On the Hardness of LWE with Binary Error: Revisiting the Hybrid Lattice-Reduction and Meet-in-the-Middle Attack

Johannes Buchmann[1(✉)], Florian Göpfert[1], Rachel Player[2], and Thomas Wunderer[1]

[1] Technische Universität Darmstadt, Darmstadt, Germany
{buchmann,fgoepfert,twunderer}@cdc.informatik.tu-darmstadt.de
[2] Information Security Group, Royal Holloway, University of London, Egham, UK
Rachel.Player.2013@live.rhul.ac.uk

Abstract. The security of many cryptographic schemes has been based on special instances of the Learning with Errors (LWE) problem, e.g., Ring-LWE, LWE with binary secret, or LWE with ternary error. However, recent results show that some subclasses are weaker than expected. In this work we show that *LWE with binary error*, introduced by Micciancio and Peikert, is one such subclass. We achieve this by applying the Howgrave-Graham attack on NTRU, which is a combination of lattice techniques and a Meet-in-the-Middle approach, to this setting. We show that the attack outperforms all other currently existing algorithms for several natural parameter sets. For instance, for the parameter set $n = 256$, $m = 512$, $q = 256$, this attack on LWE with binary error only requires 2^{85} operations, while the previously best attack requires 2^{117} operations. We additionally present a complete and improved analysis of the attack, using analytic techniques. Finally, based on the attack, we give concrete hardness estimations that can be used to select secure parameters for schemes based on LWE with binary error.

Keywords: Learning with errors · Lattice-based cryptography · Cryptanalysis · NTRU · Hybrid attack

1 Introduction

The Learning with Errors problem (LWE) is one of the most important problems in lattice-based cryptography. A huge variety of schemes, ranging from basic primitives like signature [18] and encryption schemes [32] to highly advanced schemes like group signatures [30] and fully homomorphic encryption [12], base their security on the LWE assumption. Understanding the concrete hardness of LWE is therefore important for selecting parameters.

Many cryptographic schemes are based on the hardness of special LWE instances like Ring-LWE [34], or LWE with ternary error [22]. Understanding the hardness of subclasses of the LWE problem and identifying those that are easy to

D. Pointcheval et al. (Eds.): AFRICACRYPT 2016, LNCS 9646, pp. 24–43, 2016.
DOI: 10.1007/978-3-319-31517-1_2

solve is therefore an important task. In fact, several recent results [15,19,20,29] show that some subclasses are easier than expected.

We show that the subclass LWE with binary error, which has been considered before in several papers [1,35], fits into this category. To show that LWE with binary error is considerably easier than expected, we modify the hybrid lattice-reduction and meet-in-the-middle attack by Howgrave-Graham [25] (refered to as hybrid attack in the following), apply it to this setting, and analyze its complexity. In order to compare our approach to existing ones, we apply known attacks on LWE to the binary error setting and analyze their complexities in this case. Our comparison shows that the hybrid attack is much faster than existing methods such as the enumeration attack [32,33], or the embedding approach [4] for several natural parameter sets. Figure 1 illustrates our improvement, by comparing the runtime of the best previously known attack with the hybrid attack, where $m = 2n$ samples from an LWE distribution with binary error are given and n is the dimension of the secret vector. For example, in the case of $n = 256$ and $q = 256$, the hardness of the problem drops from 117 to 85 bits, which is a significant improvement. A detailed comparison between the hybrid attack and previous approaches is given in Table 1 in Sect. 4.

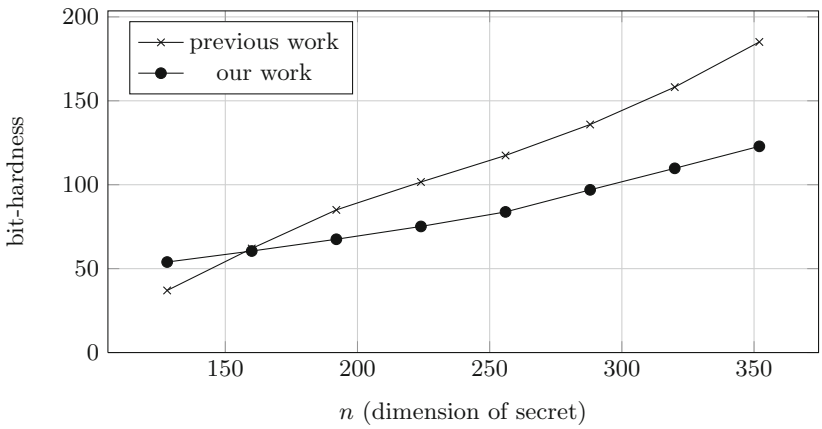

Fig. 1. Hardness of LWE instances with number of samples $m = 2n$ and modulus $q = 256$ before and after this work

The hybrid attack can also be seen as an improvement of an idea sketched by Bai and Galbraith [9]. However, Bai and Galbraith did not provide an analysis of their suggestion, and the analysis of Howgrave-Graham is partly based on experiments. A theoretical analysis of the hybrid attack that is not based on experimental results has been presented by Hirschhorn et al. in [24]. However, their analysis requires an additional assumption.

In this work we present a complete and improved analysis based on the same assumptions used in [25] without the additional assumption of [24], that does not

require experimental support. For this reason, we introduce new analytic techniques. Our new analysis can also be applied to the Howgrave-Graham attack, as well as to the attack mentioned by Bai and Galbraith (see [9]). In addition, we show how to use our techniques to analyze the decoding attack on LWE with binary error.

Related Work. A number of recent works have highlighted the importance of considering the hardness of variants of LWE. For example, certain choices of rings lead to weak instances of the Ring-LWE problem [15,19,20]. Additionally, Laine and Lauter [29] provide a polynomial time attack for LWE instances with an exponentially large modulus q and a sufficiently narrow Gaussian error. The existence of such weak instances shows the necessity of studying the hardness of special instances of the LWE problem separately.

The hardness of LWE with binary error has been considered in some detail. So far, there are known attacks that require access to superlinearly many samples (i.e., $m > \mathcal{O}(n)$), and hardness results when the crypanalyst is given a sublinear number of additional samples (i.e., $m = n + \mathcal{O}(n/\log(n))$), where n is the dimension of the secret vector. More precisely, the problem can be solved in polynomial time using the algorithm of Arora and Ge [6], when the number of samples is $m = \mathcal{O}(n^2)$ (see, e.g., [1]). Furthermore, Albrecht et al. [1] showed that LWE with binary error can be solved in subexponential time using an improved version of the Arora-Ge attack, if the attacker has access to a quasi-linear number of samples, e.g., $m = \mathcal{O}(n \log\log n)$. On the other hand, Micciancio and Peikert [35] proved that LWE with binary error reduces to worst-case lattice problems when the number of samples is restricted to $n + \mathcal{O}(n/\log(n))$. We close the margin between these hardness results on the one side and the weakness results on the other side by presenting an attack that runs with only n additional samples.

The idea of Bai and Galbraith which we build upon is to guess the first r components of the secret vector and apply a lattice attack on the remaining problem [9]. As noted in [5], this strategy enables the transformation of any algorithm for solving LWE into another one whose complexity is bounded by the cost of exhaustive search. Howgrave-Graham's algorithm [25], which we apply here, involves a Meet-in-the-Middle component to speed up this guessing: this was not considered in either of [5,9]. The existence of a Meet-in-the-Middle approach for solving LWE (without combining with any another algorithm) was mentioned in [9] and such an algorithm was presented in [5]. In Sect. 4 we show that it is much more efficient to combine a Meet-in-the-Middle approach with a decoding attack than to solve LWE with binary error entirely by a Meet-in-the-Middle approach.

Structure. In Sect. 2 we give some notation and required preliminaries. In Sect. 3 we describe how to apply the hybrid attack to LWE with binary error and analyze its complexity. In Sect. 4 we apply other possible attacks on LWE to the binary error case, analyze their complexities, and compare the results to the hybrid attack.

2 Notation and Preliminaries

Notation. In this work vectors are denoted in bold lowercase letters, e.g., $\mathbf{a}$, and matrices in bold uppercase letters, e.g., $\mathbf{A}$. For a vector $\mathbf{v} \in \mathbb{R}^n$ we write $\mathbf{v} \mod q$ for its unique representative modulo q in $[-\lfloor \frac{q}{2} \rfloor, \frac{q}{2})^n$. Logarithms are base two unless stated otherwise, and $\ln(x)$ denotes the natural logarithm of x.

Learning with Errors. The Learning with Errors (LWE) problem, introduced by Regev [41], is a computational problem, whose presumed hardness is the basis for several cryptographic constructions, e.g., [39–41]. In this work, we consider the variant *LWE with binary error*.

Problem Statement 1 (LWE with binary error). *Let n, q be positive integers, $\mathcal{U}$ be the uniform distribution on $\{0,1\}$ and $\mathbf{s} \xleftarrow{\$} \mathcal{U}^n$ be a secret vector in $\{0,1\}^n$. We denote by $L_{\mathbf{s},\mathcal{U}}$ the probability distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$ obtained by choosing $\mathbf{a} \in \mathbb{Z}_q^n$ uniformly at random, choosing $e \xleftarrow{\$} \mathcal{U}$ and returning $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$.*
LWE with binary error is the problem of recovering $\mathbf{s}$ from m samples $(\mathbf{a}_i, \langle \mathbf{a}_i, \mathbf{s}_i \rangle + e_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ sampled according to $L_{\mathbf{s},\mathcal{U}}$, with $i \in \{1, \ldots, m\}$.

Note that Regev defined LWE with a secret vector $\mathbf{s}$ chosen uniformly at random from the whole of $\mathbb{Z}_q^n$. However, it is well-known that LWE with arbitrarily distributed secret can be transformed to LWE with secret distributed according to the error distribution. Consequently, most cryptographic constructions are based on LWE where secret and error are identically distributed, and we focus on this case in this work.

Lattices and Bases. A lattice is a discrete additive subgroup of $\mathbb{R}^m$. A set of linearly independent vectors $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subset \mathbb{R}^m$ is called a basis of a lattice Λ, if $\Lambda = \Lambda(\mathbf{B})$, where

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

The dimension of a lattice Λ is defined as the cardinality of some (equivalently any) basis of Λ. For the rest of this work we restrict our studies to lattices in $\mathbb{R}^m$ whose dimension is maximal, e.g., m, which are called full-ranked lattices. The fundamental parallelepiped of a lattice basis $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_m\} \subset \mathbb{R}^m$ is given by

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

The determinant of a lattice $\Lambda(\mathbf{B})$ for a basis $\mathbf{B}$ is defined as the m dimensional volume of its fundamental parallelepiped. Note that the determinant of the lattice is independent of the choice of the basis.

Every lattice of dimension $m \geq 2$ has infinitely many different bases. A measure for the quality of a basis is provided by the Hermite delta. A lattice basis $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_m\}$ has Hermite delta δ if $\|\mathbf{b}_1\| = \delta^m \det(\Lambda)^{1/m}$.

Differing estimates exist in the literature for the number of operations of a basis reduction necessary to achieve a certain Hermite delta δ (see for example [5,16,32,33,37]). Throughout this work we will use the estimate given by Lindner and Peikert [32]. This is that the number of operations needed to achieve a certain Hermite delta δ is around

$$\mathrm{ops}_{\mathrm{BKZ}}(\delta) = 2^{1.8/\log_2(\delta)-110} \cdot 2.3 \cdot 10^9. \tag{1}$$

A lattice Λ satisfying $q \cdot \mathbb{Z}^m \subset \Lambda \subset \mathbb{R}^m$ is a q-ary lattice. For a matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$, we define the q-ary lattice

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

If $m \geq n$ and all column vectors $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ are linearly independent over $\mathbb{Z}_q$, we have $\det(\Lambda_q(\mathbf{A})) = q^{m-n}$.

The closest vector problem is the problem of recovering the lattice vector closest to a given target vector, given also a basis of the lattice. One can consider a relaxation, namely a close vector problem, where the inputs are the same (a basis and a target vector), and the task is to recover a lattice vector which is sufficiently close to the target.

Babai's Nearest Plane. The hybrid attack uses Babai's nearest plane algorithm [7] (denoted by NP in the following) as subroutine. It gets a lattice basis $\mathbf{B} \subset \mathbb{Z}^m$ and a target vector $\mathbf{t} \in \mathbb{R}^m$ as input and outputs a vector $\mathbf{e} \in \mathbb{R}^m$ such that $\mathbf{t} - \mathbf{e} \in \Lambda(\mathbf{B})$, which we denote by $\mathrm{NP}_{\mathbf{B}}(\mathbf{t}) = \mathbf{e}$. If the used lattice basis is clear from the context, we omit it in the notation and simply write $\mathrm{NP}(\mathbf{t})$. A detailed explanation of nearest plane can be found in Babai's original work [7] and Lindner and Peikert's follow up work [32]. The output of nearest plane plays an important role in the analysis of the hybrid attack and can be understood without knowing details about the algorithm itself. It depends on the Gram-Schmidt basis of the input basis $\mathbf{B}$, which is defined as $\overline{\mathbf{B}} = \{\overline{\mathbf{b}_1}, \ldots, \overline{\mathbf{b}_n}\}$ with

$$\overline{\mathbf{b}_i} = \mathbf{b}_i - \sum_{j=1}^{i-1} \frac{\langle \overline{\mathbf{b}_j}, \mathbf{b}_i \rangle}{\langle \overline{\mathbf{b}_j}, \overline{\mathbf{b}_j} \rangle} \overline{\mathbf{b}_j},$$

where $\overline{\mathbf{b}_1} = \mathbf{b}_1$. We will use the following result from [8].

Lemma 1. *For a lattice basis* $\mathbf{B}$ *with Gram-Schmidt basis* $\overline{\mathbf{B}}$ *and a target vector* $\mathbf{t}$ *as input, the nearest plane algorithm returns the unique vector* $\mathbf{e} \in \mathcal{P}(\overline{\mathbf{B}})$ *that satisfies* $\mathbf{t} - \mathbf{e} \in \Lambda(\mathbf{B})$.

Lemma 1 shows that analyzing the output of the nearest plane algorithm requires to estimate the lengths of the basis vectors of the corresponding Gram-Schmidt basis. The established way to do this is via the the following heuristic (see Lindner and Peikert [32] for more details).

Heuristic 1 (Geometric Series Assumption). *Let* $\{\mathbf{b}_1 \dots \mathbf{b}_m\} \subset \mathbb{Z}^m$ *be a reduced basis with Hermite delta* δ *of an* m*-dimensional lattice with determinant* D*. Also let* $\overline{\mathbf{b}_i}$ *denote the basis vectors of the corresponding Gram-Schmidt basis. Then the length of* $\overline{\mathbf{b}_i}$ *is approximated by*

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

3 The Attack

In this section we present and analyze the hybrid attack on LWE with binary error. The attack is described in Algorithm 1 of Sect. 3.1. In Theorem 1 of Sect. 3.2 we analyze the expected runtime of the hybrid attack. Section 3.3 shows how to optimize the attack parameters and perform a trade-off between precomputation and the actual attack in order to minimize the runtime of the attack.

3.1 The Hybrid Attack

In the following we describe the hybrid attack on LWE with binary error. The attack is presented in Algorithm 1.

Let $m, n, q \in \mathbb{N}$ and let

$$(\mathbf{A}, \mathbf{b} = \mathbf{A}\tilde{\mathbf{s}} + \mathbf{e} \mod q) \tag{2}$$

with $\mathbf{A} \in \mathbb{Z}_q^{m \times n}, \mathbf{b} \in \mathbb{Z}_q^m, \tilde{\mathbf{s}} \in \{0,1\}^n$ and $\mathbf{e} \in \{0,1\}^m$ be an LWE instance with binary error $\mathbf{e}$ and binary secret $\tilde{\mathbf{s}}$. In order to obtain a smaller error vector we can subtract the vector $(1/2) \cdot \mathbf{1}$ consisting of all $1/2$ entries from Eq. (2). This yields a new LWE instance $(\mathbf{A}, \mathbf{b}' = \mathbf{A}\tilde{\mathbf{s}} + \mathbf{e}' \mod q)$, where $\mathbf{b}' = \mathbf{b} - (1/2) \cdot \mathbf{1}$ and $\mathbf{e}' = \mathbf{e} - (1/2) \cdot \mathbf{1}$. The new error vector $\mathbf{e}'$ now has norm $\sqrt{m/4}$ instead of the expected norm $\sqrt{m/2}$ of the original error vector $\mathbf{e}$. For $r \in \{1, \dots, n-1\}$, we can split the secret $\tilde{\mathbf{s}} = \begin{pmatrix} \mathbf{v} \\ \mathbf{s} \end{pmatrix}$ and the matrix $\mathbf{A} = (\mathbf{A}_1 | \mathbf{A}_2)$ into two parts and rewrite this LWE instance as

$$\mathbf{b}' = (\mathbf{A}_1 | \mathbf{A}_2) \begin{pmatrix} \mathbf{v} \\ \mathbf{s} \end{pmatrix} + \mathbf{e}' = \mathbf{A}_1 \mathbf{v} + \mathbf{A}_2 \mathbf{s} + \mathbf{e}' \mod q, \tag{3}$$

where $\mathbf{v} \in \{0,1\}^r, \mathbf{s} \in \{0,1\}^{n-r}, \mathbf{A}_1 \in \mathbb{Z}_q^{m \times r}, \mathbf{A}_2 \in \mathbb{Z}_q^{m \times (n-r)}, \mathbf{b}' = \mathbf{b} - (1/2) \cdot \mathbf{1} \in \mathbb{Q}^m$, and $\mathbf{e}' = \mathbf{e} - (1/2) \cdot \mathbf{1} \in \{-1/2, 1/2\}^m$.

The main idea of the attack is to guess $\mathbf{v}$ and solve the remaining LWE instance $(\mathbf{A}_2, \tilde{\mathbf{b}} = \mathbf{b}' - \mathbf{A}_1 \mathbf{v} = \mathbf{A}_2 \mathbf{s} + \mathbf{e}' \mod q)$, which has binary secret $\mathbf{s}$ and error $\mathbf{e}' \in \{-1/2, 1/2\}^m$. The new LWE instance obtained in this way turns out to be considerably easier to solve, since the determinant $\det(\Lambda_q(\mathbf{A}_2)) = q^{m-n+r}$ of the new lattice is significantly bigger than the determinant $\det(\Lambda_q(\mathbf{A})) = q^{m-n}$ of the original lattice (see Sect. 6.1 of [9]). The newly obtained LWE instance is solved by solving a close vector problem in the lattice $\Lambda_q(\mathbf{A}_2)$. In more detail, $\tilde{\mathbf{b}} = \mathbf{A}_2 \mathbf{s} + q\mathbf{w} + \mathbf{e}'$ for some vector $\mathbf{w} \in \mathbb{Z}^m$ is close to the lattice

Algorithm 1. The Hybrid Attack

Input : $q, r \in \mathbb{Z}$
$\mathbf{A} = (\mathbf{A}_1 | \mathbf{A}_2)$, where $\mathbf{A}_1 \in \mathbb{Z}_q^{m \times r}, \mathbf{A}_2 \in \mathbb{Z}_q^{m \times (n-r)}$
$\mathbf{b} \in \mathbb{Z}_q^m$
$\mathbf{B}$, a lattice basis of $\Lambda_q(\mathbf{A}_2)$

calculate $c = \lfloor r/4 \rceil$;
calculate $\mathbf{b}' = \mathbf{b} - (1/2) \cdot \mathbf{1}$;
while *true* **do**
  guess a binary vector $\mathbf{v}_1 \in \{0,1\}^r$ with c ones ;
  calculate $\mathbf{x}_1 = -\operatorname{NP}_{\mathbf{B}}(-\mathbf{A}_1\mathbf{v}_1) \in \mathbb{R}^m$;
  calculate $\mathbf{x}_2 = \operatorname{NP}_{\mathbf{B}}(\mathbf{b}' - \mathbf{A}_1\mathbf{v}_1) \in \mathbb{R}^m$;
  store $\mathbf{v}_1$ in all the boxes addressed by $\mathcal{A}_{\mathbf{x}_1}^{(r)} \cup \mathcal{A}_{\mathbf{x}_2}^{(r)}$;
  for *all* $\mathbf{v}_2 \neq \mathbf{v}_1$ *in all the boxes addressed by* $\mathcal{A}_{\mathbf{x}_1}^{(r)} \cup \mathcal{A}_{\mathbf{x}_2}^{(r)}$ **do**
    Set $\mathbf{v} = \mathbf{v}_1 + \mathbf{v}_2$ and calculate $\mathbf{x} = (1/2) \cdot \mathbf{1} + \operatorname{NP}_{\mathbf{B}}(\mathbf{b}' - \mathbf{A}_1\mathbf{v}) \in \mathbb{R}^m$;
    if $\mathbf{x} \in \{0,1\}^m$ *and* $\exists \tilde{\mathbf{s}} \in \{0,1\}^n : \mathbf{b} = \mathbf{A}\tilde{\mathbf{s}} + \mathbf{x} \mod q$ **then**
      return $\mathbf{x}$;

vector $\mathbf{A}_2\mathbf{s} + q\mathbf{w} \in \Lambda_q(\mathbf{A}_2)$ since $\mathbf{e}'$ is small. Hence $\mathbf{e}'$ can be found by running the nearest plane algorithm in combination with a sufficient basis reduction as a precomputation (see [32]).

The guessing of $\mathbf{v}$ is sped up by a Meet-in-the-Middle approach, i.e., guessing binary vectors $\mathbf{v}_1 \in \{0,1\}^r$ and $\mathbf{v}_2 \in \{0,1\}^r$ such that $\mathbf{v} = \mathbf{v}_1 + \mathbf{v}_2$. In order to recognize matching guesses $\mathbf{v}_1$ and $\mathbf{v}_2$ that sum up to $\mathbf{v}$, one searches for collisions in (hash) boxes. The addresses of these boxes are determined in the following way.

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

$$\mathcal{A}_{\mathbf{x}}^{(m)} = \left\{ \mathbf{z} \in \{0,1\}^m \,\middle|\, \begin{array}{l} (\mathbf{z})_i = 1 \text{ for all } i \in \{1,\ldots,m\} \text{ with } (\mathbf{x})_i > -1/2, \text{ and} \\ (\mathbf{z})_i = 0 \text{ for all } i \in \{1,\ldots,m\} \text{ with } (\mathbf{x})_i < -1/2 \end{array} \right\}.$$

Intuitively, for $\mathbf{x}_2$ obtained during Algorithm 1, the set $\mathcal{A}_{\mathbf{x}_2}^{(m)}$ captures all the possible sign vectors of $\mathbf{x}_2$ added up with a vector in $\{-1/2, 1/2\}^m$ (where 1 represents a non-negative and 0 a negative sign). For $\mathbf{x}_1$ obtained during Algorithm 1, the set $\mathcal{A}_{\mathbf{x}_1}^{(m)}$ consists only of the sign vector of $\mathbf{x}_1$. This is due to the fact that $\mathbf{x}_2 \in \mathbb{Z}^m + \{1/2\}^m$, whereas $\mathbf{x}_1 \in \mathbb{Z}^m$. This leads to the desired collisions, as can be seen in the upcoming Lemma 3.

3.2 Runtime Analysis

In this section we analyze the runtime and success probability of the attack presented in Algorithm 1. We start by presenting our main result.

Theorem 1. *Let $n, m, q, c \in \mathbb{N}$, and $1 \leq \delta \in \mathbb{R}$ be fixed. Consider the following input distribution of $(q, r, \mathbf{A}, \mathbf{b}, \mathbf{B})$ for Algorithm 1. The modulus q and the attack*

parameter $r = 4c$ *are fixed,* $\mathbf{A} = (\mathbf{A}_1|\mathbf{A}_2)$*, where* $\mathbf{A}_1 \xleftarrow{\$} \mathbb{Z}_q^{m\times r}$, $\mathbf{A}_2 \xleftarrow{\$} \mathbb{Z}_q^{m\times(n-r)}$, $\mathbf{b} = \mathbf{A}\begin{pmatrix}\mathbf{v}\\ \mathbf{s}\end{pmatrix} + \mathbf{e} \mod q$*, where* $\mathbf{v} \xleftarrow{\$} \{0,1\}^r$, $\mathbf{s} \xleftarrow{\$} \{0,1\}^{n-r}$, $\mathbf{e} \xleftarrow{\$} \{0,1\}^m$*, and* $\mathbf{B}$ *is some lattice basis of* $\Lambda_q(\mathbf{A}_2)$ *with Hermite delta* δ*. Let all notations be as in the above description of the input distribution. Assume that the approximations given in Heuristics 2 and 4 are in fact equations and that* $\mathrm{NP}_{\mathbf{B}}(\mathbf{b} - (1/2)\cdot\mathbf{1} - \mathbf{A_1 v}) = \mathbf{e} - (1/2)\cdot\mathbf{1}$*. Then, if Algorithm 1 terminates, it finds a valid binary error vector of the LWE with binary error instance* $(\mathbf{A}, \mathbf{b})$*. The probability that Algorithm 1 terminates is at least*

$$p_0 = 2^{-r}\binom{r}{2c}.$$

In case that Algorithm 1 terminates, the expected number of operations is

$$2^{16}\binom{r}{c}\left(p\binom{2c}{c}\right)^{-1/2},$$

with

$$p = \prod_{i=1}^{m}\left(1 - \frac{1}{r_i B(\frac{m-1}{2}, \frac{1}{2})}J(r_i, m)\right),$$

where $B(\cdot,\cdot)$ *denotes the Euler beta function (see [38]),*

$$J(r_i,m) = \begin{cases} \int_{-r_i-1}^{r_i-1}\int_{-1}^{z+r_i}(1-y^2)^{\frac{m-3}{2}}dydz \\ \quad + \int_{r_i-1}^{-r_i}\int_{z-r_i}^{z+r_i}(1-y^2)^{\frac{m-3}{2}}dydz & \text{for } r_i < \frac{1}{2} \\ \int_{-r_i-1}^{-r_i}\int_{-1}^{z+r_i}(1-y^2)^{\frac{m-3}{2}}dydz & \text{for } r_i \geq \frac{1}{2}, \end{cases}$$

and

$$r_i = \frac{\delta^{-2(i-1)+m}q^{\frac{m-n+r}{m}}}{2\sqrt{m/4}}.$$

Remark 1. *Algorithm 1 gets some basis* $\mathbf{B}$ *as input. This basis has a certain quality, given by the Hermite delta* δ*. In practice, we can improve the attack by providing a basis with better, i.e., smaller, Hermite delta. We achieve this by running a basis reduction (e.g., BKZ) on* $\mathbf{B}$ *in a precomputation step (see Sect. 3.3).*

We postpone the proof of Theorem 1 to the end of this subsection, since we first need to develop some necessary tools. We start by giving a definition of a notion which is crucial to our analysis. We then give a useful lemma.

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

Intuitively, $\mathbf{x}$ being $\mathbf{y}$-admissible means that running the nearest plane algorithm on $\mathbf{x}$ and running it on $\mathbf{x} - \mathbf{y}$ yields the same lattice vector, since then we have $\mathbf{x} - \mathrm{NP}(\mathbf{x}) = (\mathbf{x} - \mathbf{y}) - \mathrm{NP}(\mathbf{x} - \mathbf{y})$.

Lemma 2. *Let* $\mathbf{t}_1 \in \mathbb{R}^m, \mathbf{t}_2 \in \mathbb{R}^m$ *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.*

A proof of this lemma can be found in the full version [13].

As we will see in our analysis, the expected runtime heavily depends on the following probability. Let all notations be as in Theorem 1 and $\mathbf{e}' = \mathbf{e} - (1/2) \cdot \mathbf{1}$. For

$$W = \{\mathbf{w} \in \{0,1\}^r : \text{ exactly } c \text{ entries of } \mathbf{w} \text{ are } 1\} \tag{4}$$

we define

$$p := \begin{cases} \Pr_{\mathbf{v}_1 \leftarrow W}[-\mathbf{A}_1\mathbf{v}_1 \text{ is } \mathbf{e}'\text{-admissible} | \mathbf{v} - \mathbf{v}_1 \in W] & \text{if } \Pr_{\mathbf{v}_1 \leftarrow W}[\mathbf{v} - \mathbf{v}_1 \in W] > 0 \\ 0 & \text{else.} \end{cases} \tag{5}$$

Note that the hybrid attack requires that nearest plane called on the target vector $\mathbf{b} - (1/2) \cdot \mathbf{1} - \mathbf{A_1}\mathbf{v}$ returns the correct shifted error vector $\mathbf{e} - (1/2) \cdot \mathbf{1}$. However, this is not a big restriction in practice, since this probability is bigger than the probability that the same vector is $\mathbf{e}'$-admissible. To see why, recall that nearest plane returns the correct error vector if and only if it lies in the fundamental parallelepiped $\Lambda(\mathbf{B})$. On the other hand, Heuristic 3 states that the probability that $\mathbf{b} - (1/2) \cdot \mathbf{1} - \mathbf{A_1}\mathbf{v}$ is $\mathbf{e}'$-admissible is approximately the probability that the sum of a random point in $\Lambda(\mathbf{B})$ and the error vector is still in $\Lambda(\mathbf{B})$. Consequently, we expect that $\mathrm{NP}_{\mathbf{B}}(\mathbf{b} - (1/2) \cdot \mathbf{1} - \mathbf{A_1}\mathbf{v}) = \mathbf{e} - (1/2) \cdot \mathbf{1}$ holds with high probability for all realistic attack parameters.

Note that the analysis of the attack on the NTRU encryption proposed by Howgrave-Graham [25] also requires to calculate the probability p. In the original work, this is done experimentally. Replacing this probability estimation with the analytic methodology presented in the following removes the dependency on experimental support in the analysis of the hybrid attack. A first mathematical calculation of the probability p has already been presented by Hirschhorn et al. in [24]. However, their analysis requires an additional assumption that we no longer need.

Success Probability. In this subsection we determine the probability that Algorithm 1 terminates. We start by giving a sufficient condition for this event.

Lemma 3. *Let all notations be as in Theorem 1 and let* $\mathbf{b}' = \mathbf{b} - (1/2) \cdot \mathbf{1}$ *and* $\mathbf{e}' = \mathbf{e} - (1/2) \cdot \mathbf{1}$*. Assume that* $\mathbf{v}_1$ *and* $\mathbf{v}_2$ *are guessed in separate loops of Algorithm 1 and satisfy* $\mathbf{v}_1 + \mathbf{v}_2 = \mathbf{v}$*. Also let* $\mathbf{t}_1 = -\mathbf{A}_1\mathbf{v}_1$ *and* $\mathbf{t}_2 = \mathbf{b}' - \mathbf{A}_1\mathbf{v}_2$ *and assume* $\mathrm{NP}(\mathbf{t}_1) + \mathrm{NP}(\mathbf{t}_2) = \mathrm{NP}(\mathbf{t}_1 + \mathbf{t}_2) = \mathbf{e}'$ *holds. Then* $\mathbf{v}_1$ *and* $\mathbf{v}_2$ *collide in at least one box chosen during Algorithm 1 and the algorithm outputs the error vector* $\mathbf{e}$ *of the given LWE instance.*

Proof: According to the notation used in Algorithm 1, let $\mathbf{x}_1 = -\mathrm{NP}(\mathbf{t}_1)$ correspond to $\mathbf{v}_1$ and $\mathbf{x}_2 = \mathrm{NP}(\mathbf{t}_2)$ correspond to $\mathbf{v}_2$. By assumption we have $\mathbf{x}_1 = \mathbf{x}_2 - \mathbf{e}'$. Using the definition it is easy to verify that $\mathbf{x}_1$ and $\mathbf{x}_2$ share at least one common address, since $\mathbf{e}' \in \{-1/2, 1/2\}^m$. Therefore $\mathbf{v}_1$ and $\mathbf{v}_2$ collide in at least one box. Again by assumption, we obtain $\mathbf{x} = \mathrm{NP}(\mathbf{b}' - \mathbf{A}_1\mathbf{v}) = \mathrm{NP}(\mathbf{t}_1 + \mathbf{t}_2) = \mathbf{e}'$. Hence the algorithm outputs the error vector $\mathbf{e}$. ■

In the following lemma we give a lower bound on the probability that Algorithm 1 terminates.

Lemma 4. *Let all notations be as in Theorem 1 and let* $\mathbf{b}' = \mathbf{b} - (1/2) \cdot \mathbf{1}$ *and* $\mathbf{e}' = \mathbf{e} - (1/2) \cdot \mathbf{1}$. *Assume that if* $\mathbf{v}$ *has exactly* $2c$ *one-entries, then* $p > 0$, *where* p *is as defined in Eq. (5). If* $\mathrm{NP}(\mathbf{b}' - \mathbf{A_1}\mathbf{v}) = \mathbf{e}'$, *then Algorithm 1 terminates with probability at least*

$$p_0 = 2^{-r} \binom{r}{2c}.$$

Proof: We show that Algorithm 1 terminates if $\mathbf{v}$ consists of exactly $2c$ one-entries. The probability of this happening is exactly p_0, since there are 2^r binary vectors of length r, and $\binom{r}{2c}$ of them have exactly $2c$ one-entries. Assume that v consists of exactly $2c$ one-entries. The claim follows directly from Lemmas 2 and 3. Since $p > 0$ there exist binary vectors $\mathbf{v}_1, \mathbf{v}_2 \in \{0,1\}^r$, each containing exactly c one-entries, such that $\mathbf{v}_1 + \mathbf{v}_2 = \mathbf{v}$ and $-\mathbf{A_1}\mathbf{v_1}$ is $\mathbf{e}'$-admissible. These vectors will eventually be guessed during Algorithm 1 if it does not terminate before. By Lemma 2 they satisfy

$$\mathrm{NP}(-\mathbf{A}_1\mathbf{v}_1) + \mathrm{NP}(\mathbf{b}' - \mathbf{A}_1\mathbf{v}_2) = \mathrm{NP}(\mathbf{b}' - \mathbf{A}_1\mathbf{v}) = \mathbf{e}'.$$

Lemma 3 now guarantees that Algorithm 1 then outputs the error vector $\mathbf{e}$. ■

Estimating the Number of Loops. The next step is to estimate the number of loops until the attack terminates.

Heuristic 2. *Let all notations be as in Theorem 1 and let* $\mathbf{b}' = \mathbf{b} - (1/2) \cdot \mathbf{1}$ *and* $\mathbf{e}' = \mathbf{e} - (1/2) \cdot \mathbf{1}$. *Assume that* $\mathrm{NP}(\mathbf{b}' - \mathbf{A_1}\mathbf{v}) = \mathbf{e}'$, *and that* $\mathbf{v}$ *consists of exactly* $2c$ *one-entries. Then the expected number of loops of Algorithm 1 is*

$$L \approx \binom{r}{c} \left(p \binom{2c}{c} \right)^{-1/2},$$

and the probability p, *as given in Eq. (5), is*

$$p \approx \prod_{i=1}^{m} \left(1 - \frac{1}{r_i B(\frac{m-1}{2}, \frac{1}{2})} J(r_i, m) \right),$$

with $B(\cdot,\cdot)$, $J(\cdot,\cdot)$, *and* r_i *defined as in Theorem 1.*

In the following, we justify the heuristic. Assume that $\mathbf{v}$ consists of exactly $2c$ one-entries. In addition to W (see Eq. (4)), define the set

$$V = \{\mathbf{v}_1 \in W : \mathbf{v} - \mathbf{v}_1 \in W \text{ and } -\mathbf{A}_1\mathbf{v}_1 \text{ is } \mathbf{e}'\text{-admissible}\}.$$

Note that W is the set from which Algorithm 1 samples the vectors $\mathbf{v}_1$. Lemma 3 shows that the attack succeeds if two vectors $\mathbf{v}_1, \mathbf{v}_2 \in V$ satisfying $\mathbf{v}_1 + \mathbf{v}_2 = \mathbf{v}$ are sampled in different loops of Algorithm 1. Since otherwise the probability of success is close to zero, for simplicity we assume that the attack is only successful in this case. Therefore we need to estimate the necessary number of loops in Algorithm 1 until some $\mathbf{v}_1, \mathbf{v}_2 \in V$ with $\mathbf{v}_1 + \mathbf{v}_2 = \mathbf{v}$ are found. Note that by Lemma 2 if $\mathbf{v}_1 \in V$, then also $\mathbf{v}_2 = \mathbf{v} - \mathbf{v}_1 \in V$.

We start by calculating the probability that a vector sampled during Algorithm 1 lies in V. By definition of p, this probability is given by

$$\Pr_{\mathbf{v}_1 \xleftarrow{\$} W}[\mathbf{v}_1 \in V] = p_1 p, \text{ where } p_1 := \Pr_{\mathbf{v}_1 \xleftarrow{\$} W}[\mathbf{v} - \mathbf{v}_1 \in W].$$

Therefore we expect to sample a vector $\mathbf{v}_1 \in V$ every $\frac{1}{p_1 p}$ loops in Algorithm 1. The above equation also implies $p_1 p = \frac{|V|}{|W|}$, which gives us

$$|V| = p_1 p |W| = p_1 p \binom{r}{c}.$$

The probability p_1 is given by $p_1 = \binom{2c}{c} / \binom{r}{c}$, see the full version [13]. Therefore by the birthday paradox, the expected number of loops in Algorithm 1 until some $\mathbf{v}_1, \mathbf{v}_2 \in V$ with $\mathbf{v}_1 + \mathbf{v}_2 = \mathbf{v}$ are found can be estimated by

$$L \approx \frac{1}{p_1 p}\sqrt{|V|} = \frac{\sqrt{\binom{r}{c}}}{\sqrt{p_1 p}} = \binom{r}{c}\left(p\binom{2c}{c}\right)^{-1/2}.$$

It remains to approximate the probability p which we do in the following. Let $\mathbf{v}_1 \in \{0,1\}^r$ and $\mathbf{B}$ be some basis of $\Lambda_q(\mathbf{A}_2)$. By Lemma 1 there exist unique $\mathbf{u}_1, \mathbf{u}_2 \in \Lambda_q(\mathbf{A}_2)$ such that $\mathrm{NP}_{\mathbf{B}}(-\mathbf{A}_1\mathbf{v}_1) = -\mathbf{A}_1\mathbf{v}_1 - \mathbf{u}_1 \in \mathcal{P}(\overline{\mathbf{B}})$ and $\mathrm{NP}_{\mathbf{B}}(-\mathbf{A}_1\mathbf{v}_1 - \mathbf{e}') + \mathbf{e}' = -\mathbf{A}_1\mathbf{v}_1 - \mathbf{u}_2 \in \mathbf{e}' + \mathcal{P}(\overline{\mathbf{B}})$. Without loss of generality, in the following we assume $\mathbf{u}_1 = \mathbf{0}$, or equivalently $-\mathbf{A}_1\mathbf{v}_1 \in \mathcal{P}(\overline{\mathbf{B}})$. Now $-\mathbf{A}_1\mathbf{v}_1$ is $\mathbf{e}'$-admissible if and only if $\mathbf{u}_2 = \mathbf{u}_1 = \mathbf{0}$, which is equivalent to $\mathbf{e}' + \mathbf{A}_1\mathbf{v}_1 \in \mathcal{P}(\overline{\mathbf{B}})$. Therefore p is equal to the probability that $\mathbf{e}' + \mathbf{A}_1\mathbf{v}_1 \in \mathcal{P}(\overline{\mathbf{B}})$, which we determine in the following.

There exists some orthonormal transformation that aligns $\mathcal{P}(\overline{\mathbf{B}})$ along the standard axes of $\mathbb{R}^m$. By applying this transformation, we may therefore assume that $\mathcal{P}(\overline{\mathbf{B}})$ is aligned along the standard axes of $\mathbb{R}^m$ and that in consequence $\mathbf{e}'$ is a uniformly random vector of length $\sqrt{m/4}$. Because $\mathbf{A}_1$ is uniformly random in $\mathbb{Z}_q^{m\times r}$ we may further assume that $\mathbf{A}_1\mathbf{v}_1$ is uniformly random in $\mathcal{P}(\overline{\mathbf{B}})$, since without loss of generality we assume $\mathbf{A}_1\mathbf{v}_1 \in \mathcal{P}(\overline{\mathbf{B}})$. This gives rise to the following heuristic.

Heuristic 3. *The probability p as defined in Eq. 5 (with respect to a reduced basis with Hermite delta δ) is*

$$p \approx \Pr_{\mathbf{t} \xleftarrow{\$} R,\, \mathbf{e}' \xleftarrow{\$} S_m(\sqrt{m/4})} [\mathbf{t} + \mathbf{e}' \in R],$$

where

$$S_m(\sqrt{m/4}) = \{\mathbf{x} \in \mathbb{R}^m \mid \|\mathbf{x}\| = \sqrt{m/4}\}$$

is the surface of a sphere with radius $\sqrt{m/4}$ centered around the origin and

$$R = \{\mathbf{x} \in \mathbb{R}^m \mid \forall i \in \{1, \ldots, m\} : -R_i/2 \leq x_i < R_i/2\}$$

is the search rectangle with edge lengths

$$R_i = \delta^{-2(i-1)+m} q^{\frac{m-n+r}{m}}.$$

In the heuristic, the edge lengths are implied by the Geometric Series Assumption.

We continue calculating the approximation of p given in Heuristic 3. Let R and R_i be as defined in Heuristic 3. We can rewrite the approximation given in Heuristic 3 as

$$p \approx \Pr_{t_i \xleftarrow{\$} [-R_i/2, R_i/2], \mathbf{e}' \xleftarrow{\$} S_m(\sqrt{m/4})} [\forall i \in \{1, \ldots, m\} : t_i + e'_i \in [-R_i/2, R_i/2]].$$

Rescaling everything by a factor of $1/\sqrt{m/4}$ leads to

$$p \approx \Pr_{t_i \xleftarrow{\$} [-r_i, r_i], \mathbf{e}' \xleftarrow{\$} S_m(1)} [\forall i \in \{1, \ldots, m\} : t_i + e'_i \in [-r_i, r_i]],$$

where

$$r_i = \frac{R_i}{2\sqrt{m/4}} = \frac{\delta^{-2(i-1)+m} q^{\frac{m-n+r}{m}}}{2\sqrt{m/4}}. \tag{6}$$

Unfortunately, the distributions of the coordinates of $\mathbf{e}$ are not independent, which makes calculating p extremely complicated. In practice, however, the probability that $e_i \in [-R_i/2, R_i/2]$ is big for all but the last few indices i. This is due to the fact that by the Geometric Series Assumption typically only the last values R_i are small. Consequently, we expect the dependence of the remaining entries not to be strong. This assumption was already established by Howgrave-Graham [25] and appears to hold for all values of R_i appearing in practice.

It is therefore reasonable to assume that

$$p \approx \prod_{i=1}^{m} \Pr_{t_i \xleftarrow{\$} [-r_i, r_i], e'_i \xleftarrow{\$} D_m} [t_i + e'_i \in [-r_i, r_i]],$$

were D_m denotes the distribution on the interval $[-1, 1]$ obtained by the following experiment: sample a vector $\mathbf{w}$ uniformly at random on the unit sphere and then output the first (equivalently, any arbitrary but fixed) coordinate of $\mathbf{w}$.

Next we explore the density function of D_m. The probability that $e_i' \leq x$ for some $-1 < x < 0$, where $e_i' \xleftarrow{\$} D_m$, is given by the ratio of the surface area of a hyperspherical cap of the unit sphere in $\mathbb{R}^m$ with height $h = 1 + x$ and the surface area of the unit sphere. This is illustrated in the full version [13] for $m = 2$. The surface area of a hyperspherical cap of the unit sphere in $\mathbb{R}^m$ with height $h < 1$ is given by (see [31])

$$A_m(h) = \frac{1}{2} A_m I_{2h-h^2}\left(\frac{m-1}{2}, \frac{1}{2}\right),$$

where $A_m = 2\pi^{m/2}/\Gamma(m/2)$ is the surface area of the unit sphere and

$$I_x(a, b) = \frac{\int_0^x t^{a-1}(1-t)^{b-1} dt}{B(a, b)}$$

is the regularized incomplete beta function (see [38]) and $B(a, b)$ is the Euler beta function.

Consequently, for $-1 < x < 0$, we have

$$\begin{aligned}
\Pr_{e_i' \xleftarrow{\$} D_m}[e_i' \leq x] &= \frac{A_m(1+x)}{A_m} \\
&= \frac{1}{2} I_{1-x^2}\left(\frac{m-1}{2}, \frac{1}{2}\right) \\
&= \frac{1}{2B(\frac{m-1}{2}, \frac{1}{2})} \int_0^{1-x^2} t^{\frac{m-3}{2}} (1-t)^{-1/2} dt \\
&= \frac{1}{B(\frac{m-1}{2}, \frac{1}{2})} \int_{-1}^{x} (1-t^2)^{\frac{m-3}{2}} dt. \qquad (7)
\end{aligned}$$

Together with

$$\Pr_{t_i \xleftarrow{\$} [-r_i, r_i]}[t_i \leq x] = \int_{-r_i}^{x} \frac{1}{2r_i} dy,$$

we can use a convolution to obtain

$$\Pr_{t_i \xleftarrow{\$} [-r_i, r_i], e_i' \xleftarrow{\$} D_m}[t_i + e_i' \leq x] = \frac{1}{2r_i B(\frac{k-1}{2}, \frac{1}{2})} \int_{-r-1}^{x} \int_{\max(-1, z-r_i)}^{\min(1, z+r_i)} (1-y^2)^{\frac{m-3}{2}} dy dz.$$

Since

$$\Pr_{t_i \xleftarrow{\$} [-r_i, r_i], e_i' \xleftarrow{\$} D_m}[t_i + e_i' \in [-r_i, r_i]] = 1 - 2\left(\Pr_{t_i \xleftarrow{\$} [-r_i, r_i], e_i' \xleftarrow{\$} D_m}[t_i + e_i' < -r_i]\right),$$

it suffices to calculate the integral

$$J(r_i, m) = \int_{-r_i-1}^{-r_i} \int_{\max(-1, z-r_i)}^{z+r_i} (1-y^2)^{\frac{m-3}{2}} dy dz \tag{8}$$

in order to calculate p. We calculated the integral symbolically using sage [42], which allows an efficient calculation of p.

Time Spend per Loop Cycle. With the estimation of the number of loops given, the remaining task is to estimate the time spend per loop cycle. Each cycle consists of four steps:

1. Guessing a binary vector.
2. Running the nearest plane algorithm (twice).
3. Calculating $\mathcal{A}_{\mathbf{x}_1}^{(r)} \cup \mathcal{A}_{\mathbf{x}'_1}^{(r)}$.
4. Dealing with collisions in the boxes.

We assume that the runtime of one inner loop of Algorithm 1 is dominated by the runtime of the nearest plane algorithm, as argued in the following. It is well known that sampling a binary vector is extremely fast. Furthermore, note that only very few of the 2^n addresses contain a vector, since filling a significant proportional would take exponential time. Consequently, collisions are extremely rare, and lines 8–11 of Algorithm 1 do not contribute much to the overall runtime.

An estimation by Howgrave-Graham [25] shows that for typical instances, the runtime of the nearest plane algorithm exceeds the time spent for storing the collision. We therefore omit the latter from our considerations.

Lindner and Peikert [32] estimated the time necessary to run the nearest plane algorithm to be about 2^{-16} seconds, which amounts to about 2^{15} bit operations on their machine. This leads to the following heuristic for the runtime of the attack.

Heuristic 4. *The average number of operations per inner loop in Algorithm 1 is* $N \approx 2^{16}$.

Total Runtime. We are now able to prove our main theorem.

Proof (Theorem 1): By definition, every output of Algorithm 1 is a valid binary error vector of the given LWE with binary error instance. The rest follows directly from Lemma 4, Heuristics 2 and 4. ■

3.3 Minimizing the Expected Runtime

As mentioned in Remark 1, we can perform a basis reduction to obtain a lattice basis with smaller Hermite delta δ before running the actual attack in order to speed up the attack. We perform a binary search for the δ such that the estimated runtimes of both the basis reduction and the actual attack are about equal. We also need to optimise r, the Meet-in-the-Middle dimension, which we do numerically, as there are only finitely many r to check. We refer the reader to the full version [13] for further details on the choice of δ and r.

4 Comparison

In this section we consider other approaches to solve LWE with binary error and compare these algorithms to Algorithm 1. In particular we give upper bounds for the runtimes of the algorithms. A comparison of the most practical attacks, including the hybrid attack, is given in Table 1.

Much of the analyses below are in a similar spirit to that given in the survey [5] for methods of solving standard LWE. However we are often able to specifically adapt the analysis for the binary error case. Note that to solve LWE with binary error, in addition to algorithms for standard LWE, one may also be able to apply algorithms for the related Inhomogeneous Short Integer Solution problem. A discussion of these algorithms is given in [10].

4.1 Number of Samples

Recall that for reducing LWE with binary error to worst-case problems on lattices, one must restrict the number of samples to be $m = n\,(1 + \Omega(1/\log n))$ [35, Theorem 1.2]. On the other hand, with slightly more than linear samples, such as $m = \mathcal{O}(n \log\log n)$, the algorithm given in [1] is subexponential. Therefore if a scheme bases its security on the hardness of LWE with binary error, it is reasonable to expect that one has only access to at most linearly many samples. We assume this is the case in our analysis below. For concreteness, we fix $m = 2n$.

4.2 Algorithms for Solving LWE

There are several approaches one could use to solve LWE or its variants (see the survey [5]). One may employ combinatorial algorithms such as the BKW [2,11]

Table 1. Comparison of attacks on LWE with binary error using at most $m = 2n$ samples. $\log_2(T_{\text{attack}})$ denotes the bit operations required to perform the algorithm described in 'attack'. For algorithms requiring lattice reduction, we choose whichever is the fewer of $m = 2n$ or the 'optimal subdimension' $m = \sqrt{n \log(q)/\log(\delta)}$ [36].

Instance	n	q	$\log_2(T_{\text{Hybrid attack}})$	$\log_2(T_{\text{Decoding}})$	$\log_2(T_{\text{uSVP}})$	$\log_2(T_{\text{Distinguishing}})$
I	128	256	**55**	67	82	**37**
II	160	256	**61**	77	122	**62**
III	192	256	**68**	88	162	**85**
IV	224	256	**76**	**102**	165	109
V	256	256	**85**	**117**	203	132
VI	288	256	**98**	**136**	254	154
VII	320	256	**110**	**158**	327	176
VIII	352	256	**123**	**185**	443	198

algorithm and its variants [3,17,23,27]. However, all these algorithms require far more samples than are available in the binary error case, and are therefore ruled out. We also omit a Meet-in-the-Middle attack [5] or attacks based on the algorithm of Arora and Ge [1,6], as they will be slower than other methods. We consider them in the full version [13] for completeness.

Distinguishing Attack. One can solve LWE via a distinguishing attack as described in [32,36]. The idea is to find a short vector $\|\mathbf{v}\|$ in the scaled dual lattice of $\mathbf{A}$, i.e. the lattice $\Lambda = \{\mathbf{w} \in \mathbb{Z}_q^m \mid \mathbf{w}\mathbf{A} \equiv 0 \mod q\}$. Then, if the problem is to distinguish $(\mathbf{A}, \mathbf{b})$ where $\mathbf{b}$ is either formed as an LWE instance $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$ or is uniformly random, one can use this short vector $\mathbf{v}$ as follows. Consider $\langle \mathbf{v}, \mathbf{b} \rangle = \langle \mathbf{v}, \mathbf{e} \rangle$ if $\mathbf{b}$ is from an LWE instance, which as the inner product of two short vectors, is small mod q. On the other hand, if $\mathbf{b}$ is uniform then $\langle \mathbf{v}, \mathbf{b} \rangle$ is uniform on $\mathbb{Z}_q$ so these cases can be distinguished if $\mathbf{v}$ is suitably small.

We determine how small a $\mathbf{v}$ which must be found as follows. Recall that our errors are chosen uniformly at random from $\{0, 1\}$. So they follow a Bernoulli distribution with parameter $1/2$, and have expectation $1/2$ and variance $1/4$. Consider the distribution of $\langle \mathbf{v}, \mathbf{e} \rangle$. Since the errors e_i are chosen independently, its expectation is $\frac{1}{2}\sum_{i=1}^{m} v_i$ and its variance is $\frac{1}{4}\sum_{i=1}^{m} v_i^2$. Since $\langle \mathbf{v}, \mathbf{e} \rangle$ is the sum of many independent random variables, asymptotically it follows a normal distribution with those parameters. Since the distinguishing attack success is determined by the variance and not the mean, and we can account for the mean, we assume it is zero. Then we can use the result of [32] to say that we can distinguish a Gaussian from uniform with advantage close to $\exp(-\pi(\|\mathbf{v}\| \cdot s/q)^2)$, where s is the width parameter of the Gaussian. In our case $s^2 = 2\pi \cdot \frac{1}{4}$ so we can distinguish with advantage close to $\epsilon = \exp(-\pi^2 \|\mathbf{v}\|^2 / 2q^2)$. Therefore to distinguish with advantage ϵ we require a vector $\mathbf{v}$ of length $\|\mathbf{v}\| = q \cdot \frac{\sqrt{2\ln(1/\epsilon)}}{\pi}$.

We calculate a basis of the scaled dual lattice Λ and find a short vector $\mathbf{v} \in \Lambda$ by lattice basis reduction. With high probability the lattice Λ has rank m and volume q^n [5,36]. By definition of the Hermite delta we therefore have $\|\mathbf{v}\| = \delta^m q^{n/m}$. So the Hermite delta we require to achieve for the attack to succeed with advantage ϵ is given by $\delta^m q^{n/m} = q \cdot \frac{\sqrt{2\ln(1/\epsilon)}}{\pi}$. Assuming that the number of samples m is large enough to use the 'optimal subdimension' $m = \sqrt{n \log(q)/\log(\delta)}$ [36], we rearrange to obtain

$$\log \delta = \frac{\left(\log(q) + \log\left(\frac{\sqrt{2\ln(1/\epsilon)}}{\pi}\right)\right)^2}{4n\log(q)}.$$

To establish the estimates for the runtime of this attack given in Table 1, we assume one has to run the algorithm about $1/\epsilon$ times to succeed, and consider δ as a function of ϵ. The overall running time is then given by $1/\epsilon$ multiplied the estimated time, according to Eq. (1), to achieve $\delta(\epsilon)$. We pick the optimal ϵ such that this overall running time is minimized.

It is possible that we do not have enough samples to use the 'optimal subdimension', in which case we use $m = 2n$. For details, see the full version [13].

Reducing to uSVP. One may solve LWE via Kannan's embedding technique [26], thus seeing an LWE instance as a unique shortest vector problem instance. This technique is used in [4,9]. We follow analogously the analysis in [4,5] for the LWE with binary error case and obtain that we require a Hermite delta of $\log(\delta) = \frac{[\log(q)-\log(2\tau\sqrt{\pi e})]^2}{4n\log(q)}$ for this attack to succeed. The number of operation necessary to achieve this Hermite delta is estimated using Eq. (1). A comprehensive analysis can be found in the full version [13].

Decoding. The decoding approach for solving LWE was first described in [32] and is based on Babai's nearest plane algorithm [7]. The aim is to recover the error vector (so seeing LWE as a Bounded Distance Decoding instance). Recall (Lemma 1) that the error vector can be recovered using Babai's algorithm if it lies within the fundamental parallelepiped of the Gram-Schmidt basis. The idea of Lindner and Peikert in [32] is to widen the search parallelepiped to

$$\mathcal{P}_{\text{decoding}} = \{\mathbf{x} \in \mathbb{Z}^m \mid \mathbf{x} = \sum_{i=1}^{n} \alpha_i d_i \overline{\mathbf{b}}_i \text{ for } -1/2 \leq \alpha_i < 1/2\},$$

where $d_1, \ldots, d_m$ are integers chosen by the attacker.

Following the analysis of Lindner and Peikert, we estimate that an attack on a reduced basis with Hermite delta δ requires about $2^{15} \cdot \prod_{i=1}^{m} d_i$ operations. However, the analysis of the success probability is more complicated. By definition of search parallelepiped, the attack succeeds if (and only if) the error $\mathbf{e}$ lies in the search rectangle $\mathcal{P}_{\text{decoding}}$. Under the same assumption as in Sect. 3.2 (and using the same error transformation), this probability can be estimated via

$$p_{\text{decoding}} \approx \prod_{i=1}^{m} \left(\Pr_{\mathbf{e}_i \xleftarrow{\$} D_m} [\mathbf{e}_i \in [-r_i, r_i]] \right)$$

where

$$r_i = d_i \frac{\delta^{-2(i-1)+m} q^{\frac{m-n}{m}}}{2\sqrt{m/4}}.$$

Together with Eq. (7), this leads to

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

A standard way to increase the runtime of the attack is to use basis reduction (like BKZ2.0) as precomputation. Predicting the runtime of BKZ2.0 according to Eq. (1) leads to the runtime estimation

$$T_{\text{decoding}} \approx \frac{2^{1.8/\log_2(\delta)-110} \cdot 2.3 \cdot 10^9 + 2^{15} \prod_{i=1}^{m} d_i}{p_{\text{decoding}}}.$$

Using the same numeric optimization techniques as presented above to minimize the expected runtime leads to the complexity estimates given in Table 1.

Acknowledgements. Player was supported by an ACE-CSR PhD grant. This work has been co-funded by the DFG as part of project P1 within the CRC 1119 CROSSING. We thank Sean Murphy for useful discussions and comments.

References

1. Albrecht, M.R., Cid, C., Faugère, J., Fitzpatrick, R., Perret, L.: Algebraic algorithms for LWE problems. In: IACR Cryptology ePrint Archive 2014, p. 1018 (2014)
2. Albrecht, M.R., Cid, C., Faugère, J., Fitzpatrick, R., Perret, L.: On the complexity of the BKW algorithm on LWE. Des. Codes Crypt. **74**(2), 325–354 (2015)
3. Albrecht, M.R., Faugère, J., Fitzpatrick, R., Perret, L.: Lazy modulus switching for the BKW algorithm on LWE. In: Krawczyk [28], pp. 429–445
4. Albrecht, M.R., Fitzpatrick, R., Göpfert, F.: On the efficacy of solving LWE by reduction to unique-SVP. In: Lee, H.-S., Han, D.-G. (eds.) ICISC 2013. LNCS, vol. 8565, pp. 293–310. Springer, Heidelberg (2014)
5. Albrecht, M.R., Player, R., Scott, S.: On the concrete hardness of learning with errors. J. Math. Cryptology **9**(3), 169–203 (2015)
6. Arora, S., Ge, R.: New algorithms for learning in presence of errors. In: Aceto, L., Henzinger, M., Sgall, J. (eds.) ICALP 2011, Part I. LNCS, vol. 6755, pp. 403–415. Springer, Heidelberg (2011)
7. Babai, L.: On Lovász' lattice reduction and the nearest lattice pointproblem. In: Mehlhorn, K. (ed.) STACS 85. LNCS, vol. 182, pp. 13–20. Springer, Berlin (1985)
8. Babai, L.: On Lovász' lattice reduction and the nearest lattice point problem. Combinatorica **6**(1), 1–13 (1986)
9. Bai, S., Galbraith, S.D.: Lattice decoding attacks on binary LWE. In: Susilo, W., Mu, Y. (eds.) ACISP 2014. LNCS, vol. 8544, pp. 322–337. Springer, Heidelberg (2014)
10. Bai, S., Galbraith, S.D., Li, L., Sheffield, D.: Improved exponential-time algorithms for inhomogeneous-sis. In: IACR Cryptology ePrint Archive 2014, p. 593 (2014)
11. Blum, A., Kalai, A., Wasserman, H.: Noise-tolerant learning, the parity problem, and the statistical query model. J. ACM **50**(4), 506–519 (2003)
12. Brakerski, Z., Vaikuntanathan, V.: Efficient fully homomorphic encryption from(standard) LWE. In: Ostrovsky, R. (eds.) FOCS 2011, pp. 97–106, Palm Springs, CA, USA. IEEE Computer Society , 22–25 October 2011
13. Buchmann, J., Göpfert, F., Player, R., Wunderer, T.: On the hardness of LWE with binary error: revisiting the hybridlattice-reduction and meet-in-the-middle attack. Cryptology ePrint Archive, Report 2016/089 (2016). http://eprint.iacr.org/
14. Canetti, R., Garay, J.A. (eds.): CRYPTO 2013, Part I. LNCS, vol. 8042. Springer, Heidelberg (2013)
15. Chen, H., Lauter, K.E., Stange, K.E.: Attacks on search RLWE. IACR Cryptology ePrint Archive 2015, p. 971 (2015)
16. Chen, Y., Nguyen, P.Q.: BKZ 2.0: better lattice security estimates. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 1–20. Springer, Heidelberg (2011)

17. Duc, A., Tramèr, F., Vaudenay, S.: Better algorithms for LWE and LWR. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9056, pp. 173–202. Springer, Heidelberg (2015)
18. Ducas, L., Durmus, A., Lepoint, T., Lyubashevsky, V.: Lattice signatures and bimodal gaussians. In: Canetti, R., Garay, J.A. (eds.) [14], pp. 40–56
19. Eisenträger, K., Hallgren, S., Lauter, K.: Weak Instances of PLWE. In: Joux, A., Youssef, A. (eds.) SAC 2014. LNCS, vol. 8781, pp. 183–194. Springer, Heidelberg (2014)
20. Elias, Y., Lauter, K.E., Ozman, E., Stange, K.E.: Provably weak instances of ring-LWE. In: Gennaro, R., Robshaw, M. (eds.) [21], pp. 63–92
21. Gennaro, R., Robshaw, M. (eds.): CRYPTO 2015. LNCS, vol. 9215. Springer, Berlin (2015)
22. Güneysu, T., Lyubashevsky, V., Pöppelmann, T.: Practical lattice-based cryptography: a signature scheme for embedded systems. In: Prouff, E., Schaumont, P. (eds.) CHES 2012. LNCS, vol. 7428, pp. 530–547. Springer, Heidelberg (2012)
23. Guo, Q., Johansson, T., Stankovski, P.: Coded-BKW: solving LWE using lattice codes. In: Gennaro, R., Robshaw, M. (eds.) [21], pp. 23–42
24. Hirschhorn, P.S., Hoffstein, J., Howgrave-Graham, N., Whyte, W.: Choosing NTRUEncrypt parameters in light of combined lattice reduction and MITM approaches. In: Abdalla, M., Pointcheval, D., Fouque, P.-A., Vergnaud, D. (eds.) ACNS 2009. LNCS, vol. 5536, pp. 437–455. Springer, Heidelberg (2009)
25. Howgrave-Graham, N.: A hybrid lattice-reduction and meet-in-the-middle attack against NTRU. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 150–169. Springer, Heidelberg (2007)
26. Kannan, R.: Minkowski's convex body theorem and integer programming. Math. Oper. Res. **12**(3), 415–440 (1987)
27. Kirchner, P., Fouque, P.: An improved BKW algorithm for LWE with applications to cryptography and lattices. In: Gennaro, R., Robshaw, M. (eds.) [21], pp. 43–62
28. Krawczyk, H. (ed.): PKC 2014. LNCS, vol. 8383. Springer, Heidelberg (2014)
29. Laine, K., Lauter, K.E.: Key recovery for LWE in polynomial time. IACR Cryptology ePrint Archive 2015, p. 176 (2015)
30. Langlois, A., Ling, S., Nguyen, K., Wang, H.: Lattice-based group signature scheme with verifier-local revocation. In: Krawczyk, H. (ed.) [28], pp. 345–361
31. Li, S.: Concise formulas for the area and volume of a hyperspherical cap. Asian J. Math. Stat. **4**(1), 66–70 (2011)
32. Lindner, R., Peikert, C.: Better key sizes (and attacks) for LWE-based encryption. In: Kiayias, A. (ed.) CT-RSA 2011. LNCS, vol. 6558, pp. 319–339. Springer, Heidelberg (2011)
33. Liu, M., Nguyen, P.Q.: Solving BDD by enumeration: an update. In: Dawson, E. (ed.) CT-RSA 2013. LNCS, vol. 7779, pp. 293–309. Springer, Heidelberg (2013)
34. Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. J. ACM **60**(6), 43 (2013)
35. Micciancio, D., Peikert, C.: Hardness of SIS and LWE with small parameters. In: Canetti, R., Garay, J.A. (eds.) [14], pp. 21–39
36. Micciancio, D., Regev, O.: Lattice-based cryptography. Springer, Berlin (2009)
37. Micciancio, D., Walter, M.: Practical, predictable lattice basis reduction. IACR Cryptology ePrint Archive 2015, p. 1123 (2015)
38. Olver, F.W.: NIST Handbook of Mathematical Functions. Cambridge University Press, Cambridge (2010)

39. Peikert, C.: Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In: Mitzenmacher, M. (eds.) STOC 2009, pp. 333–342, Bethesda, MD, USA. ACM, May 31–June 2, 2009
40. Peikert, C., Waters, B.: Lossy trapdoor functions and their applications. SIAM J. Comput. **40**(6), 1803–1844 (2011)
41. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: Gabow, H.N., Fagin, R. (eds.) Proceedings of the 37th Annual ACM Symposium on Theory of Computing, pp. 84–93, Baltimore, MD, USA. ACM, 22–24 May 2005
42. Stein, W., et al.: Sage Mathematics Software (Version 6.3). The Sage Development Team (2014). http://www.sagemath.org

http://www.springer.com/978-3-319-31516-4

Progress in Cryptology – AFRICACRYPT 2016
8th International Conference on Cryptology in Africa,
Fes, Morocco, April 13-15, 2016, Proceedings
Pointcheval, D.; Nitaj, A.; Rachidi, T. (Eds.)
2016, X, 369 p. 49 illus., Softcover
ISBN: 978-3-319-31516-4