorem 3. Let $\mathbf{f}, \mathbf{g} \in R_q$ be two polynomials whose coefficients are drawn independently and uniformly from $\{-1, 0, 1\}$. Let $N_{K/L}(\mathbf{g}) = (u_1, \dots, u_n)$ and $\mathbf{g}\sigma_2(\mathbf{f}) = (w_1, \dots, w_n)$. Then $E[u_i^2 \mid u_i \neq 0] = 8n/9 - 4/9$ and $E[w_i^2] = 4n/9$. Thus, as n goes to infinity the ratio between the expected magnitude of the non-zero coefficients of $N_{K/L}(\mathbf{g})$ and $\mathbf{g}\sigma_2(\mathbf{f})$ tends to $\sqrt{2}$ in absolute value and the ratio of the expected squared Euclidean norms $E[\|N_{K/L}(\mathbf{g})\|^2] / E[\|\mathbf{g}\sigma_2(\mathbf{f})\|^2]$ tends to 1.

Proof. We start by comparing the expected size of the coefficients of $N_{K/L}(\mathbf{g})$ to those of $\mathbf{g}\sigma_2(\mathbf{f})$. Let $a_i \in \{-1, 0, 1\}$ uniformly and independently at random and consider the polynomial $\mathbf{g} = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_1x + a_0 \in R_q$. Then $\sigma_2(\mathbf{g}) = -a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots - a_1x + a_0$. Each coefficient u_k of $N_{K/L}(\mathbf{g}) = \mathbf{g}\sigma_2(\mathbf{g})$ is a sum of n terms. For k odd, $u_k = 0$, because each of the terms $a_i a_j$ in this sum appears twice with opposite signs. For k even, $u_k = 2 \sum_{i < j, i+j \equiv k \pmod n} \pm a_i a_j + a_{k/2}^2 + a_{(n+k)/2}^2$, since each term $a_i a_j$ with $i \neq j$ appears twice with similar sign. Then, we have $E[a_i a_j \mid i \neq j] = 0$, $E[a_i^2] = E[a_i^4] = 2/3$, and $E[(a_i a_j)^2] = 4/9$ and for k even

$$E[u_k^2] = E[(2 \sum_{i < j, i+j \equiv k \pmod n} \pm a_i a_j + a_{k/2}^2 + a_{(n+k)/2}^2)^2] = 8n/9 - 4/9.$$

Now, let us repeat a very similar argument for $\mathbf{g}\sigma_2(\mathbf{f})$, where $\sigma_2(\mathbf{f})$ is a polynomial of the form $\sigma_2(\mathbf{f}) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \dots + b_1x + b_0$, with $b_i \in \{-1, 0, 1\}$ uniformly and independently at random. Again, each coefficient w_k of $\mathbf{g}\sigma_2(\mathbf{f})$ is a sum of n terms. However, unlike the case above, there are no similar terms in this sum, and we have $E[a_i b_j] = 0$ and $E[(a_i b_j)^2] = 4/9$. As above, we compute

$$E[w_k^2] = E[(\sum_{i+j \equiv k \pmod n} a_i b_j)^2] = \sum_{i+j \equiv k \pmod n} E[(a_i b_j)^2] = 4n/9.$$

Thus the expected square of the Euclidean norms $E[\|N_{K/L}(\mathbf{g})\|^2] = E[\sum_i u_i^2] = \sum_i E[u_i^2] = 4n^2/9 - 2n/9$ and $E[\|\mathbf{g}\sigma_2(\mathbf{f})\|^2] = E[\sum_i w_i^2] = 4n^2/9$. $\square$

We would like to generalize this result to $r > 2$. While the coefficients of $\mathbf{g}\sigma_2(\mathbf{g})$ and $\mathbf{g}\sigma_2(\mathbf{f})$ can be expressed as random walks, and thus follow a Gaussian distribution, they may not be independent.

Assumption 2. For $r > 1$, the coefficients of $N_{K/L}(\mathbf{g})$, $N_{K/L}(\mathbf{f})$ and $N_{K/L}(\mathbf{f})\mathbf{h}$ behave as if they were independently chosen from a Gaussian distribution.

This assumption seems natural and allows us to prove Theorem 4, a generalisation of Theorem 3 to any $r > 0$. We experimentally verified that as n grows, the ratio of the norms tends to 1, as in Theorem 4, see Figure 1. From this, we directly get that the ratio of the average coefficient tends to $\sqrt{r}$, see Claim 1.

Figure 1: Experimentally verifying that the ratio of the norms converges to 1.

Theorem 4. Let $\mathbf{f}, \mathbf{g} \in R_q$ and $\mathbf{h} = \mathbf{g}/\mathbf{f}$ be NTRU private and public keys satisfying Assumption 2. For a subfield $L \subseteq K$, let $N_{K/L}(\mathbf{g}) = (u_1, \dots, u_n)$ and $N_{K/L}(\mathbf{f})\mathbf{h} = (w_1, \dots, w_n)$. Then, as n goes to infinity the ratio between the expected magnitude of the non-zero coefficients of $N_{K/L}(\mathbf{g})$ and $N_{K/L}(\mathbf{f})\mathbf{h}$ tends to $\sqrt{r}$ in absolute value. In addition, the ratio of the expected squared Euclidean norms $E[\|N_{K/L}(\mathbf{g})\|^2] / E[\|N_{K/L}(\mathbf{f})\mathbf{h}\|^2]$ tends to 1 as n goes to infinity.

Proof. We give a proof by induction on the index r where the base case is proven in Theorem 3. Suppose the claim holds for index r , we show that it holds for $[K : L] = 2r$. First note that for a tower of fields $L \subseteq E \subseteq K$ we have $N_{K/L}(\mathbf{a}) = N_{E/L}(N_{K/E}(\mathbf{a}))$ for every $\mathbf{a} \in K$ (see [16, Theorem 2.29]). Consider the case $[K : E] = r$, $[E : L] = 2$, and denote $\mathbf{G} := N_{K/E}(\mathbf{g})$ and $\mathbf{F} := N_{K/E}(\mathbf{f})$. Then, $N_{K/L}(\mathbf{g}) = N_{E/L}(\mathbf{G}) = \mathbf{G}\sigma'_2(\mathbf{G})$ and $N_{K/L}(\mathbf{f})\mathbf{h} = N_{E/L}(\mathbf{F})\mathbf{h} = \mathbf{F}\sigma'_2(\mathbf{F})\mathbf{h} = \mathbf{G}'\sigma'_2(\mathbf{F})$, where $\sigma'_2 \in \text{Gal}(E/L)$ and $\mathbf{G}' = \mathbf{F}\mathbf{h} = N_{K/E}(\mathbf{f})\mathbf{h}$. The previous case of the construction, i.e. $[K : E] = r$, shows that each (non-zero) coefficient of $\mathbf{F}$, $\mathbf{G}$ and $\mathbf{G}'$ follows a Gaussian distribution. Under Assumption 2 the coefficients can be considered to be independent. We can now repeat the process of Theorem 3. While $\mathbf{G}' \in K$, note that $\mathbf{F}, \mathbf{G} \in E$ so they have n/r non-zero coefficients. Thus, similarly to Theorem 3, each non-zero coefficient of $\mathbf{G}\sigma'_2(\mathbf{G})$ is approximately 2 multiplied by a Gaussian random walk with $n/2r$ steps, while each coefficient of $\mathbf{G}'\sigma'_2(\mathbf{F})$ is a random walk with n/r steps. By the induction hypothesis, a coefficient of $\mathbf{G}$ is expected to be larger than coefficients of $\mathbf{G}'$ by a factor of $\sqrt{r}$ for sufficiently large n . The result on the coefficients follows from evaluating the expected size of the random walks and the claim on the norms follows from Claim 1. $\square$

The following corollary compares small vectors in the subfield and subring lattices of same dimensions, without using projection in the subfield lattice.

Corollary 2. Let $B_{\text{subfield}} = \|(N_{K/L}(\mathbf{f}), N_{K/L}(\mathbf{g}))\|$ where $[K : L] = r = n/n'$. Let $B_{\text{subring}}^{\text{proj}} = \|(N_{K/L}(\mathbf{f}), \overline{N_{K/L}(\mathbf{f})\mathbf{h}})\|$ where the projection keeps $2n'$ coordinates. Under Assumptions 1 and 2, for sufficiently large n we expect to have $\frac{B_{\text{subfield}}^2}{(B_{\text{subring}}^{\text{proj}})^2} \approx \frac{2r}{r+1}$. Moreover, suppose that B_{subfield} is the norm of the shortest vector in the subfield lattice, and denote by q_{subfield} and q_{subring} the modulus in the subfield and subring attacks, respectively, that the BKZ algorithm can solve NTRU with a fixed block size β . Then $\frac{q_{\text{subfield}}}{q_{\text{subring}}} \geq \frac{2r}{r+1}$.

Proof. To simplify notation, we write $\text{coeff}(f)$ to denote the average size of the coefficients of a polynomial f . We have $B_{\text{subfield}}^2 = (n/r)(\text{coeff}(N_{K/L}(\mathbf{f}))^2 + \text{coeff}(N_{K/L}(\mathbf{g}))^2)$, and $(B_{\text{subring}}^{\text{proj}})^2 = (n/r)(\text{coeff}(N_{K/L}(\mathbf{f}))^2 + \text{coeff}(N_{K/L}(\mathbf{f})\mathbf{h})^2)$. We know that $\text{coeff}(N_{K/L}(\mathbf{f}))^2 \approx \text{coeff}(N_{K/L}(\mathbf{g}))^2$ and from Theorem 4, we also know that $\text{coeff}(N_{K/L}(\mathbf{g}))^2 \approx r \text{coeff}(N_{K/L}(\mathbf{f})\mathbf{h})^2$. BKZ is guaranteed to output a vector bounded by $\beta^{2n'/\beta} \lambda_1(\mathcal{L})$. The second result follows from bounding this value by $\sqrt{q}$ in both lattices. $\square$

It follows that if we take the same lattice dimension in both attacks, the subring lattice contains vectors of smaller size. Therefore one can solve the NTRU problem using the subring attack with a smaller q . As mentioned in [1, Section 6], it is not known that B_{subfield} is the norm of the shortest vector (see [12, Theorem 5]). Moreover, our experiments in Table 2 show that the ratio between q_{subfield} and q_{subring} grows with r . One possible explanation is that $(N_{K/L}(\mathbf{f}), \overline{N_{K/L}(\mathbf{f})\mathbf{h}})$ is unbalanced, as we show its f part is much larger than the g part. Therefore, if there exists an integral multiple of this vector that decreases the size of the f part and increases the size of the g part so that the vector becomes balanced, the ratio between the feasible q s would increase.

If the systems of equations derived from the lattices given in Corollary 2 are overdetermined, we can project and get smaller lattices. Since the g part in the subring lattice is smaller than in the subfield one, the subring attack system is more determined than the subfield one.

The following corollary shows that one can use projection to discard more equations in the subring attack and achieve a lower dimension.

Corollary 3. With the notation from Theorem 2 and Corollary 2, set $B := B_{\text{subfield}}$. Under Assumptions 1 and 2, for sufficiently large n , we can find a multiple αv for some non-zero $\alpha \in \mathcal{O}$ such that using BKZ with block size β on the lattice $\mathcal{L}'$ of dimension $n' + d$, we have the following two cases. If $\mathcal{L}'$ is the subfield lattice, then $n' + d \geq \frac{n' \log(q)+1}{\log(q/(2B+1))}$ and $\frac{\beta}{\log \beta} = \frac{2n' \log q}{(\log(q/B))^2}$, and if $\mathcal{L}'$ is the subring lattice, then $n' + d \geq \frac{n' \log(q)+1}{\log(q\sqrt{r}/(\sqrt{2r+2B}+\sqrt{r}))}$ and $\frac{\beta}{\log \beta} = \frac{2n' \log q}{(\log(\sqrt{2r}q/\sqrt{r+1}B))^2}$.

Table 2: Experimentally determining the minimal q for each attack. For a fixed dimension, we compare the subring attack to the subfield attack without projection, and note whether the attack succeeded. In some cases the full field attack only succeeded with projection; (384;512) means we ran the full field attack in these two dimensions.

Parameters				Attacks		
$\log n$	Dimension (Full/subfield)	$\log r$	$\log q$	Full field	Subring	Subfield
8	(384;512)/256	1	22	Yes ;No	Yes	Yes
8	(384;512)/256	1	21	No	Yes	No
9	(768;1024)/512	1	34	Yes ;No	Yes	Yes
9	768/512	1	32	No	Yes	Yes
9	768/512	1	31	No	No	No
9	1024/256	2	40	Yes	Yes	Yes
9	1024/256	2	38	Yes	Yes	No
9	1024/256	2	37	Yes	No	No
9	1024/256	2	36	Yes	No	No
10	2048/512	2	52	-	Yes	Yes
10	2048/512	2	50	-	Yes	No
10	2048/512	2	49	-	No	No
11	4096/512	3	95	-	Yes	Yes
11	4096/512	3	92	-	Yes	No
11	4096/512	3	91	-	No	No
11	4096/256	4	165	-	Yes	Yes
11	4096/256	4	162	-	Yes	No
11	4096/256	4	161	-	No	No
12	4096/512	4	189	-	Yes	Yes
12	4096/512	4	185	-	Yes	No
12	4096/512	4	184	-	No	No

Table 3: Experimentally determining the minimal dimension for each attack. For fixed parameters $\log n$ and $\log q$, we compare the subfield and the subring attacks applied to a lattice of the *same* dimension, using the projection technique where applicable, and note whether the attack succeeded.

Parameters				Attacks		LLL reduction time (s)	
$\log n$	$\log q$	$\log r$	Dimension	Subfield	Subring	Subfield	Subring
8	22	1	233	Yes	Yes	715.4	577.6
8	22	1	223	No	Yes	454.5	452.3
8	22	1	222	No	No	456.5	424.3
9	70	3	122	Yes	Yes	132.6	121.1
9	70	3	117	No	Yes	116.2	117.0
9	70	3	116	No	No	108.7	108.9
10	150	4	124	Yes	Yes	344.8	325.3
10	150	4	120	No	Yes	298.6	304.1
10	150	4	119	No	No	290.2	286.5
11	165	4	254	Yes	Yes	15333.0	12423.7
11	165	4	249	No	Yes	12708.7	12072.0
11	165	4	248	No	No	12086.3	11722.8

4.2.1 Experimental results

We implemented all three attacks in Sage and experimentally compared them using Sage's default LLL implementation. A success in our experiments is recovering a vector v such that $\|v\| < q^{3/4}$. As noted by [12], we either get vectors which are roughly of size q , or vectors of size $\sqrt{q}$ that are short integral multiples of the private key. First, we fix the parameters (n , dimension, r) and compare the smallest modulus q that succeeded for each of the three attacks using LLL. Details are given in Table 2. Note that we do not apply the projection technique to the subfield attack in these experiments. The analysis of the subfield attack without projection is given in Corollary 2. Then, we compared the subring and subfield attacks by fixing (n , q , r) and comparing the smallest dimension that succeeded using LLL. For some of the lattices we used the projection technique by deleting the right-most columns until we reached the desired dimension. The difference is greater than our analysis predicts. Details are given in Table 3. The analysis of the subfield attack with projection is given in Corollary 3. Experiments were run on a single core of an Intel Xeon E5-2699 v3 running at 2.30GHz, with 128 GB of RAM.

Acknowledgement: We thank Shi Bai for some helpful discussions.

This material supported by the National Science Foundation under Grants No. CNS-1513671 and CNS-1651344 and by the ONR SynCrypt project. We are grateful to Cisco for donating the Cisco UCS servers used for our experiments.

References

- [1] M. Albrecht, S. Bai, and L. Ducas. A Subfield Lattice Attack on Overstretched NTRU Assumptions. *CRYPTO 2016*.
- [2] W.D. Banks and I.E. Shparlinski. Distribution of Inverses in Polynomial Rings. *Indagationes Mathematicae*, 12(3), 2001.
- [3] D. Boneh and R. Venkatesan. Hardness of Computing the Most Significant Bits of Secret Keys in Diffie–Hellman and Related Schemes. *CRYPTO 1996*.
- [4] J. H. Cheon, J. Jeong, and C. Lee. An Algorithm for NTRU Problems and Cryptanalysis of the GGH Multilinear Map without a Low-Level Encoding of Zero. *LMS Journal of Computation and Mathematics*, 19(A): 2016.
- [5] D. Coppersmith and A. Shamir. Lattice Attacks on NTRU. *Eurocrypt '97*.
- [6] G. De Micheli, N. Heninger, and B. Shani. Characterizing overstretched NTRU attacks. ePrint 2018/630
- [7] M. Drmota and R. Tichy. *Discrepancies and Applications*.
- [8] D. H. Duong, M. Yasuda, and T. Takagi. Choosing Parameters for the Subfield Lattice Attack Against Overstretched NTRU. *Information Security 2017*.
- [9] S. Garg, C. Gentry, and S. Halevi. Candidate Multilinear Maps from Ideal Lattices. *EUROCRYPT 2013*.
- [10] J. Hoffstein, N. Howgrave-Graham, J. Pipher, J. H. Silverman, and W. Whyte. NTRUSign: Digital Signatures Using the NTRU Lattice. *CT-RSA 2003*.
- [11] J. Hoffstein, J. Pipher, and J. H. Silverman. NTRU: A Ring-based Public Key Cryptosystem. *Algorithmic Number Theory 1998*.
- [12] P. Kirchner and P.-A. Fouque. Revisiting Lattice Attacks on Overstretched NTRU Parameters. *EUROCRYPT 2017*.
- [13] R. Kuipers and H. Niederreiter. *Uniform Distribution of Sequences*.
- [14] A. López-Alt, E. Tromer, and V. Vaikuntanathan. On-the-fly Multiparty Computation on the Cloud via Multikey Fully Homomorphic Encryption. *STOC '12*.
- [15] G. F. Lawler and V. Limic. *Random Walk: A Modern Introduction*.
- [16] R. Lidl and H. Niederreiter. *Finite Fields*. Cambridge University Press, 1997.
- [17] A. May. Cryptanalysis of NTRU, 1999.
- [18] A. May and J. H. Silverman. Dimension Reduction Methods for Convolution Modular Lattices. *Cryptography and Lattices*.
- [19] G. Pataki and M. Tural. On Sublattice Determinants in Reduced Bases, 2008.
- [20] P. Samuel. *Algebraic Theory of Numbers*. Hermann, 1970.
- [21] C. P. Schnorr. A Hierarchy of Polynomial Time Lattice Basis Reduction Algorithms. *Theor. Comput. Sci.*, 53(2-3):201–224, August 1987.
- [22] D. Stehlé and R. Steinfeld. Making NTRU as Secure as Worst-Case Problems over Ideal Lattices. *EUROCRYPT 2011*.
- [23] R. Steinfeld. *NTRU Cryptosystem: Recent Developments and Emerging Mathematical Problems in Finite Polynomial Rings*. Walter de Gruyter, 2014.