Institute of Information Security

University of Stuttgart
Universitätsstraße 38
D–70569 Stuttgart

Bachelorarbeit

# A Tool for the Estimation of Lattice Parameters

Nicolai Krebs

**Course of Study:** Informatik, B.Sc.

**Examiner:** Prof. Dr. Ralf Küsters

**Supervisor:** Marc Rivinius, M.Sc.

**Commenced:** April 22, 2021

**Completed:** October 22, 2021

## Abstract

<Short summary of the thesis>

# Contents

# List of Figures

# List of Tables

# List of Listings

# List of Algorithms

# 1 Introduction

- rise of quantum computing (short history)

* conceptual

* reality

- problem: some hard classical problems no longer hard

* Shor's Algorithm (Peter Shor, 1994) => quantum computers can solve the factoring and the discrete logarithm problem in polynomial time

* application to encryption

* overview of current encryption methods that will become insecure

- one solution (among hash-based, code-based, isogeny-based, and multivariate): lattice crypto

* overview over history and capability of lattice crypto

* advantages: good (quasilinear) asymptotic key sized, good concrete runtimes and key sizes, worst-case secure instantiations, advanced cryptographic primitives previously infeasible

* including intro to LWE/SIS and applications to build crypto systems

. SIS: signature schemes, hash functions

. LWE: “cryptomania” applications (PKE, ...), signature schemes, lines:

- cryptographic applications

- establishing theoretical and asymptotic hardness [Reg05] [BLP+13; MP13] - concrete hardness of LWE: attacks, runtime estimates,

* briefly outline concept and benefits of hard-case to average-case reductions

- purpose of this thesis

* building schemes: need realistic hardness estimates of schemes for given parameter settings

* lack in the past: no unified/easy to use tool => thesis aims to solve this problem tool we call *Lattice Parameter Estimation*

- overview of chapters/how to read

# 2 Preliminaries

## 2.1 Notation

In the following, we denote vectors by bold lower-case letters like $\mathbf{v}$ and matrices by bold upper-case letters $\mathbf{M}$. Unless specified otherwise, $\|\cdot\|$ is the Euclidean norm. By $[n]$ we denote the set $\{1, \ldots, n\}$ for $n \in \mathbb{Z}^+$.

## 2.2 Math

### 2.2.1 Norms and Bounds

Let $\mathcal{R}_q$ be a ring as defined in [BDL+18] and $f \in \mathcal{R}_q$ with $f = \sum_i f_i X^i$. We define the following norms [BDL+18]:

$$\ell_1 : \|f\|\|_1 = \sum_i |f_i| \tag{2.1}$$

$$\ell_2 : \|f\|\|_2 = \left(\sum_i |f_i|^2\right)^{\frac{1}{2}} \tag{2.2}$$

$$\ell_\infty : \|f\|\|_\infty = \max_i |f_i| \tag{2.3}$$

Then the following inequations hold [BDL+18]:

$$\|f\|_1 \leq \sqrt{n}\|f\|_2 \tag{2.4}$$

$$\|f\|_1 \leq n\|f\|_\infty \tag{2.5}$$

$$\|f\|_2 \leq \sqrt{n}\|f\|_\infty \quad (\text{since } \sqrt{n}\|f\|_2 \leq n\|f\|_\infty) \tag{2.6}$$

$$\|f\|_\infty \leq \|f\|_1 \tag{2.7}$$

Let $O_K$ be the ring of integers of a number field $K = \mathbb{Q}(\theta)$, where $\theta$ is an algebraic number and $\sigma$ denote the canonical embedding as defined in [DPSZ12]. Then, for $x, y \in O_K$ it holds the following inequations hold (we assume that $C_m$ in [DPSZ12] is 1) [DPSZ12].

$$\|f\|_\infty \leq \|\sigma(f)\|_\infty \tag{2.8}$$

$$\|\sigma(f)\|_\infty \leq \|f\|_1 \tag{2.9}$$

From the above inequations, we obtain the following norm transformations to $\ell_p$-norms:

- From Equation (2.4), it follows that $\|f\|_1 \leq \sqrt{n}\|f\|_2$ and from Equation (2.5), $\|f\|_1 \leq n\|f\|_\infty$.
- From Equation (2.6) and Equation (2.7), it follows that $\|f\|_2 \leq \sqrt{n}\|f\|_1$ and from Equation (2.6), $\|f\|_2 \leq \sqrt{n}\|f\|_\infty$.
- From Equation (2.7), it follows that $\|f\|_\infty \leq \|f\|_1$ and from Equation (2.4) and Equation (2.7), $\|f\|_\infty \leq \sqrt{n}\|f\|_2$.
- From Equation (2.9), it follows that $\|\sigma(f)\|_\infty \leq \|f\|_1$, from Equation (2.4) and Equation (2.9), $\|\sigma(f)\|_\infty \leq \sqrt{n}\|f\|_2$, and from Equation (2.5) and Equation (2.9), $\|\sigma(f)\|_\infty \leq n\|f\|_\infty$.

Likewise, we get the following transformations to the $C_\infty$-norm:

- From Equation (2.5) and Equation (2.8), it follows that $\|f\|_1 \leq n\|\sigma(f)\|_\infty$.
- From Equation (2.6) and Equation (2.8), it follows that $\|f\|_2 \leq \sqrt{n}\|\sigma(f)\|_\infty$.
- From Equation (2.8), it follows that $\|f\|_\infty \leq \|\sigma(f)\|_\infty$.

Let $f$ be defined as above and let $g \in \mathcal{R}_q$ where $g = \sum_i \overline{g}_i X^i$ where $g_i \in [-(q-1)/2, (q-1)/2]$ and $\overline{g}_i = g_i \mod q$ as in [BDL+18]. Then, we can define the following inequations for multiplication according to [BDL+18]:

- If $\|f\|_\infty \leq \beta, \|g\|_1 \leq \gamma$ then $\|f \cdot g\|_\infty \leq \beta \cdot \gamma$.
- If $\|f\|_2 \leq \beta, \|g\|_2 \leq \gamma$ then $\|f \cdot g\|_\infty \leq \beta \cdot \gamma$.

Let $x, y \in \mathcal{O}_K$. Again, we assume that $C_m = 1$. Then, the following inequation holds according to [DPSZ12]:

(2.10)
$$\|x \cdot y\|_\infty \leq C_m \cdot n^2 \cdot \|x\|_\infty \cdot \|y\|_\infty$$
(2.11)
$$\|\sigma(x \cdot y)\|_\infty \leq \|\sigma(x)\|_\infty \cdot \|\sigma(y)\|_\infty.$$

### 2.2.2 lattice

- background and history: example from lecture -> change

* Birhoff [Bir40]

* cryptoanalysis [LLL82]

* cryptosystems [Ajt96, HPS98] SIS introduced Ajtai [Ajt96]

* [MR04]

* LWE, assumption: worst-case lattice problems are hard [Reg05]

* fully homomorphic [Gen09]

* BGV scheme [BV11, BGV12]

* tools [LPR10, LPR13] ideal latties, RLWE

Other Notes: - PKE [AD97; Reg03; Reg05], CCA security [Pei09; PW08], identity-based encryption [ABB10; CHKP10; GPV08], fully homomorphic [Gen09] - , LWE introduced by [Reg05] "provably as hard as certain lattice problems in worst case, appear to require time exponential in main security parameter to solve NTRU [HPS98] - $q$-ary lattice: modulus $q \geq 2$

- math * lattice $\Lambda$

- discrete additive subgroup of $\mathbb{R}^m$

- Let $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$ be a set of linearly independent basis vectors and $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n] \in \mathbb{R}^{m \times n}$ be the corresponding basis with column vectors $\mathbf{b}_i$

- $n$ is the dimension of the Lattice

- $\Lambda(\mathbf{B})$ defined by all integer combinations of elements of $\mathbf{B}$:

$$\Lambda(\mathbf{B}) = \left\{ x \in \mathbb{R}^m \mid \exists \alpha_1, \ldots, \alpha_n \in \mathbb{Z} : \mathbf{x} = \sum_{i=1}^{n} \alpha_i \mathbf{b}_i \right\} \tag{2.12}$$

- show example plot

- full-ranked lattice: dimension is maximal, $m$

- basis $\mathbf{B}$ is not unique -> let $\mathbf{U} \in \mathbb{Z}^{n \times n}$ be a modular matrix (determinant is $\pm 1$), then $\mathbf{B} \cdot \mathbf{U}$ is also a basis of the $\Lambda$ ($\mathbf{U} \cdot \mathbb{Z}^n = \mathbb{Z}^n$) -> different basis for the same lattice $\Lambda$

- lattice coset: quotient group $\mathbb{R}^n / \Lambda$ of cosets

$$\mathbf{c} + \Lambda = \mathbf{c} + \mathbf{v} \mid v \in \Lambda$$

with $\mathbf{c} \in \mathbb{R}^n$

- fundamental domain: subset of $\mathbb{R}^m$ containing exactly one representative of every coset

- fundamental parallelipiped : $\mathcal{P}(\mathbf{B}) = \mathbf{B} \cdot [-1/2, 1/2)^n = \left\{ \mathbf{x} \in \mathbb{R}^m \mid \mathbf{x} \sum_{i=1}^{n} \gamma_i \mathbf{x}_i, \gamma_i \in [-1/2, 1/2) \right\}$ every coset has representative

- determinant of a full-ranked lattice $\Lambda(\mathbf{B})$

$$\det(\Lambda(\mathbf{B})) = |\det(\mathbf{B})| \tag{2.13}$$

is well-defined (independent from basis) => volume of fundamental domain can be generalized to not full-ranked => $\det(\Lambda(\mathbf{A})) = \sqrt{\det(\mathbf{A}^{\perp}\mathbf{A})}$

* minimum distance of $\lambda_1(\Lambda)$ of a lattice is the length of its shortest nonzero vector, i.e. $\lambda_1(\Lambda) \min_{v \in \Lambda \setminus \{0\}}$ * $i$th successive minimum $\lambda_i(\Lambda)$

- smallest radius $r$ such that $\Lambda$ has $i$ linearly independent lattice vectors of norm at most $r$

- in general hard to calculate $\lambda_i(\Lambda(\mathbf{B}))$ for a given basis

* modular integer (or $q$-ary) lattices

- full-ranked lattice $\Lambda$ such that $q\mathbb{Z}^m \subseteq \Lambda \subseteq \mathbb{Z}^m$ given $q \in \mathbb{N}$ => if $\mathbf{x} \in \mathbb{Z}^m$ in $\Lambda$ then $\mathbf{x} \mod q$ also in $\Lambda$.

- can be specified in two ways by matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$:

(2.14) $\Lambda_q(\mathbf{A}) = \{x \in \mathbb{Z}^m \mid \exists y \in \mathbb{Z}^n : \mathbf{x} = \mathbf{A}\mathbf{y} \mod q\}$

or

(2.15) $\Lambda_q^\perp(\mathbf{A}) = \{x \in \mathbb{Z}^m \mid \mathbf{A}^\intercal \mathbf{x} = 0 \mod q\}$

- finding a short vector in $\Lambda_q(\mathbf{A})$ corresponds to LWE

- finding short vectors in $\Lambda_q^\perp(\mathbf{A})$ corresponds to SIS

- easy to find basis of $\Lambda_q(\mathbf{A})$ [AFG13]

- with high probability determinant of $q$-ary lattice is $\det(\Lambda_q(\mathbf{A})) = q^{m-n}$ if $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$

* Gram-Schmidt basis

- set of column vectors $\mathbf{B} \in \mathbb{Z}_q^{m \times n}$, $\pi_{\mathrm{span}(\mathbf{B})}(\mathbf{t})$ for projection of vector $\mathbf{t}$ unto span of vectors of $\mathbf{B}$

- $\pi_{\mathrm{span}(\mathbf{B})}(\mathbf{t}) = \mathbf{B}(\mathbf{B}^\perp \mathbf{B})^{-1}\mathbf{B}^\intercal \cdot \mathbf{t}$

- Gram-Schmidt orthogonalization $\tilde{\mathbf{B}} = \left[\tilde{\mathbf{b}}_1 \cdots \tilde{\mathbf{b}}_n\right]$ of basis $\mathbf{B}$: $\tilde{\mathbf{b}}_i = \mathbf{b}_i - \pi_{\mathrm{span}(\mathbf{b}_1,\ldots,\mathbf{b}_{i-1})}(\mathbf{b}_i)$ for $i \in \{1, \ldots, n\}$

Alternative: Let $\mathbf{B} = [\mathbf{b}_1 \cdots \mathbf{b}_n], \mathbf{b}_i \in \mathbb{Z}_q^m$ be a basis. Define $\tilde{\mathbf{b}}_i$ as follows: $\tilde{\mathbf{b}}_1 = \mathbf{b}_1$. For $i \in \{2, \ldots, n\}$ let $\tilde{\mathbf{b}}_i$ be the component of $\mathbf{b}_i$ that is orthogonal to the span of $\{\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}\}$. Then, $\tilde{\mathbf{B}} = \left[\tilde{\mathbf{b}}_1 \cdots \tilde{\mathbf{b}}_n\right]$ is called the Gram-Schmidt orthogonalization of basis $\mathbf{B}$ where $\|\tilde{\mathbf{b}}_i\| \leq \|\mathbf{b}_i\|$.

* dual of a lattice is "the set of points whose inner products with the vectors in the lattice are integers"$\Lambda$: $\Lambda^\perp := \{\mathbf{w} \mid \langle \mathbf{w}, \Lambda \rangle \subset \mathbb{Z}\}$

* smoothing lemma

* Voronoi region The fundamental Voronoi region $\mathcal{V}$ is defined as

(2.16) $\mathcal{V} = \{\mathbf{x} \in \mathbb{R}^n \mid \forall \mathbf{y} \in \Lambda : \|\mathbf{x}\| \leq \|\mathbf{x} - \mathbf{y}\|\}$

* Linear Code [Van12] Let $\mathbb{F}_q^n$ be the $n$-dimensional vector space over the field $\mathbb{F}_q$. A $q$-ary linear code $C$ or $[n, k]$-code is a $k$-dimensional linear subspace of $\mathbb{F}_q^n$ such that

- $\mathbf{0} \in C$,
- if $\mathbf{x}, \mathbf{y} \in C$, then $\mathbf{x} + \mathbf{x} \in C$,
- and if $\mathbf{x} \in C$ and $\gamma \in \mathbb{F}_q$, then $\gamma\mathbf{x} \in C$.

There are $q^k$ different codewords in $C$.

Let $C$ be a $q$-ary linear $[n, k]$-code. The lattice over $C$ is defined as

(2.17) $\Lambda(C) = \{\mathbf{x} \in \mathbb{R}^n \mid \exists \mathbf{y} \in C : \mathbf{x} = \mathbf{y} \mod q\}$.

Similarly, for a lattice $\Lambda(\mathbf{B})$ a lattice code $C$ defined by $\Lambda(\mathbf{B})$ and a shaping region $\mathcal{V} \subset \mathbb{R}^n$ (e.g. the Voronoi region) is a subspace of $\mathbb{R}^n$ such that all codewords are lattice vectors in $\Lambda(\mathbf{B})$ within the region $\mathcal{V}$ [SFS08]:

(2.18) $C' = \{x \in \Lambda(\mathbf{B}) \mid x \in \mathcal{V}\}$ .

We define $\mathrm{dist}(\mathbf{t}, \Lambda(\mathbf{B}))$ where $\Lambda(\mathbf{B})) \subset \mathbb{R}^m$ as the distance of some vector $\mathbf{t} \in \mathbb{R}^m$ to the closest lattice vector $\mathbf{v} \in \Lambda(\mathbf{B})$, i.e.

(2.19) $\mathrm{dist}(\mathbf{t}, \Lambda(\mathbf{B})) = \min_{\mathbf{v} \in \Lambda(\mathbf{B})} \|\mathbf{t} - \mathbf{v}\|$.

- Lattice problems

* Minkowski theorem: Let $\Lambda$ be a lattice of dimension $n$, then $\lambda_1 \leq \sqrt{n} \cdot (\det \Lambda)^{\frac{1}{n}}$

* Lattice reduction: find short basis compared to $\lambda_1(\Lambda)$...

* SVP: given a basis $\mathbf{B}$ of lattice $\Lambda$ find shortest nonzero lattice vector => $v \in \Lambda$ s.t. $\|v\| = \lambda_1(\Lambda)$

* $\mathrm{SVP}_\gamma$: given a basis $\mathbf{B}$ of lattice $\Lambda$ find $v \in \Lambda$ s.t. $0 < \|v\| \leq \gamma\lambda_1(\Lambda)$

* $\alpha$-Approximate SVP: vector of length $\alpha\lambda_1$

* $\textsc{GapSVP}_\gamma$ (decision version of SVP): "given basis $\mathbf{B}$ of $n$-dimensional lattice $\Lambda$ with either $\lambda_1\Lambda \leq 1$ or $\lambda_1\Lambda \geq \gamma(n)$, decide which is the case"

* $\mathrm{CVP}_\gamma$: given basis $\mathbf{B}$ of $n$-dimensional lattice $\Lambda$ and target $\mathbf{t} \in \mathbb{R}^n$ find point in lattice that is close to $\mathbf{t}$ => find $\mathbf{v} \in \mathbb{R}^n$ with $\|\mathbf{t} - \mathbf{v}\| < \gamma \min_{\mathbf{v}' \in \Lambda} \|\mathbf{v}' - \mathbf{v}\|$

* SIVP (shortest independent vector problem): given basis $\mathbf{B}$ of $n$-dimensional lattice $\Lambda$, find $n$ linearly independent lattice vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \Lambda(\mathbf{B})$ such that $\max_i \|\mathbf{v}_i\|$ for $i \in \{1, \ldots, n\}$ is minimal

* $\mathrm{BDD}_\gamma$: given basis $\mathbf{B}$ of $n$-dimensional lattice $\Lambda$ and target $\mathbf{t} \in \mathbb{R}^n$ with $\mathrm{dist}(\mathbf{t}, \Lambda) < d)\lambda_1(\Lambda)/(2\gamma(n))$, find unique lattice vector $\mathbf{v} \in \Lambda$ such that $\|\mathbf{t} - \mathbf{v}\| < d$

* ideal lattice (do I need that?)

* ...?

* eher die Sachen für LWE/SIS als die Sachen für Algorithmen (analog Vorlesung), evtl.

Intuition für die anderen Sachen... Solving SVP with approximation factors: - 1 => NP-hard [Ajt98] - $\tilde{O}(n)$ => OWF [Ajt96; MR04] - $2^{n \log\log n / \log n}$ and $2^{n/2}$ in Poly-time [LLL82] => best known $2^k$-approx in $2^{\tilde{O}(n/k)}$ time (even quantum!)

### 2.2.3 distributions

- Gaussian, def, component-wise, trafo to bound

* definition: discrete Gaussian distribution over $q$-ary lattice $\Lambda$ with Gaussian width parameter $s > 0$ and center $\mathbf{c}$, denoted by $D_{\Lambda,s,\mathbf{c}}$: probability of sampling a vector $\mathbf{x} \in \Lambda$ is proportional to $e^{-\pi \|\mathbf{x}-\mathbf{c}\|^2/s^2}$ In order to avoid confusion, throughout this work and in the *Lattice Parameter Estimation* we use $\sigma$ to denote the standard deviation, where $\sigma = \frac{s}{\sqrt{2\pi}}$, and define $\alpha := \frac{s}{q} = \frac{\sqrt{2\pi}\sigma}{q}$.

* better definition in GPV08 => different definition needed for LWE??? * how to do this? => variant of Babai's "nearest-plane" algorithm, see [GPV08]

* component-wise

For some applications, we receive a Gaussian distribution as input, but require a bound in some norm in order to estimate the hardness of SIS. Hence, we need to transform the Gaussian width parameter into a bound $\beta$ given some security parameter sec. Note that a $n$-dimensional Gaussian can be sampled by sampling $n$ independent 1-dimensional Gaussians.

For a Gaussian distribution, the following holds:

$$\Pr\left[|X| \geq \beta\right] \leq 2e^{-\pi\beta^2/s^2} \tag{2.20}$$

We demand $2e^{-\pi\beta^2/s^2} \approx 2^{-sec}$, hence

$$\begin{aligned} 2e^{-\pi\beta^2/s^2} &\approx 2^{-sec} \\ -\pi\frac{\beta^2}{s^2} &\approx (-sec - 1)\ln(2) \\ \beta &\approx s\sqrt{\frac{(sec+1)\ln(2)}{\pi}} \end{aligned}$$

* smoothing factor here?

* Uniform (stuff I use in tool)

## 2.3 LWE and SIS

Applications: SIS can be used for one-way functions and collision-resistant hasing. LWE can be used to build pseudo-random number generators, public-key encryption schemes and oblivious transfer and secure MPC. Lattice Trapdoors (trapdoor functions, digital signatures)? Punctured Trapdoors (identity-based encryption, attribute-based encryption, predicate encryption)?

### 2.3.1 LWE

Following based on [Reg10]:

Introduced by Regev in [Reg09] Origin: work of Ajtai and Dwork [AD97], first public-key cryptosystem based on worst-case lattice problems, simlifications/improvements [GGH97; Reg03] imply hardness result for LWE. Early work: hardness based on unique-SVP, Peikert [Pei09] and Lyubashevsky and Micciancio [LM09] show that unique-SVP is essentially equivalent to GapSVP.

- ´cryptomania´ applications: public-key encryption schemes under chosen-plaintext attacks [KTX07; PVW08; Reg05], and chosen-ciphertext attacks [Pei09; PW08], oblivious transfer protocoles [PVW08], identity-based encryption (IBE) schemes [ABB10; CHKP10; GPV08], leakage-resilient encryption [ACPS09; AGV09; DGK+10; GKPV10], and more

- most important: fully homomorphic encryption schemes [Bra12; BV11; Gen09; GSW13]

Intuition: "recover $\mathbf{s} \in \mathbb{Z}_q^n$ given sequence of ´approximate´ random linear equations on $\mathbf{s}$"

Formal Definition:

**Definition 2.3.1 (LWE Distribution [Reg10])**
*For $n \geq 1$, modulus $q \geq 2$, error distribution $\chi$ on $\mathbb{Z}_q$, and a fixed secret vector $\mathbf{s}$, let $\mathcal{A}_{\mathbf{s},\chi}$ be the probability distribution over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ by choosing a vector $\mathbf{a}_i \in \mathbb{Z}_q^n$ uniformly at random, $e_i \in \mathbb{Z}_q$ according to $\chi$ and returning pairs of $(\mathbf{a}_i, \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i \mod q) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$.*

Additions are performed in $\mathbb{Z}_q$. We say that an algorithm solves LWE with modulus $q$ and error distribution $\chi$ if, for any $\mathbf{s} \in \mathbb{Z}_q^n$, given an arbitrary number of independent samples from $\mathcal{A}_{\mathbf{s},\chi}$ it outputs $\mathbf{s}$ (with high probability). For $q = 2$ corresponds to *learning parity with noise* (LPN) problem.

**Definition 2.3.2 (Search-LWE$_{n,q,m,\chi}$)**
*Search-LWE$_{n,q,m,\chi}$ asks for the recovery of the secret vector $\mathbf{s}$ given $m$ independent samples $(\mathbf{a}_i, z_i) \leftarrow \mathcal{A}_{\mathbf{s},\chi}$*

**Definition 2.3.3 (Decision-LWE$_{n,q,m,\chi}$)**
*Given $m$ samples, Search-LWE$_{n,q,m,\chi}$ asks to distinguish whether the samples were drawn from $\mathcal{A}_{\mathbf{s},\chi}$ or from a uniform distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$.*

#### LWE as a Decoding Problem

We request $m$ samples $(\mathbf{a}_1, z_1), \ldots, (\mathbf{a}_m, z_m)$ where $z_i = \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i \in \mathbb{Z}_q$. Let $A = [\mathbf{a}_1 \cdots \mathbf{a}_m]$, $\mathbf{z} = [z_1, \ldots, z_m]^\top$ and $e = [e_1, \ldots, e_n]^\top$. Hence, we can reformulate LWE as a decoding problem as in [GJS15]:

(2.21) $\mathbf{z} = \mathbf{A}^\top \mathbf{s} + \mathbf{e}$

with generator matrix $\mathbf{A}$ for a linear code over $\mathbb{Z}_q$ and $\mathbf{z}$ as the received word. Finding the secret vector $\mathbf{z}$ is equivalent to finding the codeword $\mathbf{y} = \mathbf{A}^\top \mathbf{s}$ with minimum distance $\|\mathbf{y} - \mathbf{z}\|$.

An $\mathrm{LWE}_{n,q,m,\chi}$ instance with a secret vector $\mathbf{s}$ chosen according to a uniform distribution can be transformed into an $\mathrm{LWE}_{n,q,m-n,\chi}$ instance with a secret vector $\hat{\mathbf{s}}$ chosen according to the error distribution $\chi$ at a loss of $n$ samples as follows: Let $\mathbf{A}_0 = [\mathbf{a}_1 \cdots \mathbf{a}_n]$ where $\mathbf{a}_1, \ldots, \mathbf{a}_n$ are the first $n$ columns of $\mathbf{A}$. We introduce new variables $\hat{\mathbf{s}} = \mathbf{A}_0^\top \mathbf{s} - [z_1, \ldots, z_n]^\top = [e_0, \ldots, e_n]^\top$ and $\hat{\mathbf{A}} = \mathbf{A}_0^{-1}\mathbf{A} = [\mathbf{I}\ \hat{\mathbf{a}}_{n+1} \cdots \hat{\mathbf{a}}_m]$ and compute $\hat{\mathbf{z}} = \mathbf{z} - \hat{\mathbf{A}}^\top [z_1, \ldots, z_n]^\top = [\mathbf{0}, \hat{z}_{n+1} \cdots \hat{z}_m]^\top$.

#### LWE as a BDD Problem

Solving LWE also corresponds to solving the *Bounded Distance Decoding problem* (BDD) in the lattice $\Lambda(\mathbf{A}^\top) = \{\mathbf{x} \in \mathbb{Z}_q^m \mid \exists \mathbf{s} \in \mathbb{Z}_q^n : \mathbf{x} = \mathbf{A}^\top \mathbf{s} \mod q\}$, where the $m$ columns of $\mathbf{A}$ correspond to the vectors $\mathbf{a}_i \in \mathbb{Z}_q^n$ of $m$ independent LWE samples $(\mathbf{a}_i, z_i) \leftarrow \mathcal{A}_{\mathbf{s},\chi}$ and the components $z_i$ correspond to a perturbed lattice point in $\Lambda(\mathbf{A}^\top)$.

Best algorithm to solve LWE: Blum, Kalai, and Wasserman [BKW03] with $2^{O(n)}$ samples and time.

Hardness: best algorithm exponential, extension of LPN (LPN believed to be hard), hard assuming worst-case hardness of GapSVP and SIVP [Pei09; Reg05]. More details? Different cases for $q$ exponential/polynomial, approximation factors... Hardness based on worst-case lattice problems => strong security guarantees, such as conjectured security against quantum computers...

Search to decision reduction => distiguishing is LWE samples from uniform samples sufficient, worst-case to average-case reduction => sufficient to solve distinguishing for uniform secret

### 2.3.2 Short Integer Solution (SIS)

The dual problem to LWE is the *Short Integer Solution problem* (SIS).

- principle: given a set of set of uniformly random vectors $\mathbf{a}_1, \ldots, \mathbf{a}_m \in \mathbb{Z}_q^n$ find a subset of them or combination with small coefficients that sums to zero (modulo $q$).

- introduced in [MR04], origins in [Ajt96], used for ´minicrypt´ primitives: one-way functions [Ajt96], collision resistant hash functions [GGH96], digital signature schemes [CHKP10; GPV08], and identification schemes [KTX07; Lyu08; MV03]

**Definition 2.3.4 (SIS Problem (Adapted from [[LS15], Definition 3.1)**
*)] The problem $\mathit{SIS}_{n,q,m,\beta}$ is defined as follows: Given a uniformly random matrix $\mathbf{A}^{n\times m}$, find a vector $\mathbf{s} \in \mathbb{Z}_q^m$ such that $\mathbf{A} \cdot \mathbf{s} = 0$ mod $q$ and $0 < \|\mathbf{s}\| \leq \beta$.*

Finding such a vector corresponds to finding a short lattice vector in costets of the lattice $\Lambda^\perp(\mathbf{A}) = \{y \mid \mathbf{A} \cdot y \mod q\}$

Hardness: for any poly-bounded $m, \beta$ and for "large enough" prime $q$: $\mathrm{SIS}_{n,q,m,\beta}$ is as hard as worst-case approx-SIVP (and GapSVP) to within $\beta \cdot \tilde{O}(\sqrt{n})$ factor

### 2.3.3 Ring and Module Variants

- problem key sizes in LWE/SIS in $O(n^2)$ (matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$), where $m \in \Omega(n)$)

- idea: introduce some sort of a structure in samples: $n$ power of two, $\mathbf{a}$ vectors in groups of size $n$, for each group $\mathbf{a}_1 = [a_1, \ldots, a_n]^\top$, $a_i$ are uniformly random in $\mathbb{Z}_q$, and $\mathbf{a}_i = [a_i, \ldots, a_n, -a_1, \ldots, -a_{i-1}]^\top$. Hence, $n$ vectors only need $O(n)$ memory, also speedups in operations by using FFT

- formally: vectors are elements of the ring $\mathbb{Z}_q\,[x]\,/\langle x^n + 1\rangle$ which we call $\mathcal{R}_q$ instead of the group $\mathbb{Z}_q^n$, $n$ power of two ensures that $x^n + 1$ is irreducible over the rationals

- add more?

**Definition 2.3.5 (Ring-SIS Problem [[LS15], Definition 3.3)**
*)] The problem $RSIS_{n,q,m,\beta}$ is defined as follows: Given $a_1, \ldots, a_n \in \mathcal{R}_q$ chosen independently from the uniform distribution, find $s_1, \ldots, s_n \in \mathcal{R}$ such that $\sum_{i=1}^m a_i \cdot s_i = 0 \mod q$ and $0 < \|\mathbf{s}\| \leq \beta$, where $\mathbf{s} = [s_1, \ldots, s_m]^\top \in \mathcal{R}^m$.*

**Definition 2.3.6 (Module-SIS Problem [[LS15], Definition 3.3)**
*)] The problem $MSIS_{n,d,q,m,\beta}$ is defined as follows: Given $a_1, \ldots, a_n \in \mathcal{R}_q^d$ chosen independently from the uniform distribution, find $s_1, \ldots, s_n \in \mathcal{R}$ such that $\sum_{i=1}^m a_i \cdot s_i = 0 \mod q$ and $0 < \|\mathbf{s}\| \leq \beta$, where $\mathbf{s} = [s_1, \ldots, s_m]^\top \in \mathcal{R}^m$.*

While there exist special cases where the Ring structure of problem instances can be exploited in an attack on LWE or SIS, in general, the hardness of Ring and Module variants is estimated by interpreting the coefficients of elements of $\mathcal{R}_q$ as vectors in $\mathbb{Z}_q^n$ [ACD+18]. We thus reduce Ring and Module instances as follows:

- $\mathrm{RLWE}_{n,q,m,\chi} \longrightarrow \mathrm{LWE}_{n,q,m\cdot n,\chi}$
- $\mathrm{MLWE}_{n,d,q,m,\chi} \longrightarrow \mathrm{LWE}_{n\cdot d,q,m\cdot n,\chi}$
- $\mathrm{RSIS}_{n,q,m,\beta} \longrightarrow \mathrm{SIS}_{n,q,m\cdot n,\beta}$
- $\mathrm{MSIS}_{n,d,q,m,\beta} \longrightarrow \mathrm{SIS}_{n\cdot d,q,m\cdot n,\beta}$

Note that in the Ring and Module variants $n$ denotes the degree of the polnomial of the underlying Ring, while in the standard variant, $n$ denotes the dimension of the secret.

# 3 Algorithms and Estimates

## 3.1 Lattice Basis Reduction

- measure quality of basis: Hermite factor

* basis $\mathbf{B} = \{\mathbf{b}_1, \dots, \mathbf{b}_m\}$, $m$-dimensional lattice $\Lambda(\mathbf{B})$ has Hermite factor $\delta$ if

(3.1) $\|\mathbf{b}_1\| \approx \delta^m \det(\Lambda)^{1/m}$

* use Geometric Series Assumption (GSA) to obtain estimates for $\mathbf{b}_i$:

(3.2) $\|\tilde{\mathbf{b}}_i\| \approx \alpha^{i-1} \|\mathbf{b}_1\|$

for $0 < \alpha < 1$ Equation (3.1) into Equation (3.2) -> $\|\tilde{\mathbf{b}}_i\| \approx \alpha^{i-1}\delta^m \det(\Lambda)^{1/m}$ with $\prod_{i-1}^{m} \|\tilde{\mathbf{b}}_i\| = \det(\Lambda)$ we get

$$
\begin{aligned}
& & \prod_{i-1}^{m} \|\tilde{\mathbf{b}}_i\| &\approx \prod_{i-1}^{m} \alpha^{i-1}\delta^m \det(\Lambda)^{1/m} \\
\Leftrightarrow & & \det(\Lambda) &\approx \delta^{2m} \det(\Lambda) \prod_{i-1}^{m} \alpha^{i-1} \\
\Leftrightarrow & & \delta^{-m^2} &\approx \alpha^{\frac{m(m-1)}{2}} \\
\Leftrightarrow & & \delta^{-2} &\approx \alpha^{(m-1)/m}
\end{aligned}
$$

Hence, $alpha \approx \delta^{-2}$ and

(3.3) $\|\tilde{\mathbf{b}}_i\| \approx \delta^{-2(i-1)+m} \det(\Lambda)^{1/m}$

* good basis -> first Gram-Schmidt vectors become shorter (latter longer)

* $\delta = 1.01$ feasible, $\delta = 1.007$ seems infeasible for now

* gap between provable and experimental cost estimate to reach some hermite $\delta$ => provable results only give upper bounds, for practical security we need lower bound => combine theoretical results with experimental results

* well-established estimate [LP11]

### 3.1.1 Cost Models for Lattice Reduction

Just insert a table and reference somewhere else? Warum notwendig, wie kommt man darauf? ... alg laufen lassen, extrapolieren...

## 3.2 LWE

### 3.2.1 Approaches

Distinguishing attacks (MR09, RS10): distinguish (with noticeable advantage) LWE instance from uniformly random => break semantic security of LWE-based cryptosystem with same advantage (typically), find short nonzero integral vector $\mathbf{v}$ s.t. $\mathbf{A}^{\intercal}\mathbf{v} = 0 \mod q$ => short vector in (scaled) dual of LWE lattice $\Lambda(\mathbf{A})$ then test whether $\langle \mathbf{v}, z \rangle$ is close to zero mod q. If uniform test accepts with prob 1/2, if LWE with parameter s, $\langle \mathbf{v}, \mathbf{z} \rangle = \langle \mathbf{v}, \mathbf{e} \rangle \mod q$, Gaussian mod q with parameter $\|\mathbf{v}\| \cdot s$. If that's not much larger than q, advantage for distinguishing very close to $\exp(-\pi(\|\mathbf{v}\|s/q)^2)$. high confidence needs $\|\mathbf{v}\| \le q/(2s)$ advantage an computational effort need to be balanced (often inverse distinguising advantage is in total cost of attack)

#### SIS

rewrite LWE as the problem of finding short vector in dual lattice => SIS

#### BDD

lattice reduction algorithms solve SIS and BDD

#### Direct

- algebraic approach Arora and Ge with subexponential complexity when $\sigma \le \sqrt{n}$, else fully exponential, mainly of asymptotic interest (higher complexity than others)

- combinatorial algorithms: BKW as basis [BKW03], resembles generalized birthday approach by Wagner, originally for solving LPN, can be analyzed => explicit complexity for different LWE instances, theoretical analysis and actual performance close, very memory expensive (often same order as time complexity)

### 3.2.2 Algorithms in Estimator

#### BKW [BKW03]

- BKW by Blum, Kalai and Wasserman [BKW03] to solve Learning Parity with Noise problem (LPN), subproblem of LWE - applied to LWE in [ACF+15] (original paper appeared in 2013) - time and space complexity $2^{O(n)}$ for LWE with prime modulus $q \in \mathrm{poly}(n)$ - Various improvements have been suggested since. For example, [AFFP14] and [KF15] use modulus switching for binary-LWE and other small secret variants [AFFP14] and [DTV15] applies multidimensional Furier transformations.

modified BKW step -> coded-BKW step to cancel out more positions in the **a** vectors than traditional BKW step

map part of **a** vector into nearest codeword in lattice code (linear code over $\mathcal{Z}_q$, Euclidean distance)

introduces some noise, can be kept small by appropriate parameters

pair of **a** vectors map to same codeword => add together to create new sample with part of **a** vector cancelled

samples are input to next step in BKW procedure

additional steps using discrete FFT

slightly modified for BINARY-LWE (secret vector uniformly chosen from $\{0, 1\}^n$) greatly increases performance

In the following, we present an outline of the original BKW algorithm. The steps in Algorithm 1 are inspired by the textual description in [GJS15] with minor adjustments in notation.

For the algorithm, we use the matrix notation of LWE as in Equation (2.21), i.e. $\mathbf{z} = \mathbf{A}^\intercal \mathbf{s} + \mathbf{e}$. BKW consists of a series of BKW steps that iteratively reduce the dimension of input matrix $\mathbf{A}$ by finding collisions of its column vectors in the currently examined block of $b$ entries. We start from the last $b$ entries of $\mathbf{A}^{(1)} = \mathbf{A}$. In every step $i$, we maintain a collision table $\mathbf{T}^{(i)}$ and loop over the columns $\mathbf{a}_k^{(i)}$ of $\mathbf{A}^{(i)}$ and distinguish between the following cases: (1) If $\mathbf{a}_k^{(i)}$ only has zero entries in the examined block, pass $\mathbf{a}_k^{(i)}$ and $z_k^{(i)}$ to the next step, (2) if no match of $\mathbf{a}_k^{(i)}$ or the negation of $\mathbf{a}_k^{(i)}$ can be found in the collision table, add $\mathbf{a}_k^{(i)}$ to the colission table, and (3) if a match $\mathbf{a}_l^{(i)}$ is found, compute $\mathbf{a}_l^{(i)} + \mathbf{a}_k^{(i)}$ or in the case of a negation match $\mathbf{a}_l^{(i)} - \mathbf{a}_k^{(i)}$ (in $\mathbb{Z}_q$) such that the last $b$ nonzero entries cancel out. By exploiting the symmetry of $\mathbb{Z}_q$ in this way, in every step we obtain at most $(q^b - 1)/2$ columns with distinct coefficients in the current $b$ entries. We also make note of "observed symbols" $z_j^{(i)}$ that represent the combination of two samples given their respective matching columns (see lines 20, 24 for more details).

In each BKW step, the number of columns (and samples) decreases by at least $(q^b - 1)/2$ (size of the colusion set) and the variance of the error distribution $\sigma^2$ increases by a factor of two. Once the number of remaining nonzero rows of $\mathbf{A}$ is small enough, the remaining part of the secret vector $\mathbf{s}$ is guessed. A hypothesis test ensures that the remaining samples follow a Gaussian with noise $2^t \cdot \sigma^2$, where $t$ is the number of steps. Finally, back substitution is applied to obtain the complete secret vector $\mathbf{s}$.

**Algorithm 1:** BKW

**function** BKW($\mathbf{A}, \mathbf{z}, t$)
    $i = 1$
    $\mathbf{A}^{(i)} = \mathbf{A}$
    $\mathbf{z}^{(i)} = \mathbf{z}$
    **while** *the last $t$ coefficients of the columns of* $\mathbf{A}^{(i)}$ *are nonzero* **do**
        // BKW step
        $j = 1$
        $\mathbf{T}^{(i)} = []$ // Collision table
        **for** $k = 1, \ldots, m^{(i)}$ **do**
            // $m^{(i)}$ is number of columns in $\mathbf{A}^{(i)}$
            **if** *last* $(i \cdot b)$ *coefficients of* $\mathbf{a}_k^{(i)}$ *are zero* **then**
                $\mathbf{a}_j^{(i+1)} = \mathbf{a}_k^{(i)}$
                $z_j^{(i+1)} = z_k$
                $j = j + 1$
            **else if** *no match for* $\mathbf{a}_k^{(i)}$ *in* $\mathbf{T}$ **then**
                $\mathbf{T} = \mathbf{T} + \left[\mathbf{a}_k^{(i)}\right]$ // append to collision set
            **else if** *match* $\mathbf{a}_l^{(i)}$ *for* $\mathbf{a}_k^{(i)}$ *is found* **then**
                **if** $\mathbf{a}_l^{(i)}$ *matches* $\mathbf{a}_k^{(i)}$ *in the last* $(i \cdot b)$ *components* **then**
                    $\mathbf{a}_j^{(i+1)} = \mathbf{a}_k^{(i)} - \mathbf{a}_l^{(i)}$; // last $i \cdot b$ coefficients of $\mathbf{a}_j^{(i+1)}$ are now zero
                    $z_j^{(i+1)} = z_k^{(i)} - z_l^{(i)} = y_j^{(i)} + e_j^{(i)}$, where $y_j^{(i)} = \left\langle \mathbf{s}, \mathbf{a}_j^{(i)} \right\rangle$ and $e_j^{(i)} = e_k^{(i)} - e_l^{(i)}$
                    $j = j + 1$
                **else if** *the negation of* $\mathbf{a}_l^{(i)}$ *in* $\mathbb{Z}_q^n$ *matches* $\mathbf{a}_k^{(i)}$ *in the last* $(i \cdot b)$ *components* **then**
                    $\mathbf{a}_j^{(i+1)} = \mathbf{a}_k^{(i)} + \mathbf{a}_l^{(i)}$
                    $z_j^{(i+1)} = z_k^{(i)} + z_l^{(i)} = y_j^{(i)} + e_j^{(i)}$, where $y_j^{(i)} = \left\langle \mathbf{s}, \mathbf{a}_j^{(i)} \right\rangle$ and $e_j^{(i)} = e_k^{(i)} + e_l^{(i)}$
                    $j = j + 1$
        $i = i + 1$
        // Calculate input for next BKW step
        $\mathbf{A}^{(i)} = (\mathbf{a}_1^{(i)} \cdots \mathbf{a}_{j-1}^{(i)})$
        $\mathbf{z} = (z_1^{(i)}, \ldots, z_{j-1}^{(i)})$

#### Coded-BKW [GJS15]

- change BKW step -> more column entries are removed, but additional noise - index set $I$, $\mathbf{x}_I$ is part of $\mathbf{x}$ with entries indexed by $I$ - step $i$: $I$ set of $b$ positions to be removed, fix some $q$-ary linear $[N_i, b]$ code $C_i$ with $q^b$ codewords, find the closest codeword $\mathbf{c}_I \in C$ for every input vector $\mathbf{a}_I$ such that $\mathbf{a}_I = \mathbf{c}_I + \mathbf{e}_I$, where the error part $\mathbf{e}_I \in \mathbb{Z}_q^{N_i}$ is minimized by a decoding procedure.

Finally, we subtract two vectors and their correpsonding samples and pass the result to the next BKW step. Consider the inner product$\langle \mathbf{s}_I, \mathbf{a}_I \rangle = \langle \mathbf{s}_I, \mathbf{c}_I \rangle + \langle \mathbf{s}_I, \mathbf{e}_I \rangle$. In the subtraction, only the error part $\langle \mathbf{s}_I, \mathbf{e}_I \rangle$ remains.

#### Dual Attack [MicReg09]

"Gama and Nguyen [GN08]: (in)feasibility of obtaining various Hermite factors natural distinguishing attack on LWE by finding one relatively short vector in associated lattice"

#### Decoding Attack [LinPei11]

combines lattice basis reduction followed by an enumeration algorithm (bounded-distance decoding with preprocessing?) => time/success tradeoff specifically for LWE, exploits structural properties of LWE on search version of LWE problem, approach preferable to distinguishing attack on decision LWE in [MR09; RS10], same or better advantage than distinguishing attack using lattice vectors of lower quality => runtime is smaller post-reduction: simple extension of Babai's "nearest-plane" algorithm [Bab85] => trade basis quality against decoding time related to Klein's (de)randomized algorithm [Kle00] for bounded-distance decoding

use entire reduced basis, post-reduction part is fully parallelizable

Properties of a $\delta$-LLL Reduced Basis:

1. $|\mu_{i,j}| \leq \frac{1}{2}$ for $1 \leq i \leq n$ and $j < i$
2. $\delta \|\tilde{\mathbf{b}}_i\|^2 > \|\mu_{i+1,i}\tilde{\mathbf{b}}_i + \tilde{\mathbf{b}}_{i+1}\|^2$ for $1 \leq i < n$

LLL reduction to input Lattice, integer combination of basis vectors close to target (like inner loop in reduction step of LLL), seek vector in lattice close to target, finds output that is in fundamental parallelipiped $\mathcal{P}(\mathbf{B})$ Section 2.2.2 => if error vector not in $\mathcal{P}(\mathbf{B})$, secret is not restored => basis quality has to be sufficiently good

Output is a lattice vector $\mathbf{v} \in \Lambda(\mathbf{B})$ such that $\|\mathbf{v} - \mathbf{t}\| \leq 2^{n/2}\text{dist}(\mathbf{t}, \Lambda(\mathbf{B}))$

Goal: recover lattice vector relatively close to target vector Intuition: - project $\mathbf{t}$ to span$(\mathbf{B})$ - from $i = n, \ldots, 1$ find closest hyperplane $c_i\tilde{\mathbf{b}}_i + \text{span}(\mathbf{b}_1, \ldots, \mathbf{b}_i)$ to the projection, subtract $c_i\mathbf{b}_i$ from the projection and continue - output vector is $\sum_{i=1}^n c_i\mathbf{b}_i$ for every basis vector $\mathbf{b}_i$ find $c_i$ such that distance between target and hyperplane spanned by $\mathbf{b}_1, ..., \mathbf{b}_{i-1}$ and shifted by $c_i\tilde{\mathbf{b}}_i$ is minimal , subtract $c_i\mathbf{b}_i$ from target vector and continue for $i = n, \ldots, 1$. After the last iteration $\sum_{i=1}^n c_i\mathbf{b}_i$ is returned.

Application to LWE: $\mathbf{t} = \mathbf{A}^\top\mathbf{s} + \mathbf{e}$ => we get $\mathbf{v}$ where $\mathbf{t} - \mathbf{v} = \mathbf{e}$ is in fundamental parallelipiped of Gram-Schmidt basis

**Algorithm 2:** The $\delta$-LLL Algorithm

**function** $\delta$-LLL($\mathbf{B} \in \mathbb{Z}^{n \times n}$)
  Start: compute Gram-Schmidt orthogonalization $\tilde{\mathbf{B}}$
  Reduction Step:
  **for** $i = 2, \ldots, n$ **do**
    **for** $j = i - 1, \ldots, 1$ **do**
      $c_{i,j} = \text{round}(\langle \mathbf{b}_i, \hat{\mathbf{b}}_j \rangle / \langle \hat{\mathbf{b}}_j, \hat{\mathbf{b}}_j \rangle)$
      $\mathbf{b}_i = \mathbf{b}_i - c_{i,j} \mathbf{b}_j$
  Swap Step:
  **if** $\exists i$ such that $\delta \|\tilde{\mathbf{b}}_i\|^2 > \|\mu_{i+1,i} \tilde{\mathbf{b}}_i + \tilde{\mathbf{b}}_{i+1}\|^2$ **then**
    tmp $= \mathbf{b}_i$
    $\mathbf{b}_i = \mathbf{b}_{i+1}$
    $\mathbf{b}_{i+1} = \mathbf{b}_i$

**Algorithm 3:** Babai's Nearest Plane Algorithm [Bab85]

**function** NearestPlane($\mathbf{B} \in \mathbb{R}^{m \times n}, \mathbf{t} \in \mathbb{R}^m$)
  run $\delta$-LLL on basis $\mathbf{B}$ with $\delta = \frac{3}{4}$
  $\mathbf{b} = \mathbf{t}$
  **for** $i = n, \ldots, 1$ **do**
    $c_i = \text{round}(\langle \mathbf{b}, \tilde{\mathbf{b}}_i \rangle / \langle \tilde{\mathbf{b}}_i, \tilde{\mathbf{b}}_i \rangle)$ $\mathbf{b} = \mathbf{b} - c_i \mathbf{b}_i$
  output $\mathbf{t} - \mathbf{b}$

Generalized version by [LP11]: Problem: in reduced basis last Gram-Schmidt vectors of B short, first long => long and skinny parallelipiped, Gaussian e unlikely to be in it => incorrect answer from NearestPlane

=> generalized version admitting time/success tradeoff recurse on some $d_i \geq 1$ distinct planes in ith

**Algorithm 4:** Generalized Nearest Plane Algorithm [LP11]

**function** GeneralizedNearestPlane($\mathbf{B} \in \mathbb{R}^{m \times k}, \mathbf{t} \in \mathbb{R}^m, \mathbf{d} \in (\mathbb{Z}^+)^k$)
  **if** $k = 0$ **then**
    Return $\mathbf{0}$
  **else**
    Compute projection $\mathbf{v}$ of $\mathbf{t}$ onto span($\mathbf{B}$)
    Compute the $d_k$ distinct integers $c_1, \ldots, c_{d_k}$ closest to $\langle \mathbf{v}, \tilde{\mathbf{b}}_k \rangle / \langle \tilde{\mathbf{b}}_k, \tilde{\mathbf{b}}_k \rangle$)
    Return $\bigcup_{i \in \{1,\ldots,d_k\}} (c_i \cdot \mathbf{b}_k +$
     GeneralizedNearestPlane($\{\mathbf{b}_1, \ldots, \mathbf{b}_{k-1}\}, (d_1, \ldots, d_{k-1}), \mathbf{v} - c_i \cdot \mathbf{b}_k$))

Instead of choosing only the nearest plane in each iteration step, Algorithm 4 selects a variable amount $d_k$ of distinct planes in each step. As a consequence, the fundamental parallelipiped of the Gram-Schmidt basis is stretched in the direction of $\tilde{\mathbf{b}}_k$. The values of $\mathbf{d}$ should be chosen such that the covered area is approximately the same in each direction (i.e. by maximizing $\min_i(d_i \cdot \|\tilde{\mathbf{b}}_i\|)$). In particular this implies that the $d_k$ are larger for larger $k$ as the Gram-Schmidt vectors have a smaller length. Compared to Algorithm 3 the runtime increases by a factor $\prod_{i\in\{1,\dots,d_k\}} d_i$, however, the recursion step can be fully parallelized.

It should be evident that a lower quality of the reduced input basis can be compensated for by increasing the values of $\mathbf{d}$. Hence we can adjust the input parameters for the lattice reduction and Algorithm 4 to minimize the runtime given a fixed required success probability.

#### Primal-uSVP [ADPS16, BaiGal14]

BKZ: reduce lattice basis using SVP oracle in smaller dimension $b$, known that number of calls to oracle polynomial - enumeration algorithm as oracle: in super-exponential time - sieve algorithms as oracle: exponential time but so far slower in practice for accesible dimensions $b \approx 130$

primal attack: construct unique-SVP instance from LWE instance LWE instance $(\mathbf{A}, \mathbf{z} = \mathbf{A}^\intercal\mathbf{s} + \mathbf{e})$ construct lattice

$$\Lambda = \left\{\mathbf{x} \in \mathbb{Z}^{m+n+1} \mid (\mathbf{A}^\intercal | - \mathbf{I}_m | - \mathbf{b})\mathbf{x} = \mathbf{0} \mod q\right\} \tag{3.4}$$

lattice has dimension $d = m + n + 1$, volume $q^m$ and unique-SVP solution $\mathbf{v} = (\mathbf{s}, \mathbf{e}, 1)$

success condition: - geometric series assumption known to be optimistic from attacker's point of view => finds basis with Gram-Schmidt norms $\|mat\tilde{h}bfb_i\| = \delta^{d-2i-1} \cdot \mathrm{Vol}(\Lambda)^{1/d}$ and $\delta = ((\pi b)^{1/b} \cdot b/2\pi e)^{1/2(b-1)}$ unique short vector $\mathbf{v}$ is detected if projection of $\mathbf{v}$ onto span of last $b$ Gram-Schmidt vectors is shorter than $mat\tilde{h}bfb_{d-b}$, norm of projection is expected to be $\gamma\sqrt{b}$ => attack successful iff $\gamma\sqrt{b} \leq \delta^{d-2i-1} \cdot q^{m/d}$

LWE as inhomogeneous-SIS (ISIS)

$\gamma$-uSVP: given lattice $\Lambda$ such that $\lambda_2(\Lambda) > \gamma\lambda_1(\Lambda)$, find shortest nonzero vector in $\Lambda$ reduce BDD to uSVP Kannan's embedding technique [Kan87]: given lattice $\Lambda(\mathbf{A}^\intercal) = \{\mathbf{x} \in \mathbb{Z}_q^m \mid \exists \mathbf{s} \in \mathbb{Z}_q^n : \mathbf{x} = \mathbf{A}^\intercal\mathbf{s} \mod q\}$ Section 2.3.1 generated by rows of LWE instance Let $\mathbf{B}$ be a basis of the $q$-ary lattice $\Lambda(\mathbf{A}^\intercal)$ and $t = \mathrm{dist}(\mathbf{z}, \Lambda(\mathbf{A}^\intercal))$ be the embedding factor. embed $\Lambda(\mathbf{A}^\intercal)$ into $\Lambda(\tilde{\mathbf{B}})$ with $\gamma$-uSVP structure as follows:

$$\tilde{\mathbf{B}} = \begin{pmatrix} \mathbf{B} & \mathbf{0} \\ \mathbf{z} & t \end{pmatrix} \tag{3.5}$$

If $t < \frac{\lambda_1(\Lambda(\mathbf{A}^\intercal))}{2\gamma}$, then $\Lambda(\tilde{\mathbf{B}})$ contains a $\gamma$-unique shortest vector $\mathbf{z}' = (\mathbf{e}, -t)$ [LM09]. By recovering $\mathbf{e}$, BDD is solved.

#### Meet-in-the-Middle [AlbPlaSco15]

#### Arora-Ge [AroGe11,ACFP14]

## 3.3 SIS

### 3.3.1 Dual Attack

#### MR variant [MR09]

#### RS variant [RS10]

"concrete estimates of “symmetric bit security”, concrete runtime estimates for various Hermite factors in random $q$-ary lattices"permissive form of distiguishing attack in [MR09], adversarial advantage is about $2^{-72}$

### 3.3.2 Combinatorial Attack [MR09]

## 3.4 Tool

class for distributions... from section this modelling, problems, generic search... Überblick, wie verwendbar, automatische norm umwandlung, sonstige features

### 3.4.1 Runtime and Cost Comparison

defaults... schnellste, beste => effizient, etc. parallel... problem reductions...

# 4 Usage Examples

## 4.1 Two Problem Search

basiert auf [BDLOP18]

## 4.2 TODO: find other schemes to apply

# 5 Conclusion

# Bibliography


[ABB10] S. Agrawal, D. Boneh, X. Boyen. “Efficient Lattice (H)IBE in the Standard Model”. In: *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Monaco / French Riviera, May 30 - June 3, 2010. Proceedings*. Ed. by H. Gilbert. Vol. 6110. Lecture Notes in Computer Science. Springer, 2010, pp. 553–572. DOI: 10.1007/978-3-642-13190-5_28. URL: https://doi.org/10.1007/978-3-642-13190-5%5C_28 (cit. on pp. 19, 23).

[ACD+18] M. R. Albrecht, B. R. Curtis, A. Deo, A. Davidson, R. Player, E. W. Postlethwaite, F. Virdia, T. Wunderer. “Estimate All the {LWE, NTRU} Schemes!” In: *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*. Ed. by D. Catalano, R. D. Prisco. Vol. 11035. Lecture Notes in Computer Science. Springer, 2018, pp. 351–367. URL: %5Curl%7Bhttps://doi.org/10.1007/978-3-319-98113-0_19%7D (cit. on p. 25).

[ACF+15] M. R. Albrecht, C. Cid, J.-C. Faugère, R. Fitzpatrick, L. Perret. “On the complexity of the BKW algorithm on LWE”. In: *Des. Codes Cryptogr.* 74.2 (2015), pp. 325–354. URL: https://doi.org/10.1007/s10623-013-9864-x (cit. on p. 29).

[ACPS09] B. Applebaum, D. Cash, C. Peikert, A. Sahai. “Fast Cryptographic Primitives and Circular-Secure Encryption Based on Hard Learning Problems”. In: *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings*. Ed. by S. Halevi. Vol. 5677. Lecture Notes in Computer Science. Springer, 2009, pp. 595–618. DOI: 10.1007/978-3-642-03356-8_35. URL: https://doi.org/10.1007/978-3-642-03356-8%5C_35 (cit. on p. 23).

[AD97] M. Ajtai, C. Dwork. “A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence”. In: *Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing*. STOC ’97. El Paso, Texas, USA: Association for Computing Machinery, 1997, pp. 284–293. ISBN: 0897918886. URL: https://doi.org/10.1145/258533.258604 (cit. on pp. 19, 23).

[AFFP14] M. R. Albrecht, J.-C. Faugère, R. Fitzpatrick, L. Perret. “Lazy Modulus Switching for the BKW Algorithm on LWE”. In: *IACR Cryptol. ePrint Arch.* (2014), p. 19. URL: http://eprint.iacr.org/2014/019 (cit. on p. 29).

[AFG13] M. R. Albrecht, R. Fitzpatrick, F. Göpfert. “On the Efficacy of Solving LWE by Reduction to Unique-SVP”. In: *Information Security and Cryptology - ICISC 2013 - 16th International Conference, Seoul, Korea, November 27-29, 2013, Revised Selected Papers*. Ed. by H.-S. Lee, D.-G. Han. Vol. 8565. Lecture Notes in Computer Science. Springer, 2013, pp. 293–310. DOI: 10.1007/978-3-319-12160-4_18. URL: %5Curl%7Bhttps://doi.org/10.1007/978-3-319-12160-4_18%7D (cit. on p. 20).

[AGV09] A. Akavia, S. Goldwasser, V. Vaikuntanathan. "Simultaneous Hardcore Bits and Cryptography against Memory Attacks". In: *Theory of Cryptography, 6th Theory of Cryptography Conference, TCC 2009, San Francisco, CA, USA, March 15-17, 2009. Proceedings*. Ed. by O. Reingold. Vol. 5444. Lecture Notes in Computer Science. Springer, 2009, pp. 474–495. DOI: 10.1007/978-3-642-00457-5_28. URL: https://doi.org/10.1007/978-3-642-00457-5%5C_28 (cit. on p. 23).

[Ajt96] M. Ajtai. "Generating Hard Instances of Lattice Problems (Extended Abstract)". In: *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996*. Ed. by G. L. Miller. ACM, 1996, pp. 99–108. URL: https://doi.org/10.1145/237814.237838 (cit. on pp. 18, 21, 24).

[Ajt98] M. Ajtai. "The Shortest Vector Problem in $L_2$ is *NP*-hard for Randomized Reductions (Extended Abstract)". In: *Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing, Dallas, Texas, USA, May 23-26, 1998*. Ed. by J. S. Vitter. ACM, 1998, pp. 10–19. DOI: 10.1145/276698.276705. URL: https://doi.org/10.1145/276698.276705 (cit. on p. 21).

[Bab85] L. Babai. "On Lovász' Lattice Reduction and the Nearest Lattice Point Problem (Shortened Version)". In: *STACS 85, 2nd Symposium of Theoretical Aspects of Computer Science, Saarbrücken, Germany, January 3-5, 1985, Proceedings*. Ed. by K. Mehlhorn. Vol. 182. Lecture Notes in Computer Science. Springer, 1985, pp. 13–20. DOI: 10.1007/BFb0023990. URL: https://doi.org/10.1007/BFb0023990 (cit. on pp. 31, 32).

[BDL+18] C. Baum, I. Damgård, V. Lyubashevsky, S. Oechsner, C. Peikert. "More Efficient Commitments from Structured Lattice Assumptions". In: *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*. Ed. by D. Catalano, R. D. Prisco. Vol. 11035. Lecture Notes in Computer Science. Springer, 2018, pp. 368–385. URL: %5Curl%7Bhttps://doi.org/10.1007/978-3-319-98113-0_20%7D (cit. on pp. 17, 18).

[BKW03] A. Blum, A. Kalai, H. Wasserman. "Noise-tolerant learning, the parity problem, and the statistical query model". In: *J. ACM* 50.4 (2003), pp. 506–519. URL: https://doi.org/10.1145/792538.792543 (cit. on pp. 24, 28, 29).

[BLP+13] Z. Brakerski, A. Langlois, C. Peikert, O. Regev, D. Stehlé. "Classical hardness of learning with errors". In: *Symposium on Theory of Computing Conference, STOC'13, Palo Alto, CA, USA, June 1-4, 2013*. Ed. by D. Boneh, T. Roughgarden, J. Feigenbaum. ACM, 2013, pp. 575–584. URL: https://doi.org/10.1145/2488608.2488680 (cit. on p. 15).

[Bra12] Z. Brakerski. "Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP". In: *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*. Ed. by R. Safavi-Naini, R. Canetti. Vol. 7417. Lecture Notes in Computer Science. Springer, 2012, pp. 868–886. DOI: 10.1007/978-3-642-32009-5_50. URL: %5Curl%7Bhttps://doi.org/10.1007/978-3-642-32009-5_50%7D (cit. on p. 23).

[BV11] Z. Brakerski, V. Vaikuntanathan. "Efficient Fully Homomorphic Encryption from (Standard) LWE". In: *IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011, Palm Springs, CA, USA, October 22-25, 2011*. Ed. by R. Ostrovsky. IEEE Computer Society, 2011, pp. 97–106. URL: https://doi.org/10.1109/FOCS.2011.12 (cit. on p. 23).

[CHKP10] D. Cash, D. Hofheinz, E. Kiltz, C. Peikert. "Bonsai Trees, or How to Delegate a Lattice Basis". In: *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Monaco / French Riviera, May 30 - June 3, 2010. Proceedings*. Ed. by H. Gilbert. Vol. 6110. Lecture Notes in Computer Science. Springer, 2010, pp. 523–552. DOI: 10.1007/978-3-642-13190-5_27. URL: https://doi.org/10.1007/978-3-642-13190-5%5C_27 (cit. on pp. 19, 23, 24).

[DGK+10] Y. Dodis, S. Goldwasser, Y. T. Kalai, C. Peikert, V. Vaikuntanathan. "Public-Key Encryption Schemes with Auxiliary Inputs". In: *Theory of Cryptography, 7th Theory of Cryptography Conference, TCC 2010, Zurich, Switzerland, February 9-11, 2010. Proceedings*. Ed. by D. Micciancio. Vol. 5978. Lecture Notes in Computer Science. Springer, 2010, pp. 361–381. DOI: 10.1007/978-3-642-11799-2_22. URL: https://doi.org/10.1007/978-3-642-11799-2%5C_22 (cit. on p. 23).

[DPSZ12] I. Damgård, V. Pastro, N. P. Smart, S. Zakarias. "Multiparty Computation from Somewhat Homomorphic Encryption". In: *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*. Ed. by R. Safavi-Naini, R. Canetti. Vol. 7417. Lecture Notes in Computer Science. Springer, 2012, pp. 643–662. URL: %5Curl%7Bhttps://doi.org/10.1007/978-3-642-32009-5_38%7D (cit. on pp. 17, 18).

[DTV15] A. Duc, F. Tramèr, S. Vaudenay. "Better Algorithms for LWE and LWR". In: *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*. Ed. by E. Oswald, M. Fischlin. Vol. 9056. Lecture Notes in Computer Science. Springer, 2015, pp. 173–202. DOI: 10.1007/978-3-662-46800-5_8. URL: %5Curl%7Bhttps://doi.org/10.1007/978-3-662-46800-5_8%7D (cit. on p. 29).

[Gen09] C. Gentry. "A Fully Homomorphic Encryption Scheme". AAI3382729. PhD thesis. Stanford, CA, USA, 2009. ISBN: 9781109444506 (cit. on pp. 19, 23).

[GGH96] O. Goldreich, S. Goldwasser, S. Halevi. "Collision-Free Hashing from Lattice Problems". In: *Electron. Colloquium Comput. Complex.* 3.42 (1996). URL: https://eccc.weizmann.ac.il/eccc-reports/1996/TR96-042/index.html (cit. on p. 24).

[GGH97] O. Goldreich, S. Goldwasser, S. Halevi. "Eliminating Decryption Errors in the Ajtai-Dwork Cryptosystem". In: *Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings*. Ed. by B. S. K. Jr. Vol. 1294. Lecture Notes in Computer Science. Springer, 1997, pp. 105–111. DOI: 10.1007/BFb0052230. URL: https://doi.org/10.1007/BFb0052230 (cit. on p. 23).

[GJS15] Q. Guo, T. Johansson, P. Stankovski. “Coded-BKW: Solving LWE Using Lattice Codes”. In: *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I*. Ed. by R. Gennaro, M. Robshaw. Vol. 9215. Lecture Notes in Computer Science. Springer, 2015, pp. 23–42. URL: %5Curl%7Bhttps://doi.org/10.1007/978-3-662-47989-6_2%7D (cit. on pp. 23, 29, 31).

[GKPV10] S. Goldwasser, Y. T. Kalai, C. Peikert, V. Vaikuntanathan. “Robustness of the Learning with Errors Assumption”. In: *Innovations in Computer Science - ICS 2010, Tsinghua University, Beijing, China, January 5-7, 2010. Proceedings*. Ed. by A. C.-C. Yao. Tsinghua University Press, 2010, pp. 230–240. URL: http://conference.iiis.tsinghua.edu.cn/ICS2010/content/papers/19.html (cit. on p. 23).

[GN08] N. Gama, P. Q. Nguyen. “Predicting Lattice Reduction”. In: *Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings*. Ed. by N. P. Smart. Vol. 4965. Lecture Notes in Computer Science. Springer, 2008, pp. 31–51. URL: %5Curl%7Bhttps://doi.org/10.1007/978-3-540-78967-3_3%7D (cit. on p. 31).

[GPV08] C. Gentry, C. Peikert, V. Vaikuntanathan. “Trapdoors for hard lattices and new cryptographic constructions”. In: *Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008*. Ed. by C. Dwork. ACM, 2008, pp. 197–206. URL: https://doi.org/10.1145/1374376.1374407 (cit. on pp. 19, 22–24).

[GSW13] C. Gentry, A. Sahai, B. Waters. “Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based”. In: *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I*. Ed. by R. Canetti, J. A. Garay. Vol. 8042. Lecture Notes in Computer Science. Springer, 2013, pp. 75–92. DOI: 10.1007/978-3-642-40041-4_5. URL: %5Curl%7Bhttps://doi.org/10.1007/978-3-642-40041-4_5%7D (cit. on p. 23).

[HPS98] J. Hoffstein, J. Pipher, J. H. Silverman. “NTRU: A ring-based public key cryptosystem”. In: *Algorithmic Number Theory*. Ed. by J. P. Buhler. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998, pp. 267–288. ISBN: 978-3-540-69113-6 (cit. on p. 19).

[Kan87] R. Kannan. “Minkowski’s Convex Body Theorem and Integer Programming”. In: *Math. Oper. Res.* 12.3 (1987), pp. 415–440. DOI: 10.1287/moor.12.3.415. URL: https://doi.org/10.1287/moor.12.3.415 (cit. on p. 33).

[KF15] P. Kirchner, P.-A. Fouque. “An Improved BKW Algorithm for LWE with Applications to Cryptography and Lattices”. In: *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I*. Ed. by R. Gennaro, M. Robshaw. Vol. 9215. Lecture Notes in Computer Science. Springer, 2015, pp. 43–62. URL: %5Curl%7Bhttps://doi.org/10.1007/978-3-662-47989-6_3%7D (cit. on p. 29).

[Kle00] P. N. Klein. “Finding the closest lattice vector when it’s unusually close”. In: *Proceedings of the Eleventh Annual ACM-SIAM Symposium on Discrete Algorithms, January 9-11, 2000, San Francisco, CA, USA*. Ed. by D. B. Shmoys. ACM/SIAM, 2000, pp. 937–941. URL: http://dl.acm.org/citation.cfm?id=338219.338661 (cit. on p. 31).

[KTX07] A. Kawachi, K. Tanaka, K. Xagawa. “Multi-bit Cryptosystems Based on Lattice Problems”. In: *Public Key Cryptography - PKC 2007, 10th International Conference on Practice and Theory in Public-Key Cryptography, Beijing, China, April 16-20, 2007, Proceedings*. Ed. by T. Okamoto, X. Wang. Vol. 4450. Lecture Notes in Computer Science. Springer, 2007, pp. 315–329. DOI: 10.1007/978-3-540-71677-8_21. URL: https://doi.org/10.1007/978-3-540-71677-8%5C_21 (cit. on pp. 23, 24).

[LLL82] A. Lenstra, H. Lenstra, L. Lovász. “Factoring Polynomials with Rational Coefficients”. In: *Mathematische Annalen* 261 (Dec. 1982). URL: %5Curl%7Bhttps://doi.org/10.1007/BF01457454%7D (cit. on p. 21).

[LM09] V. Lyubashevsky, D. Micciancio. “On Bounded Distance Decoding, Unique Shortest Vectors, and the Minimum Distance Problem”. In: *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings*. Ed. by S. Halevi. Vol. 5677. Lecture Notes in Computer Science. Springer, 2009, pp. 577–594. DOI: 10.1007/978-3-642-03356-8_34. URL: %5Curl%7Bhttps://doi.org/10.1007/978-3-642-03356-8%5C_34%7D (cit. on pp. 23, 33).

[LP11] R. Lindner, C. Peikert. “Better Key Sizes (and Attacks) for LWE-Based Encryption”. In: *Topics in Cryptology - CT-RSA 2011 - The Cryptographers’ Track at the RSA Conference 2011, San Francisco, CA, USA, February 14-18, 2011. Proceedings*. Ed. by A. Kiayias. Vol. 6558. Lecture Notes in Computer Science. Springer, 2011, pp. 319–339. URL: %5Curl%7Bhttps://doi.org/10.1007/978-3-642-19074-2_21%7D (cit. on pp. 27, 32).

[LS15] A. Langlois, D. Stehlé. “Worst-case to average-case reductions for module lattices”. In: *Des. Codes Cryptogr.* 75.3 (2015), pp. 565–599. URL: https://doi.org/10.1007/s10623-014-9938-4 (cit. on pp. 24, 25).

[Lyu08] V. Lyubashevsky. “Lattice-Based Identification Schemes Secure Under Active Attacks”. In: *Public Key Cryptography - PKC 2008, 11th International Workshop on Practice and Theory in Public-Key Cryptography, Barcelona, Spain, March 9-12, 2008. Proceedings*. Ed. by R. Cramer. Vol. 4939. Lecture Notes in Computer Science. Springer, 2008, pp. 162–179. DOI: 10.1007/978-3-540-78440-1_10. URL: https://doi.org/10.1007/978-3-540-78440-1%5C_10 (cit. on p. 24).

[MP13] D. Micciancio, C. Peikert. “Hardness of SIS and LWE with Small Parameters”. In: *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I*. Ed. by R. Canetti, J. A. Garay. Vol. 8042. Lecture Notes in Computer Science. Springer, 2013, pp. 21–39. URL: %5Curl%7Bhttps://doi.org/10.1007/978-3-642-40041-4_2%7D (cit. on p. 15).

[MR04] D. Micciancio, O. Regev. “Worst-Case to Average-Case Reductions Based on Gaussian Measures”. In: *45th Symposium on Foundations of Computer Science (FOCS 2004), 17-19 October 2004, Rome, Italy, Proceedings*. IEEE Computer Society, 2004, pp. 372–381. URL: https://doi.org/10.1109/FOCS.2004.72 (cit. on pp. 21, 24).

[MR09] D. Micciancio, O. Regev. “Lattice-based Cryptography”. In: *Post-Quantum Cryptography*. Ed. by D. J. Bernstein, J. Buchmann, E. Dahmen. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 147–191. ISBN: 978-3-540-88702-7. URL: https://doi.org/10.1007/978-3-540-88702-7_5 (cit. on pp. 31, 34).

[MV03] D. Micciancio, S. P. Vadhan. “Statistical Zero-Knowledge Proofs with Efficient Provers: Lattice Problems and More”. In: *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*. Ed. by D. Boneh. Vol. 2729. Lecture Notes in Computer Science. Springer, 2003, pp. 282–298. DOI: 10.1007/978-3-540-45146-4_17. URL: https://doi.org/10.1007/978-3-540-45146-4%5C_17 (cit. on p. 24).

[Pei09] C. Peikert. “Public-key cryptosystems from the worst-case shortest vector problem: extended abstract”. In: *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, May 31 - June 2, 2009*. Ed. by M. Mitzenmacher. ACM, 2009, pp. 333–342. URL: https://doi.org/10.1145/1536414.1536461 (cit. on pp. 19, 23, 24).

[PVW08] C. Peikert, V. Vaikuntanathan, B. Waters. “A Framework for Efficient and Composable Oblivious Transfer”. In: *Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings*. Ed. by D. A. Wagner. Vol. 5157. Lecture Notes in Computer Science. Springer, 2008, pp. 554–571. DOI: 10.1007/978-3-540-85174-5_31. URL: https://doi.org/10.1007/978-3-540-85174-5%5C_31 (cit. on p. 23).

[PW08] C. Peikert, B. Waters. “Lossy trapdoor functions and their applications”. In: *Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008*. Ed. by C. Dwork. ACM, 2008, pp. 187–196. DOI: 10.1145/1374376.1374406. URL: https://doi.org/10.1145/1374376.1374406 (cit. on pp. 19, 23).

[Reg03] O. Regev. “New lattice based cryptographic constructions”. In: *Proceedings of the 35th Annual ACM Symposium on Theory of Computing, June 9-11, 2003, San Diego, CA, USA*. Ed. by L. L. Larmore, M. X. Goemans. ACM, 2003, pp. 407–416. DOI: 10.1145/780542.780603. URL: https://doi.org/10.1145/780542.780603 (cit. on pp. 19, 23).

[Reg05] O. Regev. “On lattices, learning with errors, random linear codes, and cryptography”. In: *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*. Ed. by H. N. Gabow, R. Fagin. ACM, 2005, pp. 84–93. URL: https://doi.org/10.1145/1060590.1060603 (cit. on pp. 15, 19, 23, 24).

[Reg09] O. Regev. “On lattices, learning with errors, random linear codes, and cryptography”. In: *J. ACM* 56.6 (2009), 34:1–34:40. URL: http://doi.acm.org/10.1145/1568318.1568324 (cit. on p. 23).

[Reg10] O. Regev. “The Learning with Errors Problem (Invited Survey)”. In: *Proceedings of the 25th Annual IEEE Conference on Computational Complexity, CCC 2010, Cambridge, Massachusetts, USA, June 9-12, 2010*. IEEE Computer Society, 2010, pp. 191–204. URL: https://doi.org/10.1109/CCC.2010.26 (cit. on p. 23).

[RS10] M. Rückert, M. Schneider. "Estimating the Security of Lattice-based Cryptosystems". In: *IACR Cryptol. ePrint Arch.* 2010 (2010), p. 137. URL: http://eprint.iacr.org/2010/137 (cit. on p. 31).

[SFS08] N. Sommer, M. Feder, O. Shalvi. "Low-Density Lattice Codes". In: *IEEE Trans. Inf. Theory* 54.4 (2008), pp. 1561–1585. DOI: 10.1109/TIT.2008.917684. URL: https://doi.org/10.1109/TIT.2008.917684 (cit. on p. 21).

[Van12] J. H. Van Lint. *Introduction to coding theory*. Vol. 86. Springer Science & Business Media, 2012 (cit. on p. 20).

All links were last followed on October 1, 2021.

**Declaration**

I hereby declare that the work presented in this thesis is entirely my own and that I did not use any other sources and references than the listed ones. I have marked all direct or indirect statements from other sources contained therein as quotations. Neither this work nor significant parts of it were part of another examination procedure. I have not published this work in whole or in part before. The electronic copy is consistent with all submitted copies.

place, date, signature