Revisiting the Hybrid Attack: Improved Analysis and Refined Security Estimates

Thomas Wunderer

Technische Universität Darmstadt, Germany
twunderer@cdc.informatik.tu-darmstadt.de

Abstract. Over the past decade, the hybrid lattice reduction and meet-in-the middle attack (called the Hybrid Attack) has been used to evaluate the security of many lattice-based cryprocraphic schemes such as NTRU, NTRU prime, BLISS, and more. However, unfortunately none of the previous analyses of the Hybrid Attack is entirely satisfactory: they are based on simplifying assumptions that may distort the security estimates. Such simplifying assumptions include setting probabilities equal to 1, which, for the parameter sets we analyze in this work, are in fact as small as 2^{-80}. Many of these assumptions lead to underestimating the scheme's security. However, some lead to security overestimates, and without further analysis, it is not clear which is the case. Therefore, the current security estimates against the Hybrid Attack are not reliable and the actual security levels of many lattice-based schemes are unclear.
In this work we present an improved runtime analysis of the Hybrid Attack that gets rid of incorrect simplifying assumptions. Our improved analysis can be used to derive reliable and accurate security estimates for many lattice-based schemes. In addition, we reevaluate the security against the Hybrid Attack for the NTRU, NTRU prime, and R-BinLWEEnc encryption schemes as well as for the BLISS and GLP signature schemes. Our results show that there exist both security over- and underestimates in the literature. Our results further show that the common claim that the Hybrid Attack is the best attack on all NTRU parameter sets is in fact a misconception based on incorrect analyses of the attack.

Keywords: Hybrid Attack, Lattice-based Cryptography, Cryptanalysis, SVP, LWE, NTRU, BLISS

1 Introduction

In 2007, Howgrave-Graham proposed the hybrid lattice-reduction and meet-in-the-middle attack [22] (referred to as the Hybrid Attack in the following) against the NTRU encryption scheme [21]. Several works [18–20, 22, 30] claim that the Hybrid Attack is by far the best known attack on NTRUEncrypt. In the following years, numerous cryptographers have applied the Hybrid Attack to their cryptographic schemes in order to estimate their security. These considerations include

more variants of the NTRU encryption scheme [18,20,30], the recently proposed encryption scheme NTRU prime [9], a lightweight encryption scheme based on Ring-LWE with binary error [10,11], and the signature schemes BLISS [16] and GLP [16,17]. In [30], Schanck even proposed a quantum version of the Hybrid Attack on NTRUencrypt that replaces the meet-in-the-middle phase with Grover's search algorithm. All of the above analyses of the Hybrid Attack have in common, that the authors claim that the Hybrid Attack is the best known attack on the respective schemes. Unfortunately, they also all have in common that the analyses are flawed, yielding unreliable security estimates of the schemes. These flaws are mainly due to simplifying but incorrect assumptions that are made in order to ease the theoretical analysis of the attack. Most of the time, the authors are aware of these flaws and explicitly state when such incorrect assumptions are introduced. Furthermore, many of these assumptions yield more conservative security estimates (lower than necessary), as they give more power to the attacker. While this is not a problem from a security perspective, in those cases the schemes might be instantiated more efficiently while preserving the desired security level. On the other hand, there also exist the more dangerous cases in which the security of a scheme is overestimated, i.e., the scheme is less secure than it is claimed to be, as we show in this work. In [30], Schanck summarizes the current state of the analyses of the Hybrid Attack as follows.

> "[...] it should be noted that, in the author's opinion, no analysis of the hybrid attack presented thus far is entirely satisfactory. [...] it is hoped that future work will answer some of the outstanding questions related to the attack's probability of success as a function of the effort spent in lattice reduction and enumeration."

The author further acknowledges that the fact that the Hybrid Attack is considered the best attack on NTRU might be due to flawed analyses resulting in overly conservative security estimates.

> "The hybrid attack gives the lowest estimate for the time complexity of NTRU key recovery amongst all known classical attacks. Likewise for message recovery. Perhaps this is because it is overly optimistic, in particular by ignoring the probability of failure in approximate collision search."

In this quote, Schanck mentions the following common flaw appearing in many previous runtime analyses of the Hybrid Attack. In many works [9,16,19,20,30] the authors assume that collisions in the meet-in-the-middle phase of the attack will always be detected. However, in reality collisions can only be detected with a very low probability. For instance, for the cryptographic schemes we analyze in this work this probability is sometimes as low as 2^{-80}, see Table 3, but was simply set equal to 1 in previous analyses in order to ease the runtime analysis of the attack. These numbers showcase how unrealistic some assumptions made in previous runtime estimates of the Hybrid Attack are in practice. Therefore, there is reasonable doubt about the accuracy and reliability of currently existing security estimates against the Hybrid Attack.

Our contribution. In this work we rectify the current unsatisfactory state of affairs regarding the unreliable security estimates against the Hybrid Attack. This is achieved in the following way. We present a generalized version of the Hybrid Attack applied to shortest vector problems (SVP) and show how it can also be used to solve bounded distance decoding (BDD) problems. This general framework for the Hybrid Attack can naturally be applied to many lattice-based cryptocraphic constructions, as we also show in this work. We further provide a detailed and improved analysis of the generalized version of the Hybrid Attack, which can be used to derive reliable and accurate security estimates. We offer formulas for security underestimates and formulas for security overestimates, giving a (small) range of the actual security level. We thereby meet the demand of a satisfactory analysis of the Hybrid Attack, which has been stated in previous works. In our new analysis of the attack we get rid of unnecessary and incorrect assumptions and clearly state the remaining necessary heuristics in order to offer as much transparency as possible. Whenever there is need, we make distinct assumptions on the attacker's power for our security under- and overestimates. We provide examples of typical unnecessary simplifying assumptions that have frequently been made in previous analyses of the Hybrid Attack in order to highlight the improvements of our analysis. We further show how researchers can use our newly developed techniques in the future to accurately analyze the security of their cryptographic schemes against the Hybrid Attack.

Our second main contribution is the following. Since previous analyses of the Hybrid Attack are flawed, the security estimates of many lattice-based cryptographic schemes against the Hybrid Attack might be inaccurate and their actual security level is unclear. We therefore apply our new and improved analysis to reevaluate the security of various cryptographic schemes against the Hybrid Attack in order to derive updated security estimates that can be relied upon. Our detailed security reevaluations against the Hybrid Attack are also meant to serve as a guideline how to correctly apply the attack and estimate its runtime, since some steps of the analysis are not obvious and might be overlooked at first glance. Furthermore, we provide our implementations used for the optimization of the attack parameters and the security estimates.[1] We first revisit the hybrid security estimates of the NTRU [20], NTRU prime [9], and R-BinLWEEnc [10] encryption schemes and end with the BLISS [16] and GLP [17] signature schemes. Our results show that there exist both security over- and underestimates against the Hybrid Attack across the literature, which we rectify in this work. In addition, our results show that the common claim that the Hybrid Attack is the best attack on all NTRU parameter sets is in fact a misconception based on incorrect analyses of the attack.

Outline. This work is structured as follows. First, we fix notation and provide the necessary background in the Preliminaries. In Section 3 we describe a generalized version of the Hybrid Attack on shortest vector problems (SVP)

[1] The implementation is available on `https://www.cdc.informatik.tu-darmstadt.de/cdc/personen/thomas-wunderer`.

and further explain how it can also be used to solve bounded distance decoding (BDD) problems. Our detailed and improved runtime analysis of the Hybrid Attack is presented in Section 4. In the following Section 5 we apply our new improved analysis of the Hybrid Attack to various cryptographic schemes in order to derive updated and reliable security estimates against the Hybrid Attack that replace the unreliable previous ones. We end this work by giving a conclusion and outlook for possible future work.

2 Preliminaries

Notation. In this work, we write vectors in bold lowercase letters, e.g., $\mathbf{a}$, and matrices in bold uppercase letters, e.g., $\mathbf{A}$. Polynomials are written in normal lower case letters, e.g., a. We frequently identify polynomials $a = \sum_{i=0}^{n} a_i x^i$ with their coefficient vectors $\mathbf{a} = (a_0, \ldots, a_n)$, indicated by using the corresponding bold letter. Let $n, q \in \mathbb{N}$, $f \in \mathbb{Z}[x]$ be a polynomial of degree n and $R_q = \mathbb{Z}_q[x]/(f)$. We define the rotation matrix of a polynomial $a \in R_q$ as $\mathsf{rot}(a) = (\mathbf{a}, \mathbf{ax}, \mathbf{ax}^2, \ldots, \mathbf{ax}^{n-1}) \in \mathbb{Z}_q^{n \times n}$. Then for $a, b \in R_q$, the matrix-vector product $\mathsf{rot}(a) \cdot \mathbf{b} \mod q$ corresponds to the product of polynomials $ab \in R_q$.

We use the abbreviation $\log(\cdot)$ for $\log_2(\cdot)$. We further write $\|\cdot\|$ instead of $\|\cdot\|_2$ for the Euclidean norm. For $N \in \mathbb{N}_0$ and $m_1, \ldots, m_k \in \mathbb{N}_0$ with $m_1 + \ldots + m_k = N$ the multinomial coefficient is defined as

$$\binom{N}{m_1, \ldots, m_k} = \frac{N!}{m_1! \cdot \ldots \cdot m_k!}.$$

Lattices and bases. In this work we use the following definition of lattices. A discrete additive subgroup of $\mathbb{R}^m$ for some $m \in \mathbb{N}$ is called a lattice. Let m be a positive integer. For a set of vectors $\mathbf{B} = \{\mathbf{b}_1, ..., \mathbf{b}_n\} \subset \mathbb{R}^m$, the lattice spanned by $\mathbf{B}$ is defined as

$$\Lambda(\mathbf{B}) = \left\{ \mathbf{x} \in \mathbb{R}^m \mid \mathbf{x} = \sum_{i=1}^{m} \alpha_i \mathbf{b}_i \text{ for } \alpha_i \in \mathbb{Z} \right\}.$$

Let $\Lambda \subset \mathbb{R}^m$ be a lattice. A set of vectors $\mathbf{B} = \{\mathbf{b}_1, ..., \mathbf{b}_n\} \subset \mathbb{R}^m$ is called a basis of Λ if $\mathbf{B}$ is $\mathbb{R}$-linearly independent and $\Lambda = \Lambda(\mathbf{B})$. Abusing notation, we identify lattice bases with matrices and vice versa by taking the basis vectors as the columns of the matrix. The number of vectors in a basis of a lattice is called the dimension (or rank) of the lattice. Let q be a positive integer. The length of the shortest non-zero vectors of a lattice Λ is denoted by $\lambda_1(\Lambda)$. A lattice Λ that contains $q\mathbb{Z}^m$ is called a q-ary lattice. For a matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$, we define the q-ary lattice

$$\Lambda_q(\mathbf{A}) := \{\mathbf{v} \in \mathbb{Z}^m \mid \exists \mathbf{w} \in \mathbb{Z}^n : \mathbf{Aw} = \mathbf{v} \mod q\}.$$

For a lattice basis $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_m\} \subset \mathbb{R}^m$ its fundamental parallelepiped is defined as

$$\mathcal{P}(\mathbf{B}) = \left\{ \mathbf{x} = \sum_{i=1}^{m} \alpha_i \mathbf{b}_i \in \mathbb{R}^m \mid -1/2 \leq \alpha_i < 1/2 \text{ for all } i \in \{1, \ldots, m\} \right\}.$$

The determinant $\det(\Lambda)$ of a lattice $\Lambda \subset \mathbb{R}^m$ is defined as the m-dimensional volume of the fundamental parallelepiped of a basis of Λ. Note that the determinant of the lattice is well defined, i.e., it is independent of the basis. The Hermite delta (or Hermite factor) δ of a lattice basis $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_m\} \subset \mathbb{R}^m$ is defined via the equation $\|\mathbf{b}_1\| = \delta^m \det(\Lambda)^{1/m}$. It provides a measure for the quality of the basis.

Lattice-based cryptography is based on the presumed hardness of computational problems in lattices. Two of the most important lattice problems are the following.

Shortest vector problem (SVP). Given a lattice basis $\mathbf{B}$, the task is to find a shortest non-zero vector in the lattice $\Lambda(\mathbf{B})$.

Bounded distance decoding (BDD). Given $\alpha \in \mathbb{R}_{\geq 0}$, a lattice basis $\mathbf{B} \subset \mathbb{R}^m$ and a target vector $\mathbf{t} \in \mathbb{R}^m$ with $\mathsf{dist}(\mathbf{t}, \Lambda(\mathbf{B})) < \alpha\lambda_1(\Lambda(\mathbf{B}))$, the task is to find a vector $\mathbf{e} \in \mathbb{R}^m$ with $\|\mathbf{e}\| < \alpha\lambda_1(\Lambda(\mathbf{B}))$ such that $\mathbf{t} - \mathbf{e} \in \Lambda(\mathbf{B})$.

Babai's Nearest Plane. Babai's Nearest Plane algorithm [5] (denoted by NP in the following) is an important building block of the Hybrid Attack. For more details on the algorithm we refer to Babai's original work [5] or Lindner and Peikert's work [25]. We use the Nearest Plane algorithm in a black box manner. For the reader it is sufficient to know the following. The input for the Nearest Plane algorithm is a lattice basis $\mathbf{B} \subset \mathbb{Z}^m$ and a target vector $\mathbf{t} \in \mathbb{R}^m$ and the corresponding output is a vector $\mathbf{e} \in \mathbb{R}^m$ such that $\mathbf{t} - \mathbf{e} \in \Lambda(\mathbf{B})$. We denote the output by $\mathrm{NP}_{\mathbf{B}}(\mathbf{t}) = \mathbf{e}$. If there is no risk of confusion, we might omit the basis in the notation, writing $\mathrm{NP}(\mathbf{t})$ instead of $\mathrm{NP}_{\mathbf{B}}(\mathbf{t})$. The output of Nearest Plane algorithm satisfies the following condition, as shown in [6].

Lemma 1. *Let $\mathbf{B} \subset \mathbb{Z}^m$ be a lattice basis and $\mathbf{t} \in \mathbb{R}^m$ be a target vector. Then $\mathrm{NP}_{\mathbf{B}}(\mathbf{t})$ is the unique vector $\mathbf{e} \in \mathcal{P}(\overline{\mathbf{B}})$ that satisfies $\mathbf{t} - \mathbf{e} \in \Lambda(\mathbf{B})$, where $\overline{\mathbf{B}}$ is the Gram-Schmidt basis of $\mathbf{B}$.*

The lengths of the Gram-Schmidt vectors of a reduced basis can be estimated by the following heuristic (for more details, we refer to [25]).

Heuristic (Geometric Series Assumption (GSA))**.** *Let $\mathbf{B} \subset \mathbb{Z}^m$ be a reduced basis of some full-rank lattice with Hermite delta δ and let D denote the determinant of $\Lambda(\mathbf{B})$. Further let $\overline{\mathbf{b}_1}, \ldots, \overline{\mathbf{b}_m}$ denote the corresponding Gram-Schmidt vectors of $\mathbf{B}$. Then the length of $\overline{\mathbf{b}_i}$ is approximately*

$$\left\|\overline{\mathbf{b}_i}\right\| \approx \delta^{-2(i-1)+m} D^{\frac{1}{m}}.$$

3 The Hybrid Attack

In this section we present a generalized version of the Hybrid Attack to solve shortest vector problems. Our framework for the Hybrid Attack is the following: the task is to find a shortest vector $\mathbf{v}$ in a lattice Λ, given a basis of Λ of the form

$$\mathbf{B}' = \left(\begin{array}{c|c} \mathbf{B} & \mathbf{C} \\ \hline \mathbf{0} & \mathbf{I}_r \end{array}\right) \in \mathbb{Z}^{m \times m},$$

where $0 < r < m$ is the meet-in-the-middle dimension, $\mathbf{B} \in \mathbb{Z}^{(m-r)\times(m-r)}$, and $\mathbf{C} \in \mathbb{Z}^{(m-r)\times r}$. In Appendix A.1 we show that for q-ary lattices, where q is prime, one can always construct a basis of this form, provided that the determinant of the lattice is at most q^{m-r}. Additionally, in Section 5 we show that our this framework can be applied to many lattice-based cryptographic schemes.

The main idea of the attack is the following. Let $\mathbf{v}$ be a short vector contained in the lattice Λ. We split the short vector $\mathbf{v}$ into two parts $\mathbf{v} = (\mathbf{v}_l, \mathbf{v}_g)^t$ with $\mathbf{v}_l \in \mathbb{Z}^{m-r}$ and $\mathbf{v}_g \in \mathbb{Z}^r$. The second part $\mathbf{v}_g$ represents the part of $\mathbf{v}$ that is recovered by guessing (meet-in-the-middle) during the attack, while the first part $\mathbf{v}_l$ is recovered with lattice techniques (solving BDD problems). Because of the special form of the basis $\mathbf{B}'$, we have that

$$\mathbf{v} = \begin{pmatrix} \mathbf{v}_l \\ \mathbf{v}_g \end{pmatrix} = \mathbf{B}' \begin{pmatrix} \mathbf{x} \\ \mathbf{v}_g \end{pmatrix} = \begin{pmatrix} \mathbf{B}\mathbf{x} + \mathbf{C}\mathbf{v}_g \\ \mathbf{v}_g \end{pmatrix}$$

for some vector $\mathbf{x} \in \mathbb{Z}^{m-r}$, hence $\mathbf{C}\mathbf{v}_g = -\mathbf{B}\mathbf{x} + \mathbf{v}_l$. This means $\mathbf{C}\mathbf{v}_g$ is close to the lattice $\Lambda(\mathbf{B})$, since it only differs from the lattice by the short vector $\mathbf{v}_l$, and therefore $\mathbf{v}_l$ can be recovered solving a BDD problem if $\mathbf{v}_g$ is know. The idea now is that if we can correctly guess the vector $\mathbf{v}_g$, we can hope to find $\mathbf{v}_l$ using the Nearest Plane algorithm (see the Preliminaries) via $\mathrm{NP}_{\mathbf{B}}(\mathbf{C}\mathbf{v}_g) = \mathbf{v}_l$, which is the case if the basis $\mathbf{B}$ is sufficiently reduced. Solving the BDD problem using Nearest Plane is the lattice part of the attack. The lattice $\Lambda(\mathbf{B})$ in which we need to solve BDD has the same determinant as the lattice $\Lambda(\mathbf{B}')$ in which we want to solve SVP, but it has smaller dimension, i.e., $m - r$ instead of r. Therefore we expect the newly obtained BDD problem to be easier to solve than the original SVP instance.

In the following we explain how one can speed up the guessing part of the attack by Odlyzkos meet-in-the-middle approach. Using this technique one is able to reduce the number of necessary guesses to the square root of the number of guesses needed in a naive brute-force approach. Odlyzko's meet-in-the-middle attack on NTRU was first described in [23] and applied in the hybrid lattice-reduction and meet-in-the-middle attack against NTRU in [22]. The idea is that instead of guessing $\mathbf{v}_g$ directly in a large set M of possible vectors, we guess sparser vectors $\mathbf{v}'_g$ and $\mathbf{v}''_g$ in a smaller set N of vectors such that $\mathbf{v}'_g + \mathbf{v}''_g = \mathbf{v}_g$. In our attack the larger set M will be the set of all vectors with a fixed number $2c_i$ of the non-zero entries equal to i for all $i \in \{\pm 1, \ldots, \pm k\}$, where $k = \|\mathbf{v}_g\|_\infty$. The smaller set N will be the set of all vectors with only half as many, i.e., only c_i, of the non-zero entries equal to i for all $i \in \{\pm 1, \ldots, \pm k\}$. Assume that $\mathrm{NP}_{\mathbf{B}}(\mathbf{C}\mathbf{v}_g) = \mathbf{v}_l$. First, we guess vectors $\mathbf{v}'_g$ and $\mathbf{v}''_g$ in the smaller set N. We then compute $\mathbf{v}'_l = \mathrm{NP}_{\mathbf{B}}(\mathbf{C}\mathbf{v}'_g)$ and $\mathbf{v}''_l = \mathrm{NP}_{\mathbf{B}}(\mathbf{C}\mathbf{v}''_g)$. We hope that if $\mathbf{v}'_g + \mathbf{v}''_g = \mathbf{v}_g$, then also $\mathbf{v}'_l + \mathbf{v}''_l = \mathbf{v}_l$, i.e., that Nearest Plane is additively homomorphic on those inputs. The probability that this additive property holds is one crucial element in the runtime analysis of the attack. We further need to

detect when this property holds during the attack, i.e., we need to be able to recognize matching vectors $\mathbf{v}'_g$ and $\mathbf{v}''_g$ with $\mathbf{v}'_g + \mathbf{v}''_g = \mathbf{v}_g$ and $\mathbf{v}'_l + \mathbf{v}''_l = \mathbf{v}_l$, which we call a collision. In order to do so, we store $\mathbf{v}'_g$ and $\mathbf{v}''_g$ in (hash) boxes whose addresses depend on $\mathbf{v}'_l$ and $\mathbf{v}''_l$, respectively, such that they collide in at least one box. To define those addresses properly, note that in case of a collision we have $\mathbf{v}'_l = -\mathbf{v}''_l + \mathbf{v}_l$. Thus $\mathbf{v}'_l$ and $-\mathbf{v}''_l$ differ only by a vector of infinity norm $y = \|\mathbf{v}_l\|_\infty$. Therefore, the addresses must be crafted such that for any $\mathbf{x} \in \mathbb{Z}^m$ and $\mathbf{z} \in \mathbb{Z}^m$ with $\|\mathbf{z}\|_\infty \leq y$ it holds that the intersection of the addresses of $\mathbf{x}$ and $\mathbf{x} + \mathbf{z}$ is non-empty, i.e., $\mathcal{A}_{\mathbf{x}}^{(m,y)} \cap \mathcal{A}_{\mathbf{x}+\mathbf{z}}^{(m,y)} \neq \emptyset$. Furthermore, the set of addresses should not be unnecessarily large so the hash tables do not grow too big and unwanted collisions are unlikely to happen. The following definition satisfies these properties, as can easily be verified.

Definition 1. *Let $m, y \in \mathbb{N}$. For a vector $\mathbf{x} \in \mathbb{Z}^m$ the set $\mathcal{A}_{\mathbf{x}}^{(m,y)} \subset \{0,1\}^m$ is defined as*

$$\mathcal{A}_{\mathbf{x}}^{(m,y)} = \left\{ \mathbf{a} \in \{0,1\}^m \middle| \begin{array}{l} (\mathbf{a})_i = 1 \text{ if } (\mathbf{x})_i > \lceil \frac{y}{2} - 1 \rceil \text{ for } i \in \{1, \ldots, m\}, \\ (\mathbf{a})_i = 0 \text{ if } (\mathbf{x})_i < -\lfloor \frac{y}{2} \rfloor \text{ for } i \in \{1, \ldots, m\} \end{array} \right\}.$$

We illustrate Definition 1 with some examples.

Example. *Let $m = 5$ be fix. For varying bounds y and input vectors $\mathbf{x}$ we have*

$$\begin{aligned}
\mathcal{A}_{(7,0,-1,1,-5)}^{(5,1)} &= \{(1,0,0,1,0), (1,1,0,1,0)\} \\
\mathcal{A}_{(8,0,-1,1,-2)}^{(5,2)} &= \{(1,0,0,1,0), (1,1,0,1,0), (1,0,1,1,0), (1,1,1,1,0)\} \\
\mathcal{A}_{(2,-1,9,1,-2)}^{(5,3)} &= \{(1,0,1,0,0), (1,0,1,1,0), (1,1,1,0,0), (1,1,1,1,0)\} \\
\mathcal{A}_{(2,-5,0,7,-2)}^{(5,4)} &= \{(1,0,0,1,0), (1,0,0,1,1), (1,0,1,1,0), (1,0,1,1,1)\}
\end{aligned}$$

The Hybrid Attack on SVP without precomputation is presented in Algorithm 1. A list of the attack parameters and the parameters used in the runtime analysis of the attack and their meaning is given in Table 1. In order to increase the chance of Algorithm 1 being successful one performs a basis reduction step as precomputation. Therefore, the complete Hybrid Attack, presented in Algorithm 2, is in fact a combination of a basis reduction step and Algorithm 1.

The Hybrid Attack on BDD

The Hybrid Attack can also be applied to BDD instead of SVP by rewriting a BDD instance into an SVP instance. This can be done in the following way (see for example [1]). Let $\mathbf{B}'$ be a lattice basis of the form

$$\mathbf{B}' = \left(\begin{array}{c|c} \mathbf{B} & \mathbf{C} \\ \hline \mathbf{0} & \mathbf{I}_r \end{array} \right) \in \mathbb{Z}^{m \times m},$$

Algorithm 1: The Hybrid Attack on SVP without basis reduction

Input : $m, r \in \mathbb{N}$ with $r < m$, $y, k \in \mathbb{N}$, $c_{-k}, \ldots, c_k \in \mathbb{N}_0$ with $r = \sum_{i=-k}^{k} c_i$,
$\mathbf{B}' = \left(\begin{array}{c|c} \mathbf{B} & \mathbf{C} \\ \hline \mathbf{0} & \mathbf{I}_r \end{array}\right) \in \mathbb{Z}^{m \times m}$, where $\mathbf{B} \in \mathbb{Z}^{(m-r)\times(m-r)}$ and $\mathbf{C} \in \mathbb{Z}^{(m-r)\times r}$

while *true* **do**
  guess $\mathbf{v}'_g \in \{-k, \ldots, k\}^r$ with exactly c_i entries equal to i for all $i \in \{-k, \ldots, k\}$;
  calculate $\mathbf{v}'_l = \mathrm{NP}_{\mathbf{B}}(\mathbf{C}\mathbf{v}'_g) \in \mathbb{Z}^{m-r}$;
  store $\mathbf{v}'_g$ in all the boxes addressed by $\mathcal{A}_{\mathbf{v}'_l}^{(m-r,y)} \cup \mathcal{A}_{-\mathbf{v}'_l}^{(m-r,y)}$;
  for *all* $\mathbf{v}''_g \neq \mathbf{v}'_g$ *in all the boxes addressed by* $\mathcal{A}_{\mathbf{v}'_l}^{(m-r,y)} \cup \mathcal{A}_{-\mathbf{v}'_l}^{(m-r,y)}$ **do**
    set $\mathbf{v}_g = \mathbf{v}'_g + \mathbf{v}''_g$ and calculate $\mathbf{v}_l = \mathrm{NP}_{\mathbf{B}}(\mathbf{C}\mathbf{v}_g) \in \mathbb{Z}^{m-r}$;
    if $\mathbf{v} = \begin{pmatrix} \mathbf{v}_l \\ \mathbf{v}_g \end{pmatrix} \in \Lambda(\mathbf{B}')$ *and* $\|\mathbf{v}_l\|_\infty \leq y$ *and* $\|\mathbf{v}_g\|_\infty \leq k$ **then**
      return $\mathbf{v}$;

Algorithm 2: The Hybrid Attack on SVP including basis reduction

Input : $m, r \in \mathbb{N}$ with $r < m$, $y, k \in \mathbb{N}$, $c_{-k}, \ldots, c_{-1}, c_1, \ldots, c_k \in \mathbb{N}_0$ with $r = \sum_{i=-k}^{k} c_i$,
$\mathbf{B}' = \left(\begin{array}{c|c} \mathbf{B} & \mathbf{C} \\ \hline \mathbf{0} & \mathbf{I}_r \end{array}\right) \in \mathbb{Z}^{m \times m}$, where $\mathbf{B} \in \mathbb{Z}^{(m-r)\times(m-r)}$ and $\mathbf{C} \in \mathbb{Z}^{(m-r)\times r}$

reduce $\mathbf{B}$ to some basis $\tilde{\mathbf{B}}$;
run Algorithm 1 on input $m, r, y, k, c_{-k}, \ldots, c_{-1}, c_1, \ldots, c_k, \left(\begin{array}{c|c} \tilde{\mathbf{B}} & \mathbf{C} \\ \hline \mathbf{0} & \mathbf{I}_r \end{array}\right)$;

with $\mathbf{B} \in \mathbb{Z}^{(m-r)\times(m-r)}, \mathbf{C} \in \mathbb{Z}^{(m-r)\times r}$ and let $\mathbf{t}$ be a target vector for BDD. Suppose $\mathbf{t} - \mathbf{v} \in \Lambda(\mathbf{B}')$, where $\mathbf{v}$ is the short (bounded) vector we are looking for. Then the short vector $(\mathbf{v}, 1)^t$ is contained in the lattice $\Lambda(\mathbf{B}'')$ spanned by

$$\mathbf{B}'' = \left(\begin{array}{c|c} \mathbf{B}' & \mathbf{t} \\ \hline \mathbf{0} & 1 \end{array}\right) \in \mathbb{Z}^{(m+1)\times(m+1)},$$

which is of the required form for the Hybrid Attack on SVP. Therefore we can apply the Hybrid Attack on SVP to find $(\mathbf{v}, 1)^t$, solving the BDD problem. The SVP lattice $\Lambda(\mathbf{B}'')$ has the same determinant as the BDD lattice $\Lambda(\mathbf{B}')$ and dimension $m + 1$ instead of m. However, the additional dimension can be ignored, since we know the last entry of $(\mathbf{v}, 1)^t$ and therefore do not have to guess it during the meet-in-the-middle phase. Note that by definition of BDD it is very likely that $\pm\mathbf{v}$ are the only short vectors in the lattice $\Lambda(\mathbf{B}'')$. By fixing the last coordinate to be plus one, only $\mathbf{v}$, not also $-\mathbf{v}$, can be found by the attack.

Parameter	Meaning
m	lattice dimension
r	meet-in-the-middle dimension
$\mathbf{B}'$	lattice basis of the whole lattice
$\mathbf{B}$	partially reduced lattice basis of the sublattice
c_i	number of i-entries guessed during attack
y	infinity norm bound on $\mathbf{v}_l$
k	infinity norm bound on $\mathbf{v}_g$
Y	expected Euclidean norm of $\mathbf{v}_l$
R_i	Gram-Schmidt lengths corresponding to $\mathbf{B}$
r_i	scaled Gram-Schmidt lengths corresponding to $\mathbf{B}$

Table 1. Attack parameters and parameters in the runtime analysis

4 Analysis

In this section we analyze the runtime of the Hybrid Attack. First, in our Main Result in Section 4.1, we estimate the runtime of the attack in case sufficient success conditions are satisfied. In Section 4.2, we then show how to determine the probability that those sufficient conditions are satisfied, i.e., how to determine (a lower bound on) the success probability. We conclude the runtime analysis of the attack by showing how to optimize the attack parameters to minimize its runtime in Section 4.3. We end the section by highlighting typical flaws of previous analyses of the Hybrid Attack, see Section 4.4. This showcases the improvements achieved by our new, precise analysis of the attack. Our new analysis is more detailed than all previous analyses of the Hybrid Attack, while at the same time applicable to a wider range of attack scenarios.

4.1 Runtime Analysis

We now present our main result about the runtime of the generalized Hybrid Attack. It shows that under sufficient conditions the attack is successful and estimates the expected runtime.

Main Result. *Let all inputs be denoted as in Algorithm 1,* $Y \in \mathbb{R}_{\geq 0}$*, and let* $R_1, \ldots, R_{m-r}$ *denote the lengths of the Gram-Schmidt basis vectors of the basis* $\mathbf{B}$*. Further let* $S \subset \Lambda(\mathbf{B}')$ *denote the set of all non-zero lattice vectors* $\mathbf{v} = (\mathbf{v}_l, \mathbf{v}_g)^t \in \Lambda(\mathbf{B}')$*, where* $\mathbf{v}_l \in \mathbb{Z}^{m-r}$ *and* $\mathbf{v}_g \in \mathbb{Z}^r$ *with* $\|\mathbf{v}_l\|_\infty \leq y$*,* $\|\mathbf{v}_l\| \approx Y$*,* $\|\mathbf{v}_g\|_\infty \leq k$*, exactly* $2c_i$ *entries of* $\mathbf{v}_g$ *are equal to* i *for all* $i \in \{\pm 1, \ldots \pm k\}$*, and* $\mathrm{NP}_{\mathbf{B}}(\mathbf{C}\mathbf{v}_g) = \mathbf{v}_l$*. Assume that the set* S *is non-empty.*

Then Algorithm 1 is successful and the expected number of loops can be estimated by

$$L = \binom{r}{c_{-k}, \ldots, c_k} \left(p \cdot |S| \cdot \prod_{i \in \{\pm 1, \ldots, \pm k\}} \binom{2c_i}{c_i} \right)^{-\frac{1}{2}},$$

where

$$p = \prod_{i=1}^{m-r} \left(1 - \frac{1}{r_i B(\frac{(m-r)-1}{2}, \frac{1}{2})} \int_{-r_i-1}^{-r_i} \int_{\max(-1, z-r_i)}^{z+r_i} (1-t^2)^{\frac{(m-r)-3}{2}} dt dz\right),$$

$B(\cdot,\cdot)$ denotes the Euler beta function (see [28]), and

$$r_i = \frac{R_i}{2Y} \quad \textit{for all } i \in \{1, \ldots, m-r\}.$$

Furthermore, the expected number of operations of Algorithm 1 for security under- and overestimates can be estimated by

$$T_{\mathsf{hyb,under}} = (m-r)/2^{1.06} L \quad \textit{and} \quad T_{\mathsf{hyb,over}} = (m-r)^2/2^{1.06} L.$$

In the following remark we explain the meaning of the (attack) parameters that appear in the Main Result in more detail.

Remark 1. 1) The parameters r, y, k, $c_{-k}, \ldots, c_k$ are the attack parameters that can be chosen by the attacker. The meet-in-the-middle dimension and the remaining lattice dimension are determined by the parameter r. The remaining parameters must be chosen in such a way that the requirements of the Main Result are likely to be fulfilled in order to obtain a high success probability of the attack. Choosing those parameters depends heavily on the distribution of the short vectors $\mathbf{v} \in S$. In order to obtain more flexibility, this distribution is not specified in the Main Result. However, in Section 5 we show how one can choose the attack parameters and calculate the success probability for several distributions arising in various cryptographic schemes. At this point we only want to remark that y should be (an upper bound on) $\|\mathbf{v}_l\|_\infty$, k (an upper bound on) $\|\mathbf{v}_g\|_\infty$, and $2c_i$ the (expected) number of entries of $\mathbf{v}_g$ that is equal to i for $i \in \{\pm 1, \ldots, \pm k\}$.

2) The attacker can further influence the lengths $R_1, \ldots, R_{m-r}$ of the Gram-Schmidt vectors by providing a different basis than $\mathbf{B}$ with Gram-Schmidt lengths that lead to a more efficient attack. This is typically done by performing a basis reduction on $\mathbf{B}$ or parts of $\mathbf{B}$ as precomputation, see Algorithm 2. The lengths of the Gram-Schmidt vectors achieved by the basis reduction with Hermite delta δ are typically estimated by the GSA (see the Preliminaries). However, for q-ary lattices the GSA needs to be modified in order to accurately reflect reality. For further details, see Appendix A.2. Notice that spending more time on basis reduction increases the probability p in the Main Result and the probability that the condition $\mathrm{NP}_{\mathbf{B}}(\mathbf{C}\mathbf{v}_g) = \mathbf{v}_l$ holds, as can be seen later in this section and Section 4.2.

3) Because of the previous remark, the complete attack – presented in Algorithm 2 – is actually a combination of precomputation (basis reduction) and Algorithm 1. Therefore the runtime of both steps must be considered and they have to be balanced in order to estimate the total runtime. We show how to optimize the total runtime in Section 4.3.

In the following we show how the Main Result can be derived. For the rest of this section let all notations be as in the Main Result. We further assume in the following that the assumption of the Main Result, i.e., $S \neq \emptyset$, is satisfied. We first provide the following useful definition already given in [22] and [11]. We use the notation of [11].

Definition 2. *Let $n \in \mathbb{N}$. A vector $\mathbf{x} \in \mathbb{Z}^n$ is called $\mathbf{y}$-admissible for some vector $\mathbf{y} \in \mathbb{Z}^n$ if $\mathrm{NP}(\mathbf{x}) = \mathrm{NP}(\mathbf{x} - \mathbf{y}) + \mathbf{y}$.*

This means, that if $\mathbf{x}$ is $\mathbf{y}$-admissible then $\mathrm{NP}(\mathbf{x})$ and $\mathrm{NP}(\mathbf{x} - \mathbf{y})$ yield the same lattice vector. We recall the following Lemma from [11] about Definition 2. It showcases the relevance of the definition by relating it to the equation $\mathrm{NP}(\mathbf{t}_1) + \mathrm{NP}(\mathbf{t}_2) = \mathrm{NP}(\mathbf{t}_1 + \mathbf{t}_2)$, which is necessary to hold for our attack to work.

Lemma 2. *[Lemma 2 of [11]] Let $\mathbf{t}_1 \in \mathbb{R}^n, \mathbf{t}_2 \in \mathbb{R}^n$ be two arbitrary target vectors. Then the following are equivalent.*

1. $\mathrm{NP}(\mathbf{t}_1) + \mathrm{NP}(\mathbf{t}_2) = \mathrm{NP}(\mathbf{t}_1 + \mathbf{t}_2)$.
2. $\mathbf{t}_1$ *is* $\mathrm{NP}(\mathbf{t}_1 + \mathbf{t}_2)$*-admissible.*
3. $\mathbf{t}_2$ *is* $\mathrm{NP}(\mathbf{t}_1 + \mathbf{t}_2)$*-admissible.*

Success of the Attack and Number of Loops

We now estimate the expected number of loops in case Algorithm 1 terminates. In each loop of the algorithm we sample a vector $\mathbf{v}'_g$ in the set

$$W = \{\mathbf{w} \in \mathbb{Z}^r \mid \text{exactly } c_i \text{ entries of } \mathbf{w} \text{ are equal to } i \quad \forall i \in \{-k, \ldots, k\}\}.$$

The attack succeeds if $\mathbf{v}'_g \in W$ and $\mathbf{v}''_g \in W$ such that $\mathbf{v}'_g + \mathbf{v}''_g = \mathbf{v}_g$ and $\mathrm{NP}_{\mathbf{B}}(\mathbf{C}\mathbf{v}'_g) + \mathrm{NP}_{\mathbf{B}}(\mathbf{C}\mathbf{v}''_g) = \mathbf{v}_l$ for some vector $\mathbf{v} = (\mathbf{v}_l, \mathbf{v}_g)^t \in S$ are sampled in different loops of the algorithm. By Lemma 2 the second condition is equivalent to the fact that $\mathrm{NP}_{\mathbf{B}}(\mathbf{C}\mathbf{v}'_g)$ is $\mathbf{v}_l$-admissible. We assume that the algorithm only succeeds in this case. We are therefore interested in the following subset of W:

$$V = \left\{ \mathbf{w} \in W \middle| \begin{array}{c} \mathbf{v}_g - \mathbf{w} \in W \text{ and } \mathrm{NP}_{\mathbf{B}}(\mathbf{C}\mathbf{w}) \text{ is } \mathbf{v}_l\text{-admissible} \\ \text{for some } \mathbf{v} = (\mathbf{v}_l, \mathbf{v}_g)^t \in S \end{array} \right\}.$$

For all $\mathbf{v} = (\mathbf{v}_l, \mathbf{v}_g)^t \in S$, with $\mathbf{v}_l \in \mathbb{Z}^{m-r}$ and $\mathbf{v}_g \in \mathbb{Z}^r$ let $p(\mathbf{v})$ denote the probability

$$p(\mathbf{v}) = \Pr_{\mathbf{w} \leftarrow W}[\mathrm{NP}_{\mathbf{B}}(\mathbf{C}\mathbf{w}) \text{ is } \mathbf{v}_l\text{-admissible}]$$

and $p_1(\mathbf{v})$ denote the probability

$$p_1(\mathbf{v}) = \Pr_{\mathbf{w} \leftarrow W}[\mathbf{v}_g - \mathbf{w} \in W].$$

By construction we have that $p_1(\mathbf{v})$ is constant for all $\mathbf{v} \in S$, so we can simply write p_1 instead of $p_1(\mathbf{v})$. We make the following reasonable assumption on $p(\mathbf{v})$ and p_1.

Assumption 1. *For all* $\mathbf{v} = (\mathbf{v}_l, \mathbf{v}_g)^t \in S$*, with* $\mathbf{v}_l \in \mathbb{Z}^{m-r}$ *and* $\mathbf{v}_g \in \mathbb{Z}^r$ *we assume that the independence condition*

$$p(\mathbf{v}) = \Pr_{\mathbf{w} \leftarrow W}[\mathrm{NP}_{\mathbf{B}}(\mathbf{Cw}) \text{ is } \mathbf{v}_l\text{-admissible} | \mathbf{v}_g - \mathbf{w} \in W]$$

holds, where $\overline{\mathbf{B}}$ *is the Gram-Schmidt basis of* $\mathbf{B}$*. We further assume that* $p(\mathbf{v})$ *is equal to some constant probability* p *for all* $\mathbf{v} \in S$*.*

Based on Assumption 1, we can make the following reasonable assumption.

Assumption 2. *We assume that*

$$\frac{|V|}{|W|} = \Pr_{\mathbf{w} \leftarrow W}[\mathbf{w} \in V] = p_1 p |S|.$$

From Assumption 2 it follows that $|V| = p_1 p |W||S|$. The probability p_1 is calculated by

$$p_1 = \frac{\prod\limits_{i \in \{\pm 1, \ldots, \pm k\}} \binom{2c_i}{c_i}}{|W|}, \quad \text{where} \quad |W| = \binom{r}{c_{-k}, \ldots, c_k}.$$

We further make the following assumption, which is fulfilled unless the probability p is extremely small (p is calculated later).

Assumption 3. *We assume that* $V \neq \emptyset$*.*

Assumption 3 implies that the attack is successful, since by Lemma 2 if $\mathbf{v}'_g \in V$ then also $\mathbf{v}''_g = \mathbf{v}_g - \mathbf{v}'_g \in V$ for all $\mathbf{v} = (\mathbf{v}_l, \mathbf{v}_g)^t \in S$. Such two vectors $\mathbf{v}'_g$ and $\mathbf{v}''_g$ in V will eventually be guessed in two separate loops of the algorithm and they are recognized as a collision, since by the assumption $\|\mathbf{v}_l\|_\infty \leq y$ of the Main Result they share at least one common address. By Assumption 2 we expect that during the algorithm we sample in V every $\frac{1}{p_1 p |S|}$ loops and by the birthday paradox we expect to find a collision $\mathbf{v}'_g \in V$ and $\mathbf{v}''_g \in V$ with $\mathbf{v}''_g + \mathbf{v}'_g = \mathbf{v}_g$ after $L \approx \frac{1}{p_1 p |S|} \sqrt{|V|}$ loops. In conclusion, we can estimate the expected number of loops by

$$L \approx \frac{\sqrt{|V|}}{p_1 p |S|} = \frac{\sqrt{|W|}}{\sqrt{p_1 p |S|}} = \binom{r}{c_{-k}, \ldots, c_k} \left(p|S| \prod_{i \in \{\pm 1, \ldots, \pm k\}} \binom{2c_i}{c_i} \right)^{-\frac{1}{2}}.$$

It remains to calculate the probability p. This can be done analogously as in Heuristic 3 of [11] and the calculations following it. For a detailed and convincing justification of the heuristic we refer to [11]. Following the calculations of [11] we obtain the following assumption.

Assumption 4. *We assume that the probability* p *is approximately*

$$p \approx \prod_{i=1}^{m-r} \left(1 - \frac{1}{r_i B(\frac{(m-r)-1}{2}, \frac{1}{2})} \int_{-r_i - 1}^{-r_i} \int_{\max(-1, z - r_i)}^{z + r_i} (1 - t^2)^{\frac{(m-r)-3}{2}} dt dz \right),$$

where $B(\cdot, \cdot)$ *and* $r_1, \ldots, r_{m-r}$ *are defined as in the Main Result.*

In order to calculate p one needs to estimate the lengths r_i, as discussed in the following remark.

Remark 2. Note that the probability p depends on the scaled Gram-Schmidt lengths r_i and therefore on the quality of the basis, i.e., its Hermite delta δ. For the scaling factor one simply needs to estimate $\|\mathbf{v}_l\|$. The Gram-Schmidt lengths obtained after performing a basis reduction with quality δ can be predicted by the GSA, see the Preliminaries. For q-ary lattices, this assumption needs to be modified appropriately, see Appendix A.2.

This concludes the estimation for the necessary number of loops.

Number of Operations

We now estimate the expected total number of operations of the Hybrid Attack under the conditions of the Main Result. In order to do so we need to estimate the runtime of one inner loop and multiply it by the expected number of loops. As in [22] and [11] we make the following assumption, which is plausible as long the sets of addresses are not extremely large.

Assumption 5. *We assume that the number of operations of one inner loop of Algorithm 1 is dominated by the number of operations of one Nearest Plane call.*

We remark that we see Assumption 5 as one of the more critical ones. Obviously, it does not hold for all parameter choices[2], but it is reasonable to believe that it holds for many relevant parameter sets, as claimed in [22]and [11]. However, the claim in [22] is based on the observation that for random vectors in $\mathbb{Z}_q^m$ it is highly unlikely that adding a binary vector will flip the sign of many coordinates (i.e., that a random vector in $\mathbb{Z}_q^m$ has many minus one coordinates). While this is true, the vectors in question are in fact not random vectors in $\mathbb{Z}_q^m$ but outputs of a Nearest Plane call, and thus potentially shorter than typical vectors in $\mathbb{Z}_q^m$. Therefore it can be expected that adding a binary vector will flip more signs. Additionally, in general it is not only a binary vector that is added, but a vector of infinity norm y, which makes flipping signs even more likely. However, we believe that Assumption 5 is still plausible for most relevant parameter sets and small y, and even in the worst case the assumption leads to more conservative security estimates.

In [18], Hirschhorn et al. give an experimentally verified number of bit operations (defined as in [24]) of one Nearest Plane call and state a conservative assumption on the runtime of Nearest Plane using precomputation. Based on their results, we make the following assumption for our security estimates (over and under).

[2] For instance, if the infinity norm y is too big, it is likely to have exponentially many addresses per vector and storing a vector at all addresses takes more time than a Nearest Plane call.

Assumption 6. *Let $d \in \mathbb{N}$ be the lattice dimension. For our security overestimates, we assume that the number of bit operations of one Nearest Plane call is approximately $d^2/2^{1.06}$. For our security underestimates, we assume that the number of bit operations of one Nearest Plane call is approximately $d/2^{1.06}$.*

In conclusion, under the conditions of the Main Result the expected number of operations of Algorithm 1 for security under- and overestimates is approximately

$$T_{\mathsf{hyb,under}} = (m-r)/2^{1.06}L \quad \text{and} \quad T_{\mathsf{hyb,over}} = (m-r)^2/2^{1.06}L.$$

4.2 Determining the success probability.

In the Main Result it is guaranteed that Algorithm 1 is successful if the lattice Λ contains a non-empty set S of short vectors of the form $\mathbf{v} = (\mathbf{v}_l, \mathbf{v}_g)^t$, where $\mathbf{v}_l \in \mathbb{Z}^{m-r}$ and $\mathbf{v}_g \in \mathbb{Z}^r$, with $\|\mathbf{v}_l\| \approx Y$, $\|\mathbf{v}_l\|_\infty \leq y$, $\|\mathbf{v}_g\|_\infty \leq k$, exactly $2c_i$ entries of $\mathbf{v}_g$ are equal to i for all $i \in \{\pm 1, \dots \pm k\}$, and $\mathrm{NP}_{\mathbf{B}}(\mathbf{C}\mathbf{v}_g) = \mathbf{v}_l$. In order to determine a lower bound on the success probability, one must calculate the probability that the set S of such vectors is non-empty, since

$$p_{\mathsf{succ}} \geq \Pr[S \neq \emptyset].$$

However, this probability depends heavily on the distribution of the short vectors contained in Λ and is therefore not done in the Main Result, allowing for more flexibility. In consequence, this analysis must be performed for the specific distribution at hand originating from the cryptographic scheme that is to be analyzed. The most involved part in calculating the success probability is typically calculating the probability p_{NP} that $\mathrm{NP}_{\mathbf{B}}(\mathbf{C}\mathbf{v}_g) = \mathbf{v}_l$. As shown in [11], the probability p_{NP} is approximately

$$p_{\mathrm{NP}} \approx \prod_{i=1}^{m} \left(1 - \frac{2}{B(\frac{(m-r)-1}{2}, \frac{1}{2})} \int_{-1}^{\max(-r_i,-1)} (1-t^2)^{\frac{(m-r)-3}{2}} dt\right),$$

where r_i are defined as in the Main Result and obtained as in Remark 2.

4.3 Optimizing the Runtime

The final step in our analysis is to determine the runtime of the complete Hybrid Attack (Algorithm 2) including precomputation, which involves the runtime of the basis reduction T_{red}, the runtime of the actual attack T_{hyb}, and the success probability p_{succ}. All these quantities depend on the attack parameter r and the quality of the basis $\mathbf{B}$ given by the lengths of the Gram-Schmidt vectors achieved by the basis reduction performed in the precomputation step of the attack. The quality of the basis can be measured by its Hermite Delta δ (see the Preliminaries). In order to unfold the full potential of the attack, one must

minimize the runtime over all possible attack parameters r and δ. For our security overestimates, we assume that the total runtime (which is to be minimized) is given by

$$T_{\mathsf{total,over}}(\delta, r) = \frac{T_{\mathsf{red,over}}(\delta, r) + T_{\mathsf{hyb,over}}(\delta, r)}{p_{\mathsf{succ}}(\delta, r)}.$$

For our security underestimates, we conservatively assume that given a reduced basis with quality δ it is significantly easier to find another reduced basis with same quality δ than it is to find one given an arbitrary non-reduced basis. We therefore assume that even if the attack is not successful and needs to be run again, the large precomputation cost for the basis reduction only needs to be paid once, and hence

$$T_{\mathsf{total,under}}(\delta, r) = T_{\mathsf{red,under}}(\delta, r) + \frac{T_{\mathsf{hyb,under}}(\delta, r)}{p_{\mathsf{succ}}(\delta, r)}.$$

In order to calculate $T_{\mathsf{total,under}}(\delta, r)$ and $T_{\mathsf{total,over}}(\delta, r)$ one must calculate $T_{\mathsf{hyb,under}}(\delta, r)$, $T_{\mathsf{hyb,over}}(\delta, r)$, $T_{\mathsf{red,under}}(\delta, r)$, $T_{\mathsf{red,over}}(\delta, r)$, and $p_{\mathsf{succ}}(\delta, r)$. How to calculate $T_{\mathsf{total,under}}(\delta, r)$ and $T_{\mathsf{total,over}}(\delta, r)$ is shown in the Main Result. The success probability $p_{\mathsf{succ}}(\delta, r)$ is calculated in Section 4.2.

Basis reduction. Estimating the necessary runtime $T_{\mathsf{red}}(\delta, r)$ for a basis reduction of quality δ is highly non-trivial and still an active research area. For our security overestimates we apply the following the approach. We first determine the (minimal) block size β necessary to achieve the targeted Hermite delta δ via

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

according to Chen's thesis [13] (see also [2, 3, 15]). We then use the BKZ 2.0 simulator of the full version of [14] to determine the corresponding necessary number of rounds k. Finally use the estimate

$$\mathrm{Estimate}_{\mathsf{over}}(\beta, n, k) = 0.187281\beta \log(\beta) - 1.0192\beta + \log(n \cdot k) + 16.1$$

provided in [2] to determine the (base-two) logarithm of the runtime, where n is the lattice dimension. For our implementations we used the publicly available sage code of the BKZ 2.0 simulator on van Vredendaal's website [31].

For the security underestimates we assume that only one round of BKZ 2.0 with the determined block size β is needed. The reason for this assumption is that one can use progressive BKZ strategies to reduce the number of rounds needed with blocksize β by running BKZ with block sizes smaller than β in advance, see [4,13]. Since BKZ with smaller block sizes is considerably cheaper, we do not consider the BKZ costs with smaller block sizes in our security underestimates. Furthermore, for our security underestimates we assume that the number of rounds can be brought down to one, giving

$$\mathrm{Estimate}_{\mathsf{under}}(\beta, n) = 0.187281\beta \log(\beta) - 1.0192\beta + \log(n + 1 - \beta) + 16.1.$$

Note that if someone wishes to replace the model of the behavior of basis reduction by a different one, this can simply be done while the rest of the analysis remains intact.

Runtime optimization. The optimization of the total runtime $T_{\mathsf{total}}(\delta, r)$ is performed in the following way. For each possible r we find the optimal δ_r that minimizes the runtime $T_{\mathsf{total}}(\delta, r)$. Consequently, the optimal runtime is given by $\min\{T_{\mathsf{total}}(\delta_r, r)\}$, the smallest of those minimized runtimes. Note that for fixed r the optimal δ_r for our security underestimates can easily be found in the following way. For fixed r the function $T_{\mathsf{red},\mathsf{under}}(\delta, r)$ is monotonically decreasing in δ and the function $\frac{T_{\mathsf{hyb},\mathsf{under}}(\delta,r)}{p_{\mathsf{succ}}(\delta,r)}$ is monotonically increasing in δ. Therefore $T_{\mathsf{total},\mathsf{under}}(\delta, r)$ is (close to) optimal when both those functions are balanced, i.e., take the same value. Thus the optimal δ_r can for example be found by a simple binary search.
For our security overestimates, we assume the function $\frac{T_{\mathsf{red},\mathsf{over}}(\delta,r)}{p_{\mathsf{succ}}(\delta,r)}$ is monotonically decreasing in δ in the relevant range, hence the optimal $T_{\mathsf{total},\mathsf{over}}(\delta, r)$ can be found by balancing the functions $\frac{T_{\mathsf{red},\mathsf{over}}(\delta,r)}{p_{\mathsf{succ}}(\delta,r)}$ and $\frac{T_{\mathsf{hyb},\mathsf{over}}(\delta,r)}{p_{\mathsf{succ}}(\delta,r)}$ as above. Note that this assumption might note be true, but it surely leads to upper bounds on the optimal runtime of the attack.

4.4 Typical Flaws in Previous Analyses of the Hybrid Attack

We end this section by listing the major flaws we frequently found in previous analyses of the Hybrid Attack which lead to unreliable and inaccurate security estimates. We also found several minor flaws in previous analyses, but in this section we restrict our focus to the flaws we think have the most influence on the security estimates. We remark that some flaws lead to overestimating the security of the schemes and others to underestimating it. In some analyses, both types of flaws occurred at the same time and somewhat magically almost canceled out each others effect on the security estimates for some parameter sets. Even though the security estimates in those cases are not wrong per se, they can not be relied upon, since without further analysis it is not clear if the security estimates are correct, over-, or underestimates. We straighten out this unsatisfying state of affairs by providing updated security estimates for various cryptographic schemes using our newly developed, detailed, and accurate way to analyze the Hybrid Attack, see Section 5.

Ignoring the probability p. One of the most frequently encountered problems that appeared in several works is the lack of a (correct) calculation of the probability p defined in Assumption 1. As can be seen in the Main Result, this probability plays a crucial role in the runtime analysis of the attack. Nevertheless, in several works [9, 16, 19, 20, 30] the authors completely ignore the presence of this probability by setting $p = 1$ for the sake of simplicity. However, even though

we took the probability into account when optimizing the attack parameters[3], for the parameter sets we analyze in Section 5 the probability p was sometimes as low as 2^{-80}, see Table 3. Note that the wrong assumption $p = 1$ gives more power to the attacker, since it assumes that collisions can always be detected by the attacker although this is not the case, resulting in security underestimates. We also remark that in some works the probability p is not completely ignored but determined in a purely experimental way [22] or calculated using additional unnecessary assumptions [18], introducing inaccuracies into the analysis.

Unnecessary demands on the basis reduction. In most works [9, 16, 18–20, 22, 30], the authors demand a sufficiently good basis reduction such that the Nearest Plane algorithm must unveil the searched short vector (or at least with very high probability). To be more precise, Lemma 1 of [22] is used to determine what sufficiently good exactly means. In our opinion, this demand, which leads to overestimating the security of the schemes, is unreasonable, and instead we account for the probability of this event in the success probability. In our opinion, this approach reflects the attacker's power in a more accurate way. In addition, in most cases Lemma 1 of [22] is not even applicable in the way it is claimed in several works. We briefly sketch way this is the case. Often, Lemma 1 of [22] is applied to determine the necessary quality of a reduced basis such that Nearest Plane (on correct input) unveils a vector $\mathbf{v}$ of infinity norm at most y. However, this lemma is only applicable if the basis matrix is in triangular form, which is not the case is general. Therefore, one needs to transform the basis with an orthonormal matrix $\mathbf{Y}$ in order to obtain a triangular basis. This basis however does not span the same lattice but an isomorphic one, which contains the transformed vector $\mathbf{vY}$, but (in general) not the vector $\mathbf{v}$. While the transformation $\mathbf{Y}$ preserves the Euclidean norm of the vector $\mathbf{v}$, it does not preserve its infinity norm. Therefore the lemma can not be applied with the same infinity norm bound y, which is done in most works. In fact, in the worst case the new infinity norm bound can be up to $\sqrt{m}y$, where m is the lattice dimension. In consequence one would have to apply Lemma 1 of [22] with infinity norm bound $\sqrt{m}y$ instead of y, which demands a much better basis reduction. This problem is already mentioned – but not solve – in [30]. We remark that assuming one can apply Lemma 1 of [22] with the same infinity norm bound y anyways is a conservative, but not realistic assumption, that is no longer needed in our analysis.

Missing or incorrect optimization. In some works such as [16, 22] the optimization of the attack parameters is either completely missing, ignoring the fact that there is a trade-off between the time spent on basis reduction and the actual attack, or incorrect. As a result one only obtains upper bounds on the estimated security level but not precise estimates.

[3] If the probability p is ignored in the optimization process, it can even be lower for the "optimized" attack parameters.

Other inaccuracies. Further inaccuracies we encountered include the following.

(1) Implicitly assuming that the meet-in-the-middle part $\mathbf{v}_g$ of the short vector has the right number of i-entries for each i [9, 16, 19, 20, 30]. This is not the case in general and therefore needs to be accounted for in the success probability.
(2) Simplifying the structure of the secret key when convenient in order to ease the analysis [20,30]. This can drastically change the norm of the secret vector and in consequence manipulate the runtime estimates.
(3) Assuming that an attacker could maybe utilize some algebraic structure without any evidence that this is the case [18,20,30]. This assumption results in security underestimates if the assumption is in fact wrong.
(4) Assuming that the GSA holds for q-ary lattices without modification [10]. We show how the GSA can be modified for q-ary lattices in Appendix A.2.

5 Updating Security Estimates Against the Hybrid Attack

In the recent years, the Hybrid Attack has been applied to various lattice-based cryptographic schemes in order to evaluate their security. However, most of these security estimates are unreliable due to flaws in their analysis of the Hybrid Attack. Therefore, the security estimates must be updated in such a way that they can be relied upon. In Section 4 we presented a detailed way to accurately estimate the runtime of the Hybrid Attack. In this section we apply the Hybrid Attack to various cryptographic schemes and correctly analyze its runtime in order to reevaluate their security and derive updated and reliable security estimates.
The section is structures as follows. Each scheme is analyzed in a separate subsection. We begin with subsections on the encryption schemes NTRU, NTRU prime and R-BinLWEEnc and end with subsections on the signature schemes BLISS and GLP. In each subsection we first give a brief introduction to the scheme and explain how the previous security analysis against the Hybrid Attack is flawed. We then apply the Hybrid Attack to the scheme and analyze its complexity according to Section 4. This analysis is performed the following four steps steps.

1) **Constructing the lattice.** We first construct a lattice of the required form which contains the secret key as a short vector.
2) **Determining the attack parameters.** We find suitable attack parameters c_i (depending on the meet-in-the-middle dimension r), infinity norm bounds y and k, and estimate the Euclidean Y.
3) **Determining the success probability.** We determine the success probability of the attack according to Section 4.2.
4) **Optimizing the runtime.** We optimize the runtime of the attack for our security under- and overestimate according to Section 4.3.

We end each subsection by providing a table of updated security estimates against the Hybrid Attack obtained by our analysis. In the tables we also provide the optimal attack parameters (δ_r, r) derived by our optimization process and the corresponding probability p with whom collisions can be detected. For comparison, we further provide the security estimates of the previous works. In our runtime optimization of the attack we optimized with a precision of up to one bit. As a result there may not be one unique optimal attack parameter pair (δ_r, r) and for the table we simply pick one that minimizes the runtime (up to one bit precision).

5.1 NTRU

The NTRU encryption system was officially introduced in [21] and is one of the most important lattice-based encryption schemes today due to its high efficiency. The Hybrid Attack was first developed to attack NTRU [22] and has been applied to various proposed parameter sets since [18–20, 22, 30]. In this work we restrict our studies to the most recent parameter selection paper [20]. In [20], the authors analyze the Hybrid Attack making typical simplifying assumptions such as setting the probability p equal to one or demanding a certain quality of the basis reduction. Furthermore, for simplicity the authors sometimes treat the private keys as if they were trinary vectors, even though they are of the harder to analyze product form. In consequence we conclude that the security estimates given in [20] are not reliable. We therefore accurately reevaluate the security of the NTRU EESS # 1 parameter sets given in Table 3 of [20] in order to provide new, reliable security estimates.

Constructing the Lattice

The NTRU cryptosystem is defined over the ring $R_q = \mathbb{Z}_q[X]/(X^N - 1)$, where $N, q \in \mathbb{N}$ and N is prime. The parameters N and q are public. Furthermore there exist public parameters $d_1, d_2, d_3, d_g \in \mathbb{Z}$. For the parameter sets considered in [20], the private key is a pair of polynomials $(f, g) \in R_q^2$, where g is a trinary polynomial with exactly d_g+1 ones and d_g minus ones and $f = 1+3F$ invertible in R_q with $F = A_1A_2 + A_3$ for some trinary polynomials A_i with exactly d_i one and d_i minus one entries. The corresponding public key is $(1, h)$, where $h = f^{-1}g$. In the following we assume that h and 3 are invertible in R_q. We further identify polynomials with their coefficient vectors. We can recover the private key by finding the secret vector $\mathbf{v} = (\mathbf{F}, \mathbf{g})^t$.[4] Since $h = (1 + 3F)^{-1}g$ we have $3^{-1}h^{-1}g = F + 3^{-1}$ and therefore it holds that

$$\mathbf{v} + \begin{pmatrix} \mathbf{3}^{-1} \\ \mathbf{0} \end{pmatrix} = \begin{pmatrix} 3^{-1}\mathbf{h}^{-1}\mathbf{g} + q\mathbf{w} \\ \mathbf{g} \end{pmatrix} = \left(\begin{array}{c|c} q\mathbf{I}_n & 3^{-1}\overline{\mathbf{H}} \\ \hline \mathbf{0} & \mathbf{I}_n \end{array}\right) \begin{pmatrix} \mathbf{w} \\ \mathbf{g} \end{pmatrix}$$

[4] Note that we put $\mathbf{g}$ in the half of the vector $\mathbf{v}$ that is guessed in the meet-in-the-middle part of the attack. The reason for this choice is that we exactly know the structure of $\mathbf{g}$ but not the structure of the product form polynomial $\mathbf{F}$.

for some $\mathbf{w} \in \mathbb{Z}^n$, where $\overline{\mathbf{H}}$ is the rotation matrix of $\mathbf{h}^{-1}$. Hence $\mathbf{v}$ can be recovered by solving BDD on input $(-\mathbf{3}^{-1}, \mathbf{0})^t$ in the q-ary lattice

$$\Lambda = \Lambda\left(\left(\begin{array}{c|c} q\mathbf{I}_n & 3^{-1}\overline{\mathbf{H}} \\ \hline \mathbf{0} & \mathbf{I}_n \end{array}\right)\right),$$

since $(-\mathbf{3}^{-1}, \mathbf{0})^t - \mathbf{v} \in \Lambda$.[5] A similar way to recover the private key was already mentioned in [30]. The lattice Λ has dimension $2n$ and determinant q^n. Since we take the BDD approach for the Hybrid Attack, we assume that only $\mathbf{v}$, not its rotations or additive inverse, can be found by the attack, see Section 3. Hence we assume that the set S, as defined in the Main Result, contains of at most one element.

Determining the Attack Parameters

Let $\mathbf{v} = (\mathbf{F}, \mathbf{g})^t = (\mathbf{v}_l, \mathbf{v}_g)^t$ with $\mathbf{v}_l \in \mathbb{Z}^{2n-r}$ and $\mathbf{v}_g \in \mathbb{Z}^r$. Since $\mathbf{g}$ is a trinary vector, we can set the infinity norm bound k on $\mathbf{v}_g$ equal to one. In contrast, determining an infinity norm bound on the vector $\mathbf{v}_l$ is not that trivial, since $\mathbf{F}$ is not trinary but of product form. For a specific parameter set this can either be done theoretically or experimentally. The same holds for estimating the Euclidean norm of $\mathbf{v}_l$. For our runtime estimates we determined the expected Euclidean norm of $\mathbf{F}$ experimentally and set the expected Euclidean norm of $\mathbf{v}_l$ to

$$\|\mathbf{v}_l\| \approx \sqrt{\|\mathbf{F}\|^2 + \frac{n-r}{r} \cdot (2d_g + 1)}.$$

We set $2c_{-1} = \frac{r}{n} \cdot (d_g + 1)$ and $2c_1 = \frac{r}{n} \cdot d_g$ to be equal to the expected number of minus one entries and one entries, respectively, in $\mathbf{g}$.[6] For simplicity we assume that c_{-1} and c_1 are integers in the following in order to avoid writing down the rounding operates.

Determining the Success Probability

The next step is to determine the success probability p_{succ}, i.e., the probability that $\mathbf{v}$ has exactly $2c_{-1}$ entries equal to minus one, $2c_1$ entries equal to one, and $\mathrm{NP}_{\mathbf{B}}(\mathbf{C}\mathbf{v}_g) = \mathbf{v}_l$ holds, where $\mathbf{B}$ is as given in the Main Result. Assuming independence, the success probability is approximately

$$p_{\mathsf{succ}} = p_c \cdot p_{\mathrm{NP}},$$

[5] It is also possible to construct a lattice that contains $(\mathbf{f}, \mathbf{g})$ as a short vector instead. However, since $f = 1 + 3F$ has norm larger than F, this leads to a less efficient attack.

[6] Note that this must not necessarily be the optimal choice for the c_i. However, we expect that this choice comes very close to the optimal one and therefore restrict our studies to this case.

where p_c is the probability that $\mathbf{v}$ has exactly $2c_{-1}$ entries equal to minus one and $2c_1$ entries equal to one and p_{NP} is defined and calculated as in Section 4.2. Obviously, p_c is given by

$$p_c = \frac{\binom{r}{2\tilde{c_0}, 2c_{-1}, 2c_1}\binom{n-r}{d_0 - 2\tilde{c_0}, d_g - 2c_{-1}, d_g + 1 - 2c_1}}{\binom{n}{d_0, d_g, d_g + 1}},$$

where $2\tilde{c_0} = r - 2c_{-1} - 2c_1$ and $d_0 = n - (d_g + 1) - d_g$. As explained earlier, since we use the BDD approach of the Hybrid Attack, we assume that $|S| = 1$ in case the attack is successful.

Optimizing the Runtime

We determined the optimal attack parameters to estimate the minimal runtime of the Hybrid Attack for the NTRU EESS # 1 parameter sets given in Table 3 of [20]. The results, including the optimal r, corresponding δ_r, and resulting probability p that collisions can be found, are presented in Table 2. Our analysis shows that the security levels against the Hybrid Attack claimed in [20] are lower than the actual security levels for all parameter sets. In addition, our results show that for all of the analyzed parameter sets the Hybrid Attack does not perform better than a purely combinatorial meet-in-the-middle search, see Table 3 of [20]. Our results therefore disprove the common claim that the Hybrid Attack is necessarily the best attack on NTRU.

Parameter set	$\mathbf{n = 401}$	$\mathbf{n = 439}$	$\mathbf{n = 593}$	$\mathbf{n = 743}$
Optimal $r_{\mathsf{under}}/r_{\mathsf{over}}$	104/122	122/140	206/219	290/308
Optimal $\delta_{\mathsf{r,under}}$	1.00544	1.00509	1.00412	1.00352
Optimal $\delta_{\mathsf{r,over}}$	1.00552	1.00518	1.00420	1.00357
Corresponding $p_{\mathsf{under}}/p_{\mathsf{over}}$	$2^{-70}/2^{-43}$	$2^{-56}/2^{-47}$	$2^{-67}/2^{-62}$	$2^{-78}/2^{-69}$
Security under/over in bits	**145/162**	**165/182**	**249/267**	**335/354**
In [20] conserv./normal	116/127	133/145	204/236	280/330
$r_{\mathsf{under}}/r_{\mathsf{over}}$ used in [20]	154/166	175/192	264/303	360/423

Table 2. Optimal attack parameters and security levels against the Hybrid Attack for NTRU.

5.2 NTRU prime

The NTRU prime encryption scheme was recently introduced [9] in order to eliminate worrisome algebraic structures that exist within NTRU [21] or Ring-LWE based encryption schemes such as [3,26]. The authors considered the application

of the Hybrid Attack to their scheme to derive their security estimates. However, their analysis follows the methodology of [20] and is therefore flawed in the same way and consequently the security estimates are not reliable, see Section 5.1. We therefore reevaluate the security of NTRU prime, eliminating the flaws in the analysis and providing reliable security estimates.

Constructing the Lattice

The Streamlined NTRU prime family of cryptosystems is parameterized by three integers $(n, q, t) \in \mathbb{N}^3$, where n and q are odd primes. The base ring for Streamlined NTRU prime is $R_q = \mathbb{Z}_q[X]/(X^n - X - 1)$. The private key is (essentially) a pair of polynomials $(g, f) \in R_q^2$, where g is drawn uniformly at random from the set of all trinary polynomials and f is drawn uniformly at random from the set of all trinary polynomials with exactly $2t$ non-zero coefficients. The corresponding public key is $h = g(3f)^{-1} \in R_q$. In the following we identify polynomials with their coefficient vectors. As described in [9], the secret vector $\mathbf{v} = (\mathbf{g}, \mathbf{f})$ is contained in the q-ary lattice

$$\Lambda = \Lambda\left(\left(\begin{array}{c|c} q\mathbf{I}_n & 3\mathbf{H} \\ \hline \mathbf{0} & \mathbf{I}_n \end{array}\right)\right),$$

where $\mathbf{H}$ is the rotation matrix of h, since

$$\left(\begin{array}{c|c} q\mathbf{I}_n & 3\mathbf{H} \\ \hline \mathbf{0} & \mathbf{I}_n \end{array}\right)\begin{pmatrix}\mathbf{w}\\ \mathbf{f}\end{pmatrix} = \begin{pmatrix} q\mathbf{w} + 3\mathbf{hf} \\ \mathbf{f}\end{pmatrix} = \begin{pmatrix}\mathbf{g}\\ \mathbf{f}\end{pmatrix} = \mathbf{v}$$

for some $\mathbf{w} \in \mathbb{Z}^n$. The determinant of the lattice Λ is given by q^n and its dimension is equal to $2n$. Note that in the case of Streamlined NTRU prime the rotations of a trinary polynomial are not necessarily trinary, but it is likely the some are. The authors of [9] conservatively assume that the maximum number of good rotations of $\mathbf{v}$ that can be utilized by the attack is $n - t$, which we also assume in the following. Counting their additive inverses leaves us $2(n - t)$ short vectors that can be found by the attack.

Determining the Attack Parameters

Let $\mathbf{v} = (\mathbf{f}, \mathbf{g})^t = (\mathbf{v}_l, \mathbf{v}_g)^t$ with $\mathbf{v}_l \in \mathbb{Z}^{2n-r}$ and $\mathbf{v}_g \in \mathbb{Z}^r$. Since $\mathbf{v}$ is trinary, we can set the infinity norm bounds y and k equal to one. The expected Euclidean norm of $\mathbf{v}_l$ is given by

$$\|\mathbf{v}_l\| \approx \sqrt{\frac{2}{3}n + \frac{n-r}{n}2t}.$$

We set $2c_1 = 2c_{-1} = \frac{r}{n} \cdot \frac{t}{2}$ equal to the expected number of one entries (or minus one entries, respectively) in $\mathbf{f}$. For simplicity we assume that c_1 is an integer in the following.

Determining the Success Probability

Next, we determine the success probability $p_{\mathsf{succ}} = \Pr[S \neq \emptyset]$, where S denotes the following subset of the lattice Λ:

$$S = \left\{ \mathbf{w} \in \Lambda \;\middle|\; \begin{array}{ll} & \mathbf{w} = (\mathbf{w}_l, \mathbf{w}_g)^t \text{ with } \mathbf{w}_l \in \{0, \pm 1\}^{2n-r}, \mathbf{w}_g \in \{0, \pm 1\}^r, \\ & \text{exactly } 2c_i \text{ entries of } \mathbf{w}_g \text{ equal to } i \quad \forall i \in \{-1, 1\}, \\ & \mathrm{NP}_{\mathbf{B}}(\mathbf{C}\mathbf{w}_g) = \mathbf{w}_l \end{array} \right\},$$

where $\mathbf{B}$ is as defined in the Main Result. We assume that S is a subset of all the rotations of $\mathbf{v}$ that can be utilized by the attack and their additive inverses. In particular, we assume that S has at most $2(n-t)$ elements. Note that if some vector $\mathbf{w}$ is contained in S, then we also have $-\mathbf{w} \in S$. Assuming independence, the probability p_S that $\mathbf{v} \in S$ is approximately given by

$$p_S \approx \frac{\binom{r}{2\tilde{c_0}, 2c_{-1}, 2c_1} \binom{n-r}{2t-4c_1} 2^{2t-4c_1}}{\binom{n}{2t} 2^{2t}} \cdot p_{\mathrm{NP}},$$

where $d_0 = n - 2t$ and $2\tilde{c_0} = r - 4c_1$ and p_{NP} is defined and calculated as in Section 4.2. Assuming independence, all of the $n - t$ good rotations of $\mathbf{v}$ are contained in S with probability p_S as well. Therefore, the probability p_{succ} that we have at least one good rotation is approximately

$$p_{\mathsf{succ}} = \Pr[S \neq \emptyset] \approx 1 - (1 - p_S)^{n-t}.$$

Next, we estimate the size of the set S in the case $S \neq \emptyset$, i.e., Algorithm 1 is successful. In that case, at least one rotation is contained in S. Then also its additive inverse is contained in S, hence $|S| \geq 2$. We can estimate the size of S in case of success to be

$$|S| \approx 2 + 2(n - t - 1)p_S,$$

where p_S is defined as above.

Optimizing the Runtime

We applied our new techniques to estimate the minimal runtimes for several NTRU prime parameter sets proposed in Appendix D of [9]. Besides the "case study parameter set", for our analysis we picked one parameter set that offers the lowest bit security and one that offers the highest according to the analysis of [9]. Our resulting security estimates are presented in Table 3. Our analysis shows that the authors of [9] underestimate the security of their scheme for all parameter sets we evaluated.

Parameter set	$\mathbf{n = 607}$ $\mathbf{q = 18749}$	$\mathbf{n = 739}$ $\mathbf{q = 9829}$	$\mathbf{n = 929}$ $\mathbf{q = 12953}$
Optimal $r_{\mathsf{under}}/r_{\mathsf{over}}$	148/162	235/257	328/353
Optimal $\delta_{\mathsf{r,under}}$	1.00466	1.00405	1.00346
Optimal $\delta_{\mathsf{r,over}}$	1.00466	1.00407	1.00346
Corresponding $p_{\mathsf{under}}/p_{\mathsf{over}}$	$2^{-63}/2^{-54}$	$2^{-73}/2^{-60}$	$2^{-80}/2^{-65}$
Security under/over in bits	**197/211**	**258/273**	**346/363**
In [9]	128	228	310

Table 3. Optimal attack parameters and security levels against the Hybrid Attack for NTRU prime.

5.3 R-BinLWEEnc

In [10], Buchmann et al. presented R-BinLWEEnc, a lightweight public key encryption scheme based on binary Ring-LWE[7]. To determine the security of their scheme the authors evaluate the hardness of binary LWE against the Hybrid Attack. They use the methodology of [11]. However, they do not use the methodology of the updated full version of [11], but the original one, which makes an unreasonable assumption and is therefore not reliable and has been updated in the full version. For instance, the bit security of the R-BinLWEEnc-II parameter set should be updated from 84 bits to 103 bits when using the updated version of [11]. However, even the analysis of the Hybrid Attack provided in the updated version of [11] is not completely satisfying. This is due to two issues. First, the authors use the over-simplified formulas of [25] to estimate the runtime for basis reduction and the Nearest Plane algorithm, which do not provide accurate predictions (see for example [2]). Second, the authors do not take into considerations that the GSA needs to be modified for q-ary lattices to properly fit reality, see Appendix A.2. Therefore we reevaluate the security of binary LWE against the Hybrid Attack in order to obtain reliable security estimates for R-BinLWEEnc.

Constructing the Lattice

Let $m, n, q \in \mathbb{Z}$ with $m > n$ and $(\mathbf{A}, \mathbf{b}' = \mathbf{As} + \mathbf{e}' \mod q)$ be a binary LWE instance with $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$, $\mathbf{s} \in \mathbb{Z}_q^n$, and binary error $\mathbf{e}' \in \{0, 1\}$.[8] To obtain a more efficient attack, we first subtract the vector consisting of all 1/2-entries from both sides of the equation $\mathbf{b}' = \mathbf{As} + \mathbf{e}' \mod q$ to obtain a new LWE instance $(\mathbf{A}, \mathbf{b} = \mathbf{As} + \mathbf{e} \mod q)$, where $\mathbf{e} \in \{\pm 1/2\}^m$. In the following we only consider this transformed LWE instance with smaller error. Obviously $\mathbf{e}$ is contained in the q-ary lattice

$$\Lambda = \Lambda_q(\mathbf{A}') = \{\mathbf{v} \in \mathbb{Z}^m \mid \exists \mathbf{w} \in \mathbb{Z}^{n+1} : \mathbf{v} = \mathbf{A}'\mathbf{w} \mod q\},$$

[7] For more details on (the hardness of) LWE, Ring-LWE, and binary LWE we refer to [2, 7, 11, 26, 27, 29].

[8] Note that with our approach we only need that error vector $\mathbf{e}'$ is binary, and not also that the secret vector $\mathbf{s}$ is binary, as demanded in [10, 11].

where $\mathbf{A}' = (\mathbf{A} \mid \mathbf{b}) \in \mathbb{Z}_q^{m \times (n+1)}$. Note that constructing the lattice this way we only need the error vector $\mathbf{e}'$ to be binary and not also the secret $\mathbf{s}$ as in [10,11]. The dimension of the lattice Λ is equal to m and with high probability its determinant is $q^{m-(n+1)}$, see for example [7].

Determining the Attack Parameters

Let $\mathbf{v} = \mathbf{e} = (\mathbf{v}_l, \mathbf{v}_g)^t$ with $\mathbf{v}_l \in \{\pm 1/2\}^{m-r}$ and $\mathbf{v}_g \in \{\pm 1/2\}^r$. Then obviously we have $\|\mathbf{v}\|_\infty \leq 1/2$, so we set the infinity norm bounds $y = k = 1/2$. Since $\mathbf{v}_l$ is a uniformly random vector in $\{\pm 1/2\}^{m-r}$, the expected Euclidean norm of $\mathbf{v}_l$ is

$$\|\mathbf{v}_l\| \approx \sqrt{\frac{m-r}{4}}.$$

We set $2c_{-1/2} = 2c_{1/2} = \frac{r}{2}$ to be the expected number of $-1/2$ and $1/2$ entries of $\mathbf{v}_g$. In the following we assume that $c_{-1/2} = c_{1/2}$ is an integer in order to not have to deal with rounding operators.

Determining the Success Probability

We can approximate the success probability p_{succ} by $p_{\mathsf{succ}} \approx p_c \cdot p_{\mathrm{NP}}$, where p_c is the probability that $\mathbf{v}_g$ hat exactly $2c_{-1/2}$ entries equal to $-1/2$ and $2c_{1/2}$ entries equal to $1/2$ and p_{NP} is defined as in Section 4.2. Using the fact that $2c_{-1/2} + 2c_{1/2} = r$, we therefore obtain

$$p_{\mathsf{succ}} \approx p_c \cdot p_{\mathrm{NP}} = 2^{-r} \binom{r}{2c_{1/2}} p_{\mathrm{NP}}.$$

We assume that if the attack is successful then $|S| = 2$, where S is defined as in the Main Result, since $\mathbf{e}$ and $-\mathbf{e}$ are assumed to be the only vectors that can be found by the attack.

Optimizing the Runtime

Parameter set	**Set-I**	**Set-II**	**Set-III**
Optimal $r_{\mathsf{under}}/r_{\mathsf{over}}$	104/116	88/96	276/268
Optimal $\delta_{\mathsf{r,under}}$	1.00691	1.00731	1.00478
Optimal $\delta_{\mathsf{r,over}}$	1.00698	1.00741	1.00487
Corresponding $p_{\mathsf{under}}/p_{\mathsf{over}}$	$2^{-33}/2^{-27}$	$2^{-31}/2^{-28}$	$2^{-38}/2^{-43}$
Security under/over in bits	**88/99**	**79/90**	**187/197**
In [10]	94	84	190

Table 4. Optimal attack parameters and security levels against the Hybrid Attack for R-BinLWEEnc.

We reevaluated the security of the R-BinLWEEnc parameter sets proposed in [10]. Our security estimates, the optimal attack parameters r and δ_r, and the corresponding probability p are presented in Table 4. The original security estimates given in [10] are within the security range we determined. Nevertheless, we want to stress that even though we obtained similar security estimates, our reevaluation was necessary and valuable since the original estimates were fraught with doubt.

5.4 BLISS

The signature scheme BLISS, introduced in [16], is one of the most important lattice-based signature schemes. In the original paper, the authors considered the Hybrid Attack on their signature scheme for their security estimates, but the analysis is rather vague. For instance, as frequently done, the authors assume that collisions will always be detected, neglecting the fact that this is only the case with a very small probability. In addition, the authors demand a basis reduction of a certain quality for the attack. Furthermore, the authors do not optimize the attack parameters, which ignores the fact that a non-trivial trade-off between basis reduction and the Hybrid Attack is necessary for accurate runtime estimates. The estimates given in [16] are therefore not reliable, and we provide a detailed security analysis of the proposed parameter sets in order to update the security estimates.

Constructing the Lattice

In the BLISS signature scheme the setup is the following. Let n be a power of two, $d_1, d_2 \in \mathbb{N}$ such that $d_1 + d_2 \leq n$ holds, q a prime modulus with $q \equiv 1 \mod 2n$, and $\mathcal{R}_q = \mathbb{Z}_q[x]/(x^n + 1)$. The signing key is of the form $(s_1, s_2) = (f, 2g + 1)$, where $f \in \mathcal{R}_q^\times, g \in \mathcal{R}_q$, each with d_1 coefficients in $\{\pm 1\}$ and d_2 coefficients in $\{\pm 2\}$, and the remaining coefficients equal to 0. The public key is essentially $a = s_2/s_1 \in \mathcal{R}_q$. We assume that a is invertible in $\mathcal{R}_q$, which is the case with very high probability. Hence we obtain the equation $s_1 = s_2 a^{-1} \in \mathcal{R}_q$, or equivalently $f = 2ga^{-1} + a^{-1} \mod q$. In the following we identify polynomials with their coefficient vectors.

In Order to recover the signing key, it is sufficient to find the vector $\mathbf{v} = (\mathbf{f}, \mathbf{g})^t$. Similar to our previous analysis of NTRU in Section 5.1 we have that

$$\mathbf{v} + \begin{pmatrix} -\mathbf{a}^{-1} \\ \mathbf{0} \end{pmatrix} = \begin{pmatrix} 2\mathbf{g}\mathbf{a}^{-1} + q\mathbf{w} \\ \mathbf{g} \end{pmatrix} = \left(\begin{array}{c|c} q\mathbf{I}_n & 2\mathbf{A} \\ \hline \mathbf{0} & \mathbf{I}_n \end{array}\right) \begin{pmatrix} \mathbf{w} \\ \mathbf{g} \end{pmatrix}$$

for some $\mathbf{w} \in \mathbb{Z}^n$, where $\mathbf{A}$ is the rotation matrix of $\mathbf{a}^{-1}$. Hence $\mathbf{v}$ can be recovered by solving BDD on input $(\mathbf{a}^{-1}, \mathbf{0})^t$ in the q-ary lattice

$$\Lambda = \Lambda\left(\left(\begin{array}{c|c} q\mathbf{I}_n & 2\mathbf{A} \\ \hline \mathbf{0} & \mathbf{I}_n \end{array}\right)\right),$$

since $(\mathbf{a}^{-1}, \mathbf{0})^t - \mathbf{v} \in \Lambda$. The determinant of the lattice Λ is q^n and its dimension is equal to $2n$.

Determining the Attack Parameters

In the following let $\mathbf{v} = (\mathbf{f}, \mathbf{g})^t = (\mathbf{v}_l, \mathbf{v}_g)^t$ with $\mathbf{v}_l \in \mathbb{Z}^{m-r}$ and $\mathbf{v}_g \in \mathbb{Z}^r$. Since we are using the Hybrid Attack to solve a BDD problem, the rotations of $\mathbf{v}$ can not be utilized in the attack (or at least is is not known how), see Section 3. We therefore assume that $\mathbf{v}$ is the only rotation useful in the attack, i.e. that the set the set of good rotations S contains at most $\mathbf{v}$. The first step is to determine proper bounds y on $\|\mathbf{v}_l\|_\infty$ and k on $\|\mathbf{v}_g\|_\infty$ and find suitable guessing parameters c_i. By construction we obviously have $\|\mathbf{v}\|_\infty \leq 2$, thus we can set the infinity norm bounds $y = k = 2$. The expected Euclidean norm of $\mathbf{v}_l$ is given by

$$\|\mathbf{v}_l\| \approx \sqrt{d_1 + 4d_2 + \frac{n-r}{n}(1d_1 + 4d_2)}.$$

We set $2c_i$ equal to the expected number of i-entries in $\mathbf{v}_g$, i.e., $c_{-2} = c_2 = \frac{r}{n} \cdot \frac{1}{4} d_2$ and $c_{-1} = c_1 = \frac{r}{n} \cdot \frac{1}{4} d_1$. For simplicity we assume that c_1 and c_2 are integers in the following.

Determining the Success Probability

Next, we determine the success probability p_{succ}, which is the probability that $\mathrm{NP}_{\mathbf{B}}(\mathbf{C}\mathbf{v}_g) = \mathbf{v}_l$ and exactly $2c_i$ entries of $\mathbf{v}_g$ are equal to i for $i \in \{\pm 1, \ldots, \pm k\}$. The probability p_c that exactly $2c_i$ entries of the vector $\mathbf{v}_g$ are equal to i for all $i \in \{\pm 1, \ldots, \pm k\}$ is given by

$$\frac{\binom{r}{2\tilde{c_0}, 2c_{-2}, 2c_2, 2c_{-4}, 2c_4} \binom{n-r}{d_0 - 2\tilde{c_0}, d_1 - 4c_2, d_2 - 4c_4} 2^{d_1 + d_2 - 4(c_2 + c_4)}}{\binom{n}{d_0, d_1, d_2} 2^{d_1 + d_2}},$$

where $d_0 = n - d_1 - d_2$ and $2\tilde{c_0} = r - 2(c_{-2} + c_2 + c_{-4} + c_4)$ and p_{NP} is defined as in Section 4.2. The success probability is approximately given by

$$p_{\mathsf{succ}} \approx p_c \cdot p_{\mathrm{NP}}.$$

As explained earlier, we assume that $S \subset \{\mathbf{v}\}$, so if Algorithm 1 is successful we have $|S| = 1$.

Optimizing the Runtime

We performed the optimization process for the BLISS parameter sets proposed in [16]. The results are presented in Table 5. Besides the security levels against the Hybrid Attack, we provide the optimal attack parameters r and δ_r leading to a minimal runtime of the attack as well as the probability p. Our results show that the security estimates for the BLISS-I, BLISS-II, and BLISS-III parameter sets given in [16] are within the range of security we determined, whereas the BLISS-IV parameter set is less secure than originally claimed. In addition, the authors of [16] claim that there are at least 17 bits of security margins built into their security estimates, which is incorrect for all parameter sets according to our analysis.

Parameter set	**BLISS-I**	**BLISS-II**	**BLISS-III**	**BLISS-IV**
Optimal $r_{\mathsf{under}}/r_{\mathsf{over}}$	152/152	152/152	109/144	99/137
Optimal $\delta_{\mathsf{r,under}}$	1.00588	1.00588	1.00532	1.00518
Optimal $\delta_{\mathsf{r,over}}$	1.00600	1.00600	1.00541	1.00524
Corresponding $p_{\mathsf{under}}/p_{\mathsf{over}}$	$2^{-35}/2^{-38}$	$2^{-35}/2^{-38}$	$2^{-58}/2^{-40}$	$2^{-67}/2^{-44}$
Security under/over in bits	**124/139**	**124/139**	**152/170**	**160/182**
In [16]	128	128	160	192
r used in [16]	194	194	183	201

Table 5. Optimal attack parameters and security levels against the Hybrid Attack for BLISS.

5.5 GLP

The GLP signature scheme was introduced in [17]. In the original work the authors did not consider the Hybrid Attack when deriving their security estimates. Later, in [16], the Hybrid Attack was also applied to the GLP-I parameter set. However, the analysis in [16] of the Hybrid Attack against GLP is flawed in the same way as the analysis of the BLISS signature scheme, see Section 5.4. Furthermore, the GLP-II parameter set has not been analyzed regarding the Hybrid Attack so far. We therefore reevaluate the security of the GLP-I parameter set against the Hybrid Attack and firstly evaluate the Hybrid Attack security of the GLP-II parameter set.

Constructing the Lattice

For the GLP signature scheme the setup is the following. Let n be a power of two, q a prime modulus with $q \equiv 1 \mod 2n$, and $\mathcal{R}_q = \mathbb{Z}_q[x]/(x^n + 1)$. The signing key is of the form (s_1, s_2), where s_1 and s_1 are sampled uniformly at random among all polynomials of $\mathcal{R}_q$ with coefficients in $\{-1, 0, 1\}$. The corresponding public key is then of the form $(a, b = as_1 + s_2) \in \mathcal{R}_q^2$, where a is drawn uniformly at random in $\mathcal{R}_q$. So we know that $0 = -b + as_1 + s_2$. Identifying polynomials with their coefficient vectors we therefore have that

$$\mathbf{v} := \begin{pmatrix} -1 \\ \mathbf{s}_1 \\ \mathbf{s}_2 \end{pmatrix} \in \Lambda := \Lambda_q^{\perp}(\mathbf{A}) = \{\mathbf{w} \in \mathbb{Z}^{2n+1} \mid \mathbf{A}\mathbf{w} \equiv \mathbf{0} \mod q\} \subset \mathbb{Z}^{2n+1},$$

where $\mathbf{A} = (\mathbf{b}|\mathsf{rot}(\mathbf{a})|\mathbf{I}_n)$ and $\mathsf{rot}(\mathbf{a})$ is the rotation matrix of $\mathbf{a}$. Because of how the lattice is constructed we do not assume that rotations of $\mathbf{v}$ can by utilized by the attack.[9] Therefore, with very high probability $\mathbf{v}$ and $-\mathbf{v}$ are the only non-zero trinary vectors contained in Λ, which we assume in the following. Since

[9] It is possible to construct a lattice which contains all the rotations as short vectors, but this unnecessarily blows up the lattice dimension.

q is prime and $\mathbf{A}$ has full rank, we have that $\det \Lambda = q^n$, see for example [8]. In Appendix A.1 we show how to construct a basis of the form

$$\mathbf{B}' = \left(\begin{array}{c|c} q\mathbf{I}_n & \star \\ \hline \mathbf{0} & \mathbf{I}_{n+1} \end{array}\right) \in \mathbb{Z}^{(2n+1)\times(2n+1)}$$

for the q-ary lattice Λ.

Determining the Attack Parameters

Ignoring the first -1 coordinate, the short vector $\mathbf{v}$ is drawn uniformly from $\{-1, 0, 1\}^{2n+1}$. Let $\mathbf{v} = (\mathbf{v}_l, \mathbf{v}_g)^t$ with $\mathbf{v}_l \in \mathbb{Z}^{m-r}$ and $\mathbf{v}_g \in \mathbb{Z}^r$. Then obviously $\|\mathbf{v}_l\|_\infty \leq 1$ and $\|\mathbf{v}_g\|_\infty \leq 1$ hold, so we can set the infinity norm bounds y and k equal to one. The expected Euclidean norm of $\mathbf{v}_l$ is approximately

$$\|\mathbf{v}_l\| \approx \sqrt{2(m-r)/3}.$$

We set $2c_{-1} = 2c_1 = \frac{r}{3}$ to be the expected number of ones and minus ones. For simplicity we assume that $c_{-1} = c_1$ is an integer in the following.

Determining the Success Probability

The success probability p_{succ} of the attack is approximately $p_{\mathsf{succ}} \approx p_c \cdot p_{\mathrm{NP}}$, where p_c is the probability that $\mathbf{v}_g$ hat exactly $2c_{-1}$ minus one entries and $2c_1$ one entries and p_{NP} is defined as in Section 4.2. Calculating p_c yields

$$p_{\mathsf{succ}} \approx p_c \cdot p_{\mathrm{NP}} = 3^{-r} \binom{r}{r/3, r/3, r/3} p_{\mathrm{NP}}.$$

As previously mentioned, we assume that if the attack is successful then $|S| = 2$.

Optimizing the Runtime

We performed the optimization for the GLP parameter sets proposed in [17]. The results, including the optimal attack parameters r and δ_r and the probability p, are shown in Table 6. The security level of the GLP-I parameter set claimed in [16] is within the range of security we determined. In [16], the authors did not analyze the Hybrid Attack for the GLP-II parameter set. Güneysu et al. [17] claimed a security level of at least 256 bits (not considering the Hybrid Attack) for the GLP-II parameter set, whereas we show that it offers at most 233 bits of security against the Hybrid Attack.

6 Conclusion and Future Work

In this work we described a general version of the Hybrid Attack and presented improved and detailed techniques to accurately analyze the runtime of the Hybrid Attack. For the first time, this enables researchers to correctly analyze the

Parameter set	**GLP-I**	**GLP-II**
Optimal $r_{\mathsf{under}}/r_{\mathsf{over}}$	30/54	168/192
Optimal $\delta_{\mathsf{r,under}}$ Optimal $\delta_{\mathsf{r,over}}$	1.00776 1.00769	1.00450 1.00451
Corresponding $p_{\mathsf{under}}/p_{\mathsf{over}}$	$2^{-41}/2^{-25}$	$2^{-61}/2^{-49}$
Security under/over in bits	**71/88**	**212/233**
In [16], [17]	75 to 80	≥ 256
r used in [16]	85	—

Table 6. Optimal attack parameters and security levels against the Hybrid Attack for GLP.

security of their cryptographic schemes against the Hybrid Attack such that the resulting security estimates can be relied upon. We strongly encourage researchers to use our new improved methods for future security estimates instead of the inaccurate approaches used previously. In the final part of this work we reevaluated various cryptographic schemes regarding their security against the Hybrid Attack. Our analysis shows that several the old security estimates of previous works were in fact unreliable. By updating these unreliable estimates we contributed to the trustworthiness of security estimates of lattice based cryptography.

For future work, we hope that more provable statements about the practicality of the Hybrid Attack can be derived. For instance, our results show that the Hybrid Attack is not the best known attack on all NTRU instances as previously thought. It would be interesting to prove that under certain conditions on the key structure the Hybrid Attack is always outperformed by some other attack. Another possible line of future work is applying the Hybrid Attack to a broader range of cryptographic schemes than already done in this work.

Acknowledgements. This work has been co-funded by the DFG as part of project P1 within the CRC 1119 CROSSING. We thank Florian Gpfert and John Schanck for helpful discussions and comments.

References

1. M. R. Albrecht, R. Fitzpatrick, and F. Göpfert. On the efficacy of solving LWE by reduction to unique-svp. In H. Lee and D. Han, editors, *Information Security and Cryptology - ICISC 2013 - 16th International Conference, Seoul, Korea, November 27-29, 2013, Revised Selected Papers*, volume 8565 of *Lecture Notes in Computer Science*, pages 293–310. Springer, 2013.
2. M. R. Albrecht, R. Player, and S. Scott. On the concrete hardness of learning with errors. *J. Mathematical Cryptology*, 9(3):169–203, 2015.
3. E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe. Post-quantum key exchange - a new hope. *IACR Cryptology ePrint Archive*, 2015:1092, 2015.

4. Y. Aono, Y. Wang, T. Hayashi, and T. Takagi. Improved progressive BKZ algorithms and their precise cost estimation by sharp simulator. In M. Fischlin and J. Coron, editors, *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part I*, volume 9665 of *Lecture Notes in Computer Science*, pages 789–819. Springer, 2016.
5. L. Babai. On Lovász' lattice reduction and the nearest lattice point problem (shortened version). In K. Mehlhorn, editor, *STACS '86*, volume 82 of *Lecture Notes in Computer Science*, pages 13–20. Springer, 1985.
6. L. Babai. On Lovász' lattice reduction and the nearest lattice point problem. *Combinatorica*, 6(1):1–13, 1986.
7. S. Bai and S. D. Galbraith. Lattice decoding attacks on binary LWE. In W. Susilo and Y. Mu, editors, *Information Security and Privacy - 19th Australasian Conference, ACISP 2014, Wollongong, NSW, Australia, July 7-9, 2014. Proceedings*, volume 8544 of *Lecture Notes in Computer Science*, pages 322–337. Springer, 2014.
8. D. J. Bernstein, J. Buchmann, and E. Dahmen, editors. *Post-Quantum Cryptography*. Springer, 2009.
9. D. J. Bernstein, C. Chuengsatiansup, T. Lange, and C. van Vredendaal. NTRU prime. *IACR Cryptology ePrint Archive*, 2016:461, 2016.
10. J. A. Buchmann, F. Göpfert, T. Güneysu, T. Oder, and T. Pöppelmann. High-performance and lightweight lattice-based public-key encryption. In R. Chow and G. Saldamli, editors, *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security, CPSS@AsiaCCS, Xi'an, China, May 30 - June 3, 2016*, pages 2–9. ACM, 2016.
11. J. A. Buchmann, F. Göpfert, R. Player, and T. Wunderer. On the hardness of LWE with binary error: Revisiting the hybrid lattice-reduction and meet-in-the-middle attack. In D. Pointcheval, A. Nitaj, and T. Rachidi, editors, *Progress in Cryptology - AFRICACRYPT 2016 - 8th International Conference on Cryptology in Africa, Fes, Morocco, April 13-15, 2016, Proceedings*, volume 9646 of *Lecture Notes in Computer Science*, pages 24–43. Springer, 2016.
12. R. Canetti and J. A. Garay, editors. *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I*, volume 8042 of *Lecture Notes in Computer Science*. Springer, 2013.
13. Y. Chen. *Réduction de réseau et sécurité concrete du chiffrement completement homomorphe*. PhD thesis, ENS-Lyon, France, 2013.
14. Y. Chen and P. Q. Nguyen. BKZ 2.0: Better lattice security estimates. In D. H. Lee and X. Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, volume 7073 of *Lecture Notes in Computer Science*, pages 1–20. Springer, 2011.
15. J. H. Cheon, D. Kim, J. Lee, and Y. S. Song. Lizard: Cut off the tail! // practical post-quantum public-key encryption from LWE and LWR. *IACR Cryptology ePrint Archive*, 2016:1126, 2016.
16. L. Ducas, A. Durmus, T. Lepoint, and V. Lyubashevsky. Lattice signatures and bimodal gaussians. In Canetti and Garay [12], pages 40–56.
17. T. Güneysu, V. Lyubashevsky, and T. Pöppelmann. Practical lattice-based cryptography: A signature scheme for embedded systems. In E. Prouff and P. Schaumont, editors, *Cryptographic Hardware and Embedded Systems - CHES 2012 - 14th International Workshop, Leuven, Belgium, September 9-12, 2012. Proceedings*, volume 7428 of *Lecture Notes in Computer Science*, pages 530–547. Springer, 2012.

18. P. S. Hirschhorn, J. Hoffstein, N. Howgrave-Graham, and W. Whyte. Choosing ntruencrypt parameters in light of combined lattice reduction and MITM approaches. In M. Abdalla, D. Pointcheval, P. Fouque, and D. Vergnaud, editors, *Applied Cryptography and Network Security, 7th International Conference, ACNS 2009, Paris-Rocquencourt, France, June 2-5, 2009. Proceedings*, volume 5536 of *Lecture Notes in Computer Science*, pages 437–455, 2009.
19. J. Hoffstein, N. Howgrave-Graham, J. Pipher, J. H. Silverman, and W. Whyte. Hybrid lattice reduction and meet in the middle resistant parameter selection for ntru-encrypt. *Submission/contribution to ieee p1363*, 1:2007–02, 2007.
20. J. Hoffstein, J. Pipher, J. M. Schanck, J. H. Silverman, W. Whyte, and Z. Zhang. Choosing parameters for ntruencrypt. *IACR Cryptology ePrint Archive*, 2015:708, 2015.
21. J. Hoffstein, J. Pipher, and J. H. Silverman. NTRU: A ring-based public key cryptosystem. In J. Buhler, editor, *Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998, Proceedings*, volume 1423 of *Lecture Notes in Computer Science*, pages 267–288. Springer, 1998.
22. N. Howgrave-Graham. A hybrid lattice-reduction and meet-in-the-middle attack against NTRU. In A. Menezes, editor, *Advances in Cryptology - CRYPTO 2007, 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007, Proceedings*, volume 4622 of *Lecture Notes in Computer Science*, pages 150–169. Springer, 2007.
23. N. Howgrave-Graham, J. H. Silverman, and W. Whyte. A meet-in-the-middle attack on an NTRU private key. `https://www.securityinnovation.com/uploads/Crypto/NTRUTech004v2.pdf`.
24. A. K. Lenstra and E. R. Verheul. Selecting cryptographic key sizes. *J. Cryptology*, 14(4):255–293, 2001.
25. R. Lindner and C. Peikert. Better key sizes (and attacks) for lwe-based encryption. In A. Kiayias, editor, *Topics in Cryptology - CT-RSA 2011 - The Cryptographers' Track at the RSA Conference 2011, San Francisco, CA, USA, February 14-18, 2011. Proceedings*, volume 6558 of *Lecture Notes in Computer Science*, pages 319–339. Springer, 2011.
26. V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. *J. ACM*, 60(6):43, 2013.
27. D. Micciancio and C. Peikert. Hardness of SIS and LWE with small parameters. In Canetti and Garay [12], pages 21–39.
28. F. W. Olver. *NIST handbook of mathematical functions*. Cambridge University Press, 2010.
29. O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In H. N. Gabow and R. Fagin, editors, *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*, pages 84–93. ACM, 2005.
30. J. Schanck. Practical lattice cryptosystems: Ntruencrypt and ntrumls. 2015.
31. C. van Vredendaal. Scarecryptow — personal website of christine van vredendaal. `http://scarecryptow.org/publications/ntruprime.html`, 2016. [Online; accessed 07-June-2016].

A Appendix

On q-ary Lattices

A.1 Constructing a Basis of the Required Form

In the following lemma we show that for q-ary lattices, where q is prime, there always exists a basis of the form required for the attack. The size of the identity in the bottom right corner of the basis depends on the determinant of the lattice. In the proof we also show how to construct such a basis.

Lemma 3. *Let q be prime, $m \in \mathbb{N}$, and $\Lambda \subset \mathbb{Z}^m$ a q-ary lattice.*

1. *There exists some $k \in \mathbb{Z}, 0 \leq n \leq m$ such that $\det(\Lambda) = q^k$.*
2. *Let $\det(\Lambda) = q^k$. Then there is a matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times (m-k)}$ of rank $m-k$ (over $\mathbb{Z}_q$) such that $\Lambda = \Lambda_q(\mathbf{A})$.*
3. *Let $\det(\Lambda) = q^k$ and $\mathbf{A} = \begin{pmatrix} \mathbf{A}_1 \\ \mathbf{A}_2 \end{pmatrix}$ with $\mathbf{A}_1 \in \mathbb{Z}_q^{k \times (m-k)}, \mathbf{A}_2 \in \mathbb{Z}_q^{(m-k) \times (m-k)}$ be a matrix of rank $m-k$ (over $\mathbb{Z}_q$) such that $\Lambda = \Lambda_q(\mathbf{A})$. If $\mathbf{A}_2$ is invertible over $\mathbb{Z}_q$, then the columns of the matrix*

$$\mathbf{B}' = \left(\begin{array}{c|c} q\mathbf{I}_k & \mathbf{A}_1\mathbf{A}_2^{-1} \\ \hline \mathbf{0} & \mathbf{I}_{m-k} \end{array} \right) \in \mathbb{Z}^{m \times m} \tag{1}$$

form a basis of the lattice Λ.

Proof. 1. Obviously $\det(\Lambda) \mid \det(q\mathbb{Z}^m) = q^m$, since $q\mathbb{Z}^m \subset \Lambda$, and therefore $\det(\Lambda)$ is some non-negative power of q, because q is prime.

2. We have $(\mathbb{Z}^m : q\mathbb{Z}^m) = (\mathbb{Z}^m : \Lambda) \cdot (\Lambda : q\mathbb{Z}^m)$ and therefore

$$(\Lambda : q\mathbb{Z}^m) = \frac{(\mathbb{Z}^m : q\mathbb{Z}^m)}{(\mathbb{Z}^m : \Lambda)} = \frac{\det(q\mathbb{Z}^m)}{\det(\Lambda)} = q^{m-k}.$$

   Let $\mathbf{A}' \in \mathbb{Z}_q^{m \times m}$ be some lattice basis of Λ. Since $\Lambda / q\mathbb{Z}^m$ is in one-to-one correspondence to the $\mathbb{Z}_q$–vector space spanned by $\mathbf{A}'$.This vector space has to be of dimension $m-k$ and therefore $\mathbf{A}'$ has rank $m-k$ over $\mathbb{Z}_q$. This implies that there is some matrix $\mathbf{A}$ consisting of $m-k$ columns of $\mathbf{A}'$ such that $\Lambda = \Lambda(q\mathbf{I}_m \mid \mathbf{A}) = \Lambda_q(\mathbf{A})$.

3. By assumption $\mathbf{A}_2$ is invertible and thus we have

$$\begin{aligned} \Lambda &= \left\{ \mathbf{v} \in \mathbb{Z}^m \mid \exists \mathbf{w} \in \mathbb{Z}^{(m-k)} : \mathbf{v} = \mathbf{A}\mathbf{w} \mod q \right\} \\ &= \left\{ \mathbf{v} \in \mathbb{Z}^m \mid \exists \mathbf{w} \in \mathbb{Z}^{(m-k)} : \mathbf{v} = \begin{pmatrix} \mathbf{A}_1 \\ \mathbf{A}_2 \end{pmatrix} \mathbf{A}_2^{-1}\mathbf{w} \mod q \right\} \\ &= \left\{ \begin{pmatrix} \mathbf{A}_1\mathbf{A}_2^{-1} \\ \mathbf{I}_{m-k} \end{pmatrix} \mathbf{w} \mid \mathbf{w} \in \mathbb{Z}^{(m-k)} \right\} + q\mathbb{Z}^m. \end{aligned}$$

   Therefore the columns of the matrix

$$\left(\begin{array}{c|c} q\mathbf{I}_m & \mathbf{A}_1\mathbf{A}_2^{-1} \\ & \mathbf{I}_{m-k} \end{array} \right) \in \mathbb{Z}^{m \times (m+(m-k))}$$

   form a generating set of the lattice Λ, which can be reduced to the basis $\mathbf{B}'$. □

A.2 Modifying the GSA for q-ary Lattices

Typically, the Gram-Schmidt lengths obtained after performing a basis reduction with quality δ can be approximated the Geometric Series Assumption (GSA), see the Preliminaries. However, for q-ary lattices, this assumption needs to be modified in order to accurately reflect the reality. This has already been considered and confirmed with experimental results in previous works, see for example [18, 20, 22, 30]. However, in this work we derive simple formulas predicting the quality of the reduction, and therefore explain how to obtain these formulas in more detail. We begin by sketching the reason why the unmodified GSA does not hold for q-ary lattices, given a lattice basis $\mathbf{B}$ of the form

$$\mathbf{B} = \left(\begin{array}{c|c} q\mathbf{I}_a & \star \\ \hline \mathbf{0} & \mathbf{I}_b \end{array}\right) \in \mathbb{Z}^{d\times d},$$

where $d = a + b$. How to construct such a basis for a q-ary lattice is shown in Appendix A.1. Then, if the basis reduction is not strong enough, i.e. the Hermite delta is too large, the GSA predicts that the first Gram-Schmidt vectors of the reduced basis have norm bigger than q. However, in practice this will not happen, since in this case the first vectors will simply not be reduced. This means, that instead of reducing the whole basis $\mathbf{B}$, one can just reduce the last vectors that will actually be reduced. Let k denote the (so far unknown) number of the last vectors that are actually reduced (i.e., their corresponding Gram-Schmidt vectors according to the GSA have norm smaller than q). We assume that the basis reduction is sufficiently weak that $k < d$ and sufficiently strong such that $k > b$. We write $\mathbf{B}$ in the form

$$\mathbf{B} = \left(\begin{array}{c|c} q\mathbf{I}_{d-k} & \mathbf{D} \\ \hline \mathbf{0} & \mathbf{B}_1 \end{array}\right)$$

for some $\mathbf{B}_1 \in \mathbb{Z}^{k\times k}$ and $\mathbf{D} \in \mathbb{Z}^{(d-k)\times k}$. Now instead of $\mathbf{B}$ we only reduce $\mathbf{B}_1$ to $\mathbf{B}_1' = \mathbf{B}_1\mathbf{U}$ for some unimodular $\mathbf{U} \in \mathbb{Z}^{k\times k}$. This yields a reduced basis

$$\mathbf{B}' = \left(\begin{array}{c|c} q\mathbf{I}_{d-k} & \mathbf{DU} \\ \hline \mathbf{0} & \mathbf{B}_1' \end{array}\right)$$

of $\mathbf{B}$. The Gram-Schmidt basis of this new basis $\mathbf{B}'$ is given by

$$\overline{\mathbf{B}'} = \left(\begin{array}{c|c} q\mathbf{I}_{d-k} & \mathbf{0} \\ \hline \mathbf{0} & \overline{\mathbf{B}_1'} \end{array}\right).$$

Therefore, the lengths of the Gram-Schmidt basis vectors $\overline{\mathbf{B}'}$ are q for the first $d-k$ vectors and then equal to the lengths of the Gram-Schmidt basis vectors $\overline{\mathbf{B}_1'}$, which are smaller than q. In order to predict the lengths of $\overline{\mathbf{B}'}$ we can apply the GSA to the lengths of the Gram-Schmidt basis vectors $\overline{\mathbf{B}_1'}$, since they are actually reduced. What remains is to determine k. Assume we apply a Basis reduction on $\mathbf{B}_1$ that results in a reduced basis $\mathbf{B}_1'$ of Hermite Delta δ. By our

construction we can assume that the first Gram-Schmidt basis vector of $\overline{\mathbf{B}'_1}$ has norm roughly equal to q, so the GSA implies

$$\delta^k \det(\Lambda(\mathbf{B}_1)^{\frac{1}{k}}) = q.$$

Using the fact that $\det(\Lambda(\mathbf{B}_1)) = q^{k-b}$ and $k < d$, we can solve for k and obtain

$$k = \min\left(\left\lfloor\sqrt{\frac{b}{\log_q(\delta)}}\right\rfloor, d\right). \tag{2}$$

Summarizing, we expect that after the basis reduction our Gram-Schmidt basis $\overline{\mathbf{B}'_1}$ has lengths $R_1, \ldots, R_d$, where

$$R_i = \begin{cases} q, & \text{if } i \leq d-k \\ \delta^{-2(i-(d-k)-1)+k} q^{\frac{k-b}{k}}, & \text{else} \end{cases} \tag{3}$$

and k is given as in Equation 2.

Note that it might also happen that the last Gram-Schmidt lengths are predicted to be smaller than 1. In this case these last vectors will also not be reduced in reality, since the basis matrix has the identity in the bottom right corner. Therefore, in this case the GSA has to be further modified. However, for realistic attack parameters this phenomenon never occurred during our runtime optimizations and therefore we do not include it in our formulas and leave it to the reader to do the easy calculations if needed.