

PROJECT PROMETHEUS
PRivacy preserving pOst-quantuM systEms
from advanced crypTograpHic mEchanisms
Using lattices



D3.2

Intermediate results on computational problems, cryptanalysis and basic tools

Contractual submission date
Month 24


Deliverable version
1.1

Actual submission date
December 2019

Main author
Pierre-Alain Fouque and Weiqiang Wen
(UR1)



<http://www.h2020prometheus.eu/>

 h2020prometheus

PROMETHEUS project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780701. The contents of this deliverable are the responsibility of the PROMETHEUS consortium, and do not necessarily reflect the official views of the European Union.

Document information

Grant agreement no.	780701
Project acronym	PROMETHEUS
Project full title	PRivacy preserving pOst-quantuM systEms from advanced crypTograpHic mEchanisms Using latticeS
Type of action	Research and Innovation Action (RIA)
Topic	H2020-DS-06-2017-Cybersecurity PPP: Cryptography
Project dates	1 st January 2018 (Month 1) / 31 st December 2021 (Month 48)
Duration	48 months
Project URL	http://www.h2020prometheus.eu/
EU Project Officer	Carmen IFRIM
Work package	WP3 – Computational problems, cryptanalysis and basic tools
Deliverable title	Intermediate results on computational problems, cryptanalysis and basic tools
Deliverable no.	D3.2
Deliverable version	1.1
Deliverable filename	PROMETHEUS-780701-WP3-D3.2.pdf
Nature of deliverable	Report
Dissemination level	Public
Number of pages	55
Responsible partner	UR1 (participant number 11)
Author	Pierre-Alain Fouque and Weiqiang Wen (UR1)

Abstract. This document will include all intermediate results obtained so far on lattice hard computational problems, cryptanalysis, lattice trapdoors and secure implementations against side-channel adversaries.

Keywords: Lattices, Cryptanalysis, implementation.

Signatures

Written by	Pierre-Alain Fouque and Weiqiang Wen	UR1	December 2019
Reviewed by	Thomas Ricosset	THA	15/12/2019
Reviewed by	Tim Güneysu	RUB	18/12/2019
Approved by	Benoît Libert as Project coordinator	ENSL	20/12/2019
Approved by	Sébastien Canard as Technical leader	ORA	20/12/2019

Partners

ENSL	ENS de Lyon
ORA	Orange SA
CWI	Centrum voor Wiskunde en Informatica
IDC	IDC Herzliya
RHUL	Royal Holloway, University of London
RUB	Ruhr-Universität Bochum
SCYTL	Scytl Secure Electronic Voting, S.A.
THA	Thales Communications & Security S.A.S.
TNO	Nederlandse organisatie voor Toegepast-Natuurwetenschappelijk Onderzoek
UPC	Universitat Politècnica de Catalunya · BarcelonaTech
UR1	Université de Rennes 1
WEI	Weizmann Institute of Science

Contents

Contents	IV
1 Introduction	1
1.1 Tasks in this work package and their impact	1
1.2 Publications in this work package	2
1.3 Organization of this report	2
2 Background	4
2.1 Lattices	4
2.2 Worst-case lattice problems	6
2.3 Average-case lattice problems	8
2.4 Quantum computations and quantum random oracle model	10
2.5 Lattice reduction	12
2.6 Basic cryptosystems	15
2.7 Side-channel attacks and countermeasures	17
3 TASK 3.1: Quantum assumptions and reductions	19
3.1 Review of the targets	19
3.2 Overview of current results	19
3.3 Current results on quantum assumptions	19
3.4 Current results on reductions	22
3.5 Conclusion	24
4 TASK 3.2: Algorithm design and implementation of lattice trapdoors	25
4.1 Review of the targets	25
4.2 Overview of current results	25
4.3 Current results on applying more efficient structures	25
4.4 Current results on Gaussian sampling	27
4.5 Conclusion	28
5 TASK 3.3: Classical and quantum cryptanalysis	30
5.1 Review of the targets	30
5.2 Overview of current results	30
5.3 Current results on quantum cryptanalysis	31
5.4 Current results on classical cryptanalysis	34
5.5 Current results on cryptanalysis of NIST candidates	37
5.6 Conclusion	38
6 TASK 3.4: Side-channel attacks	38
6.1 Review of the targets	39
6.2 Overview of current results	39
6.3 Current results on side-channel attacks	39
6.4 Current results on Countermeasures	43
6.5 Conclusion	44
7 Conclusion	45

List of Symbols

$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$	sets of natural, integer, rational, real numbers
\mathbb{Z}_q	the ring of integers modulo q
\mathbb{Z}^n	the set of integer vectors of dimension n
\mathbb{Z}_q^n	the set of integer vectors modulo q of dimension n
$\mathbb{Q}^n, \mathbb{R}^n$	vector-spaces of dimension n
$[n]$	the set $\{1, \dots, n\}$
\mathbf{x}	column vector
\mathbf{x}^\dagger	row vector
$\ \mathbf{x}\ $	Euclidean norm of vector \mathbf{x}
$\ \mathbf{x}\ _\infty$	ℓ_∞ -norm of \mathbf{x} : $\max_i x_i $
\mathbf{A}	matrix (composed from vectors, column-wise)
\mathbf{a}_i	i^{th} column of matrix \mathbf{A}
$\mathbf{0}$	all-zeros vector
\mathbf{I}_n	$n \times n$ identity matrix
$\log x$	$\ln x$, the natural logarithm with base e
$\mathcal{D}_{\mathbb{Z}, r, c}$	the Gaussian distribution over integers with center c and parameter r
$x \leftarrow D$	x is sampled from a probability distribution D
$x \leftarrow S$	x is uniformly sampled from set S (assuming S has finite measure)
ω_q	$\exp(2\pi i/q)$
$\text{Span}(\mathbf{W})$	span of column vectors of \mathbf{W}
\mathbf{W}^\perp	orthogonal complementation of $\text{Span}(\mathbf{W})$
$\#S$	cardinality of set S
$\text{GL}_n(\mathbb{Z})$	unimodular matrices of order n
$ \cdot\rangle$	bra-ket notation for quantum register

We use the Landau notations $\mathcal{O}(\cdot)$, $\Theta(\cdot)$, $\Omega(\cdot)$, $\omega(\cdot)$, $o(\cdot)$.

List of Tables

1	Current status of publications within this work package.	2
2	Concrete targets within TASK 3.1.	19
3	Current (intermediate) results on TASK 3.1.	20
4	Concrete targets within TASK 3.2.	25
5	Current (intermediate) results on TASK 3.2.	26
6	Concrete targets within TASK 3.3.	30
7	Current (intermediate) results on TASK 3.3.	31
8	Concrete targets within TASK 3.4.	39
9	Current (intermediate) results on TASK 3.4.	40

List of Figures

1	Impact example of each task in WP3.	2
2	Quantum circuit for accessing random oracle H with input $ x\rangle$	11
3	Relationships between variants of RLWE and PLWE.	23
4	Prior (left) and new (right) trade-offs for ideal approx-SVP in the same fields (with a pre-processing of cost $\exp(\tilde{O}(n))$).	34

1 Introduction

The objectives of work package 3 are to provide theoretical and practical foundations for work packages 4, 5 and 6. They are four-fold. At first, regarding lattice-based assumptions and reductions, it has to provide general techniques for proving security in quantum security models, to improve quantum reductions between lattice problems and to find better reductions between standard quantum problems. Secondly, on cryptanalysis, it aims at proposing quantum attacks for general and algebraic lattices, at widening the range of algorithms in FPLLL, exploring generalizations, combinations and optimisations of lattice attacks in practice and finally at obtaining precise prediction for levels of security and automatizing parameters selection. On lattice trapdoors, this work package is working on the way to lower numerical precision requirements to fit small architectures and to test practicality of the Fast-Fourier-Orthogonalisation approach, and explore generalizations. Finally, regarding side-channel attacks, it has to secure implementations with constant-time runtime, side-channel protection and fault-injection detection or prevention. In the following, we will present the tasks within this work package concretely in four parts and explain their impacts on other packages by giving an example. We will also summarize our results obtained so far.

1.1 Tasks in this work package and their impact

This deliverable will include all intermediate results we achieved so far within the four subtasks:

- **TASK 3.1:** Quantum assumptions and reductions;
- **TASK 3.2:** Algorithm design and implementation of lattice trapdoors;
- **TASK 3.3:** Classical and quantum cryptanalysis;
- **TASK 3.4:** Side-channel attacks and countermeasures.

As shown in Figure 1, the impacts of each subtask with other work packages can be summarized as follows.

- **Impact of TASK 3.1:** TASK 3.1 studies the relations between known hard problems and proposes new assumptions with better properties. It also investigates the quantum and classical security model. These results can be used to choose the appropriate underlying assumptions for designing schemes as well as security models for capturing the behavior of adversary in WP4 and 5.
- **Impact of TASK 3.2:** TASK 3.2 develops efficient algebraic structures for building cryptographic schemes. It also provides efficient solutions for implementing them. These results can be used to design efficient basic algorithms and building blocks in WP4 and privacy-preserving protocols in WP5.
- **Impact of TASK 3.3:** TASK 3.3 improves the state-of-the-art attacks on problems over Euclidean lattices and structured lattices under classical and quantum computation to provide more trustworthy parameters. In this subtask, we also cryptanalyze some NIST (National Institute of Standards and Technology) PQC (Post-Quantum Cryptography) candidates and eventually give valuable suggestions for deriving secure implementations, which is in particular related to WP2 about project's dissemination. These results can be used to build the

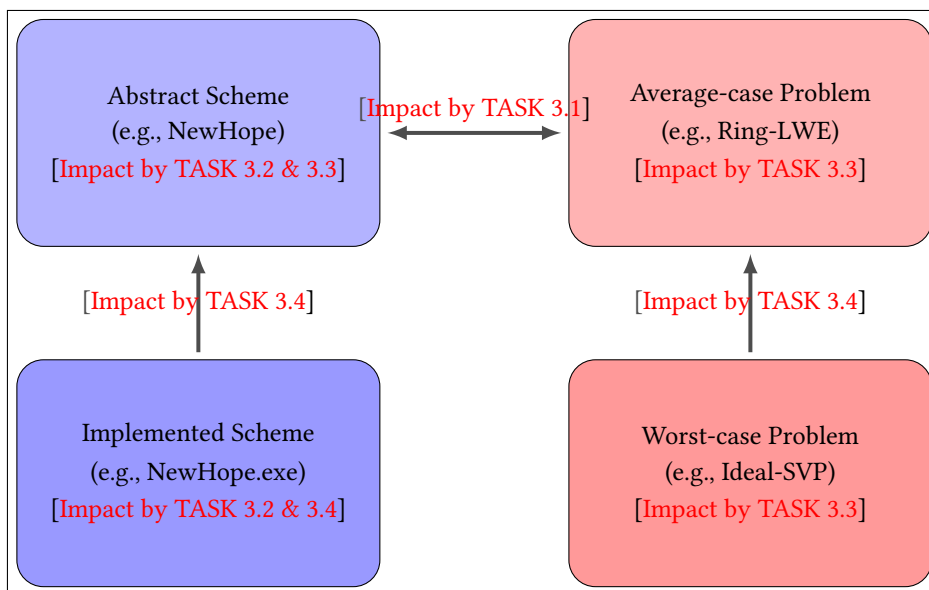


Figure 1: Impact of each task in WP3.

automated tools provided by WP4 and 5 for generating parameters targeting a given security level.

- **Impact of TASK 3.4:** TASK 3.4 investigates the security of lattice-based implementations that are provably secure based on presumed hard lattice problems. In other words, it helps to make sure that there is no big security gap between the specification and the implementation. These results can be used, not only to help to avoid insecure implementation and provide countermeasures for WP4 and 5, but also to help to design the use cases and demonstrators in WP6.

1.2 Publications in this work package

Current status of publications within this work package is summarized in Table 1. We have 36 publications (7 in TASK 3.1, 7 in TASK 3.2, 14 in TASK 3.3 and 8 in TASK 3.4). Most of the publications appear in the top-tier conferences such as Crypto, Eurocrypt and Asiacrypt as well as journals such as IEEE Transactions on Computers.

Category	Status of publications
TASK 3.1	7 publications: 6 in conferences and 1 in preprint
TASK 3.2	7 publications: 3 in conferences, 2 in journals and 2 in preprints
TASK 3.3	14 publications: 11 in conferences and 3 in preprints
TASK 3.4	8 publications: 5 in conferences, 1 in journal and 2 in preprints

Table 1: Current status of publications within this work package.

1.3 Organization of this report

This deliverable provides current results in computational problems, cryptanalysis and basic tools. It can be used to select the parameters, the underlying hard problems

and the secure implementations. Section 2 recalls necessary preliminaries on lattices, lattice assumption as well as some basic tools and schemes. Then, in Sections 3–6, we detail the results in each subtask. Finally, we conclude our intermediate report in Section 7.

2 Background

In this chapter, we recall the basic definitions for understanding this deliverable.

2.1 Lattices

We first recall the definition of lattices and some important and classical quantities about lattices. Then we briefly define the discrete Gaussian distribution over lattices as well as some important properties of it.

2.1.1 Definitions and properties

We first introduce the definition of lattices.

Definition 1 (Lattice) *An n -dimensional lattice $\Lambda \subseteq \mathbb{Q}^m$ ($m \geq n$) is a discrete additive subgroup of \mathbb{Q}^m . The lattice Λ is the set of all integral linear combinations of n linearly independent basis vectors $\mathbf{B} = \{\mathbf{b}_1, \dots, \mathbf{b}_n\} \subseteq \mathbb{Q}^m$. In other words, we have*

$$\Lambda(\mathbf{B}) = \left\{ \sum_{i \in [n]} u_i \mathbf{b}_i : \mathbf{u} \in \mathbb{Z}^n \right\}.$$

We call the matrix \mathbf{B} a basis of the lattice Λ . We can have infinitely many different bases for a lattice. They can be transferred from one to another by multiplying a basis by a unimodular matrix $\mathbf{U} \in \text{GL}_n(\mathbb{Z})$, where n is the dimension of the lattice. For example, suppose both \mathbf{B}_1 and \mathbf{B}_2 are bases of a same lattice Λ , then we can always find a unimodular matrix \mathbf{U} such that $\mathbf{B}_2 = \mathbf{B}_1 \mathbf{U}$.

For any lattice, we have a unique basis in Hermite normal form, defined as follows.

Definition 2 (Hermite normal form) *A matrix $\mathbf{A} \in \mathbb{Z}^{n \times k}$ of full row rank for some integers n, k such that $n \leq k$, is in Hermite normal form if it has the form $\text{HNF}(\mathbf{A}) = (\mathbf{H} | \mathbf{0} \cdots \mathbf{0})$, where $\mathbf{H} \in \mathbb{Z}^{n \times n}$ is a square matrix such that*

1. $h_{i,j} = 0$ for $i < j$;
2. $0 \leq h_{i,j} < h_{i,i}$ for $i > j$.

Here, we recall the uniqueness of the basis of a lattice in Hermite normal form.

Lemma 2.1 ([Sch86, Theorem 4.2]) *Let \mathbf{A} and $\widehat{\mathbf{A}}$ for some integers n, k such that $n \leq k$, with Hermite normal forms $(\mathbf{B} | \mathbf{0} \cdots \mathbf{0})$ and $(\widehat{\mathbf{B}} | \mathbf{0} \cdots \mathbf{0})$, respectively. Then $\Lambda(\mathbf{A}) = \Lambda(\widehat{\mathbf{A}})$ if and only if $\mathbf{B} = \widehat{\mathbf{B}}$.*

Further, we also recall the result that any generating set of a lattice can be transformed to a (full-rank) basis of the basis by computing the Hermite normal form.

Lemma 2.2 ([Sch86, Corollary 4.3b]) *For any matrix $\mathbf{A} \in \mathbb{Z}^{n \times k}$ of full row rank for some integers n, k such that $n \leq k$, there is a unimodular matrix \mathbf{U} such that $\text{HNF}(\mathbf{A}) = \mathbf{A}\mathbf{U}$ is the Hermite normal form of \mathbf{A} .*

According to Lemma 2.2, for any full row rank matrix $\mathbf{A} \in \mathbb{Z}^{n \times k}$ for some integers n, k such that $n \leq k$, we can compute its Hermite normal form $\text{HNF}(\mathbf{A}) = (\mathbf{B}|\mathbf{0} \cdots \mathbf{0})$ with square matrix $\mathbf{B} \in \mathbb{Z}^{n \times n}$, such that $\Lambda(\mathbf{A}) = \Lambda(\mathbf{B})$. Thus, from any generating set $\{\mathbf{a}_i\}_{i \leq k}$, we can obtain a basis \mathbf{B} of the lattice $\Lambda(\mathbf{A})$ by computing its Hermite normal form.

For $i \leq n$, we denote by π_i the orthogonal projection onto the linear subspace $(\mathbf{b}_1, \dots, \mathbf{b}_{i-1})^\perp$. For $i < j \leq n$, $\mathbf{B}_{[i,j]}$ denote the local block $(\pi_i(\mathbf{b}_i), \dots, \pi_i(\mathbf{b}_j))$ and $\Lambda_{[i,j]}$ the lattice generated by $\mathbf{B}_{[i,j]}$. It is helpful to consider these projected sublattices for reducing a problem in high dimension to another one in small dimension. Now we are ready to define the Gram–Schmidt orthogonalization.

Definition 3 (Gram–Schmidt orthogonalization, GSO) *Given $\mathbf{B} = (\mathbf{b}_1, \dots, \mathbf{b}_n)$ a matrix with linearly independent column vectors in \mathbb{R}^m , the corresponding GSO is the matrix $\mathbf{B}^* = (\mathbf{b}_1^*, \dots, \mathbf{b}_n^*)$ where \mathbf{b}_i^* is defined as $\pi_i(\mathbf{b}_i)$.*

To compute the GSO basis vectors, we can first set $\mathbf{b}_1^* = \mathbf{b}_1$, and then compute \mathbf{b}_i^* from $i = 2$ to n as follows:

$$\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j} \mathbf{b}_j^*, \text{ where } \mu_{i,j} = \frac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\langle \mathbf{b}_j^*, \mathbf{b}_j^* \rangle}.$$

Definition 4 (Successive minima) *For any lattice Λ , the i -th minimum $\lambda_i(\Lambda)$ is the radius of the smallest ball with center the origin, $\mathcal{B}(\mathbf{0}, r)$, and containing i linearly independent lattice vectors:*

$$\lambda_i(\Lambda) = \inf\{r : \dim(\text{Span}(\Lambda \cap \mathcal{B}(\mathbf{0}, r))) \geq i\}.$$

In particular, we let $\lambda_1(\Lambda)$ (respectively, $\lambda_1^\infty(\Lambda)$) denote the ℓ_2 -norm (respectively, ℓ_∞ -norm) of a shortest non-zero vector of Λ .

If the first minimum of the primal lattice becomes smaller, the last minimum of its dual lattice is likely to become larger. This relation can be quantified as follows.

Lemma 2.3 ([Ban93, Theorem 2.1]) *For any n -dimensional lattice Λ , we have $1 \leq \lambda_1(\Lambda) \cdot \lambda_n(\Lambda^*) \leq n$.*

Next, we present two important results on the first minimum of lattices, one is rigorous, another one is heuristic.

Gaussian heuristic. Given an n -dimensional lattice Λ with volume $\text{vol}(\Lambda)$, the Gaussian heuristic predicts that the number of lattice points in a measurable subset \mathcal{S} of \mathbb{R}^n of volume $\text{vol}(\mathcal{S})$ is approximately equal to $\text{vol}(\mathcal{S})/\text{vol}(\Lambda)$. Assume that Gaussian heuristic is true when $\text{vol}(\mathcal{S}) \approx \text{vol}(\Lambda)$. Then we can select \mathcal{S} as an n -ball with volume equal to $\text{vol}(\Lambda)$. In this case, the radius of \mathcal{S} can be expected to be an approximation of $\lambda_1(\Lambda)$, which is denoted by

$$\text{GH}(\Lambda) = \sqrt{n/2\pi e} \cdot \text{vol}(\Lambda)^{1/n}.$$

Further, Minkowski's first theorem states that $\lambda_1(\Lambda)$ is larger than $\text{GH}(\Lambda)$ by a factor of 2.

Lemma 2.4 (Minkowski's first theorem) *For any full-rank lattice Λ of dimension n , we have*

$$\lambda_1(\Lambda) \leq \sqrt{\gamma_n} (\det \Lambda)^{1/n},$$

where γ_n is the n -dimensional Hermite constant.

2.1.2 Gaussian distributions over lattices

In the following, we recall the discrete Gaussian distributions over lattices as well as the well-known GPV algorithm for sampling lattice points with this distribution. This will be mainly referred in Section 4 and Section 6.

Definition 5 (Discrete Gaussian over lattices) For $\mathbf{c} \in \mathbb{R}^n$, $r > 0$ and lattice Λ , the discrete Gaussian distribution over Λ , with center \mathbf{c} and standard deviation r is defined as:

$$\mathcal{D}_{\Lambda,r,\mathbf{c}}(\mathbf{x}) = \frac{\rho_{r,\mathbf{c}}(\mathbf{x})}{\rho_{r,\mathbf{c}}(\Lambda)}, \forall \mathbf{x} \in \Lambda,$$

where $\rho_r(\mathbf{x}) = \exp(-\pi\|\mathbf{x}\|^2/r^2)$.

It is well-known that one can efficiently sample from a Gaussian distribution with lattice support given a sufficiently short basis of the lattice.

Lemma 2.5 ([BLP⁺ 13, Le. 2.3]) *There exists a PPT algorithm GPVSample that takes as inputs a basis \mathbf{B} of a lattice $\Lambda \subseteq \mathbb{Z}^n$ and a rational $\sigma \geq \|\tilde{\mathbf{B}}\| \cdot \Omega(\sqrt{\log n})$, and outputs vectors $\mathbf{b} \in \Lambda$ with distribution $D_{\Lambda,\sigma}$.*

We also recall the trapdoor generation algorithm of Alwen and Peikert [AP09], which refines the technique of Gentry *et al.* [GPV08]. This trapdoor will be used to efficiently solve a hard problem such as SIS (Short Integer Solution).

Lemma 2.6 ([AP09, Th. 3.2]) *There is a PPT algorithm TrapGen that takes as inputs 1^n , 1^m and an integer $q \geq 2$ with $m \geq \Omega(n \log q)$, and outputs a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and a basis $\mathbf{T}_{\mathbf{A}}$ of $\Lambda_q^\perp(\mathbf{A})$ such that \mathbf{A} is within statistical distance $2^{-\Omega(n)}$ to $U(\mathbb{Z}_q^{n \times m})$, and $\|\tilde{\mathbf{T}}_{\mathbf{A}}\| \leq \mathcal{O}(\sqrt{n \log q})$.*

2.2 Worst-case lattice problems

In this subsection, we introduce some well-known worst-case lattice problems. They serve as the hardness foundations of lattice-based cryptography. In particular, the two central problems SVP and CVP, as well as some of their variants will be recalled. Finally, we also give some results in approximating the first minimum and distance from any target vector to the lattice. They are sufficient for presenting our results in Section 5.

2.2.1 Definitions and relations

Now we introduce the two most well-known problems in lattices: SVP and CVP, as well as their well-known variants.

Definition 6 (Shortest Vector Problem, SVP) *Given as input a lattice basis \mathbf{B} , the goal is to find a vector $\mathbf{s} \in \Lambda(\mathbf{B})$ of norm $\lambda_1(\Lambda(\mathbf{B}))$.*

We also introduce its approximation version, which is closely related to the security foundation of lattice-based cryptography.

Definition 7 (SVP _{γ}) *Given as input a lattice basis \mathbf{B} and a factor γ , the goal is to find a non-zero vector $\mathbf{s} \in \Lambda(\mathbf{B})$ such that $\|\mathbf{s}\| \leq \gamma \cdot \lambda_1(\Lambda(\mathbf{B}))$.*

We also have a decision (gap) version of SVP_γ .

Definition 8 ($\text{GapSVP}_{n,\gamma}$) *Given as input an n -dimensional lattice associated with basis \mathbf{B} and a factor γ , for $d > 0$, the goal is to distinguish the following two cases:*

1. *Yes instance: $\lambda_1(\Lambda(\mathbf{B})) < d$;*
2. *No instance: $\lambda_1(\Lambda(\mathbf{B})) > \gamma \cdot d$.*

Here we briefly review the two main practical algorithms for solving SVP (or SVP_γ): the sieve algorithm and the enumeration algorithm. Note that there are algorithms with better cost bounds [MV10b, MV10a, ADRS15], but they are less practical compared to the two algorithms below.

Sieve algorithm. The sieve algorithm was first introduced by Ajtai *et al.* [AKS01]. The idea is to first sample a lot of lattice vectors in $\Lambda \cap \mathcal{B}_n(r)$ for some initial radius r , where $\mathcal{B}_n(r)$ denotes the ball of radius r centered at the origin in dimension n . Once we have exponentially many such vectors, we can prove that there is at least a pair of vectors with their addition falling into $\Lambda \cap \mathcal{B}_n(r/c)$ for some constant c . Then by repeating this process polynomially many times, we can successfully find some short vectors with norm close to the first minimum. The polynomial number of iterations contribute to the total solving time by a factor $\text{poly}(n)$. In total, the algorithm runs in time exponential in n .

Enumeration algorithm. First appeared in the 1980s [Kan83, FP83], the enumeration algorithm is the most practical algorithm for solving SVP. The main idea is to search for the optimal solution within a given range. Suppose we aim to find a shortest vector with norm bounded by r in an n -dimensional lattice Λ , the strategy of the enumeration is to find all short vectors with norm $\leq r$ (as potential projections of some shortest vectors) in projected lattice $\pi_i(\Lambda)$ for i from n down to 1. This process can be viewed as a search on a tree: the i -th level is all short vectors in $\Lambda_{[i,n]}$; by going to the $(i-1)$ -th level, we add multiples of \mathbf{b}_{i-1}^* to short vectors found in the i -th level, and we keep only short resulting vector within given norm. We continue to search until we reach the first level, where we find a shortest non-zero vector. In practice, we use the depth first strategy when we search through the tree. Thus the enumeration algorithm is space efficient. It was noticed by Hanrot and Stehlé [HS07] that the number of nodes in level i under the Gaussian heuristic, is

$$N_i = \frac{1}{2} \cdot \frac{V_{n-i+1}(r)}{\text{vol}(\Lambda_{[i,n]})},$$

where $V_{n-i+1}(r)$ is the volume of the sphere of radius r in dimension $(n-i+1)$. When the searching radius r is estimated by Gaussian heuristic, and Geometry Series Assumption (refer to Subsection 2.5) is assumed, the number of nodes in level $\lfloor n/2 \rfloor$ is super-exponential in n . In fact, it was shown by Gama *et al* [GNR10] that the number of nodes in level $\lfloor n/2 \rfloor$ is significantly larger than in other levels.

Overall, the sieve algorithm is asymptotically faster than the enumeration algorithm. However, because of the constants hidden in the exponents, there is a crossover point between the complexity curves of solving these two algorithms. For example, the enumeration algorithm seems better than the sieve algorithm for solving SVP with practical dimensions, e.g., less than 200. Furthermore, Alkim *et al* [ADPS16] state that sieve algorithm will become more efficient than enumeration when the dimension is

≥ 250 . More recently, Ducas [Duc18] shows that we can save $\Theta(n/\log n)$ dimensions with the sieve algorithm for solving SVP on n -dimensional lattices.

For completeness, we also recall the k -list problem [BLS16, KMPM19] here.

Definition 9 (Approximate k -list problem) *Assume we are given k lists L_1, \dots, L_k of equal exponential (in $d > 1$) size t and whose elements are independently and uniformly random vectors from S^{d-1} . The approximate k -list problem is to find t solutions, where a solution is a k -tuple $(x_1, \dots, x_k) \in L_1 \times \dots \times L_k$ satisfying $\|x_1 + \dots + x_k\| \leq 1$.*

For integer $d \geq 1$, let $S^d \subset \mathbb{R}^{d+1}$ denote the d -dimensional unit sphere.

Definition 10 (Closest Vector Problem, CVP) *Given as input a lattice basis \mathbf{B} and a vector \mathbf{t} , the goal is to find a vector $\mathbf{v} \in \Lambda(\mathbf{B})$ closest to \mathbf{t} .*

Correspondingly, we also have a decision (gap) version of CVP $_\gamma$.

Definition 11 (GapCVP $_{n,\gamma}$) *Given as input an n -dimensional lattice associated with basis \mathbf{B} , a target vector \mathbf{t} and a factor γ , for $d > 0$, the goal is to distinguish the following two cases:*

1. *Yes instance:* $\text{dist}(\mathbf{t}, \Lambda(\mathbf{B})) < d$;
2. *No instance:* $\text{dist}(\mathbf{t}, \Lambda(\mathbf{B})) > \gamma \cdot d$.

There is an efficient reduction from SVP to CVP [GMSS99]. However, in the converse reduction from CVP to SVP from [Mic00], the dimension increases from n to n^c for some constant $c > 1$ and the reduction is probabilistic.

Now, we introduce two promise variants, whose instances are a specific subset of instances of SVP and CVP. They are closely related to the underlying security of lattice-based cryptographic primitives [Reg09, LM09].

Definition 12 (unique SVP $_\gamma$, uSVP $_\gamma$) *Let $\gamma \geq 1$. Given as input a lattice basis \mathbf{B} such that $\lambda_2(\mathbf{B}) \geq \gamma \cdot \lambda_1(\mathbf{B})$, the goal is to find a vector $\mathbf{s} \in \Lambda(\mathbf{B})$ of norm $\lambda_1(\Lambda(\mathbf{B}))$. SVP corresponds to $\gamma = 1$.*

uSVP is a promise variant of SVP in the sense that the second minimum is guaranteed to be much larger than the first minimum. Said differently, any vector that is not parallel to the two shortest vectors of norms λ_1 , has norm much larger than λ_1 . Thus any approximate shortest vector within this gap should be the shortest vector itself or multiple of it.

Definition 13 (Bounded Distance Decoding, BDD $_\alpha$) *Let $\alpha > 0$. Given as inputs a lattice basis \mathbf{B} and a vector \mathbf{t} such that $\text{dist}(\mathbf{t}, \Lambda(\mathbf{B})) \leq \alpha \cdot \lambda_1(\mathbf{B})$, the goal is to find a lattice vector $\mathbf{v} \in \Lambda(\mathbf{B})$ closest to \mathbf{t} .*

As opposed to CVP (in which case the target vector can be as far away from the lattice as possible), the BDD problem promises that the target vector is within a bounded distance from the lattice. Note that in some works, the range of α is restricted to $(0, 1/2)$. This is to guarantee that there is exactly one element of Λ in the ball of radius $\alpha \cdot \lambda_1(\Lambda)$ centered on \mathbf{t} . The problem is well-defined even for large α .

2.3 Average-case lattice problems

In this subsection, we first give the definition of the LWE problem, as well as its algebraic variants over polynomial, ring and module. This part of preliminary will be mainly referred in Section 3.

2.3.1 Definitions and properties

Now we introduce the LWE problem in two versions: search and decision.

Definition 14 (LWE distribution) Let $n, m \geq 1, q \geq 2$, and let χ be a probability distribution on \mathbb{Z} . For $\mathbf{s} \in \mathbb{Z}_q^n$, we define the LWE distribution as the distribution over $\mathbb{Z}_q \times \mathbb{Z}_q$ obtained by sampling $\mathbf{a} \leftarrow U(\mathbb{Z}_q^n)$, $e \leftarrow \chi$, and returning the pair $(\mathbf{a}, \mathbf{a}^T \cdot \mathbf{s} + e)$.

Definition 15 (search-LWE) The search-LWE problem consists in finding \mathbf{s} from a sampler of LWE distribution, with the secret $\mathbf{s} \in \mathbb{Z}_q^n$.

Definition 16 (decision-LWE) The decision-LWE problem consists in distinguishing between a sampler of LWE distribution and a uniform sampler over $\mathbb{Z}^n \times \mathbb{Z}_q$, with the secret $\mathbf{s} \in \mathbb{Z}_q^n$.

As a counterpart for the LWE problem, the short integer solution (SIS) [Ajt96, GPV08] and its inhomogeneous variant (Inhomogeneous-SIS (ISIS)) is also known to have many important applications such as signature, in lattice-based cryptography.

Definition 17 (SIS) Let $n, m \geq 1, q \geq 2$. Given a matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$, the SIS problem consists in finding vector $\mathbf{x} = (x_1, \dots, x_m)^T \in \mathbb{Z}^m$ with small norm, such that $\mathbf{x}^T \mathbf{A} = \mathbf{0} \pmod q$.

Definition 18 (ISIS) Let $n, m \geq 1, q \geq 2$. Given a matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ and a vector $\mathbf{u} \in \mathbb{Z}^m$, the ISIS problem consists in finding a vector $\mathbf{x} = (x_1, \dots, x_m)^T \in \mathbb{Z}^m$ with small norm, such that $\mathbf{x}^T \mathbf{A} = \mathbf{u} \pmod q$.

The q -ary lattices is a specific family of lattices, which is of particular importance in lattice-based cryptography. They are defined as follows.

Definition 19 (q -ary lattices) An n -dimensional q -ary lattice is a lattice $\Lambda \subseteq \mathbb{Z}^n$ such that $q\mathbb{Z}^n \subseteq \Lambda \subseteq \mathbb{Z}^n$.

Thus, in a q -ary lattice, it is sufficient to look at $\Lambda \pmod q$. Because all the shifts of $\Lambda \pmod q$ by $q\mathbb{Z}^n$ form a complete partition of Λ . For $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$, we define the q -ary lattice $\Lambda_q(\mathbf{A}) = \{\mathbf{A}\mathbf{x} \pmod q : \mathbf{x} \in \mathbb{Z}_q^n\}$. This specific q -ary lattice is closely related to the LWE problem. In particular, the LWE problem can be viewed as a BDD instance in this q -ary lattice $\Lambda_q(\mathbf{A})$, where \mathbf{A} is the first component of LWE sample, and the second component serves as the target vector of the BDD instance. Once we find the closest vector $\mathbf{c} = \mathbf{A}\mathbf{s}$ to target vector \mathbf{b} , the secret vector \mathbf{s} can be simply recovered by Gaussian elimination assuming the matrix \mathbf{A} is full rank. For completeness, we recall that for a matrix \mathbf{A} randomly chosen from $\mathbb{Z}_q^{m \times n}$, the matrix \mathbf{A} is full rank for a sufficiently large m with overwhelming probability [BLP⁺13, Claim 2.13].

2.3.2 Algebraic variants

The protocols relying on the hardness of LWE are inherently inefficient due to the size of the public keys which usually contain m elements of \mathbb{Z}_q^n , where m is the number of samples which is usually larger than $n \log(n)$. To improve the efficiency, structured variants of LWE have been proposed [SSTX09, LPR10, LS15]. One promising variant is the *Polynomial Learning With Errors* (P-LWE) problem, introduced by Stehlé et al. [SSTX09].

Definition 20 (PLWE distribution) *Let K be a degree n number field defined by f , \mathcal{O}_K its ring of integers, χ a distribution over $\mathbb{R}[x]/f$ and $q \geq 2$. For $s \in \mathbb{Z}_q[x]/f$, we define the PLWE distribution as the distribution over $\mathbb{Z}[x]/f \times \mathbb{R}[x]/f$ obtained by sampling $a \leftarrow U(\mathbb{Z}_q[x]/f)$, $e \leftarrow \chi$ and returning the pair $(a, a \cdot s + e)$ (with $\mathbb{R}_q = \mathbb{R}/q\mathbb{Z}$).*

Definition 21 (search-PLWE) *The search-PLWE consists in finding s from a sampler of PLWE distribution, with the secret $s \in \mathbb{Z}_q[x]/f$ and χ arbitrary.*

Definition 22 (decision-PLWE) *The decision-PLWE consists in distinguishing between a sampler of PLWE distribution and a uniform sampler over $\mathbb{Z}[x]/f \times \mathbb{R}[x]/f$, with the secret $s \in \mathbb{Z}_q[x]/f$ and χ arbitrary.*

The P-LWE problem also admits worst-case to average-case connections from well-studied lattice problems. Whereas the hardness reductions for LWE start from the lattice problem in the class of general Euclidean lattices, the class has to be restricted to *ideal lattices* in the case of P-LWE. These ideal lattices correspond to the ideals in the polynomial ring $\mathbb{Z}[x]/f$. Lyubashevsky et al. [LPR10] propose another promising variant, namely the *Ring Learning With Errors* (R-LWE) problem, where polynomial rings are replaced by the ring of integers of some number fields.

Definition 23 (RLWE and RLWE[∨] distributions) *Let K be a degree n number field defined by f , $R = \mathcal{O}_K$ its ring of integers, χ a distribution over $K_{\mathbb{R}}$ and $q \geq 2$. For $s \in R/qR$ (resp. R^{\vee}/qR^{\vee}), we define the RLWE (resp. RLWE[∨]) distribution as the distribution over $R_q \times K_{\mathbb{R}}/qR$ (resp. $R_q \times K_{\mathbb{R}}/qR^{\vee}$) obtained by sampling $a \leftarrow U(R_q)$, $e \leftarrow \chi$ and returning the pair $(a, a \cdot s + e)$.*

In the definition above, we identified the support of χ with $K_{\mathbb{R}}$.

Definition 24 (search-RLWE and search-RLWE[∨]) *The search-RLWE (resp. search-RLWE[∨]) consists in finding s from a sampler of RLWE (resp. RLWE[∨]) distribution, with the secret $s \in R_q$ (resp. R_q^{\vee}) and χ arbitrary.*

Definition 25 (decision-RLWE and decision-RLWE[∨]) *The decision-RLWE (resp. decision-RLWE[∨]) consists in distinguishing between a sampler of RLWE (resp. RLWE[∨]) distribution and a uniform sampler over $R_q \times K_{\mathbb{R}}/qR$ (resp. $R_q \times K_{\mathbb{R}}/qR^{\vee}$), with the secret $s \in R_q$ (resp. R_q^{\vee}) and χ arbitrary.*

In the case of cyclotomic fields, the P-LWE and R-LWE problems coincide up to some parameter losses. As a recent result, Roşca et al. [RSW18] show that P-LWE and R-LWE are equivalent for a larger class of polynomials. In addition, they also investigate other relations between these structured variants.

In [LS15], Langlois and Stehlé generalize RLWE problem to the module setting and propose the Module-LWE problem, which helps for a more reflexible parameter selection as well as a trade-off between hardness and efficiency.

2.4 Quantum computations and quantum random oracle model

In this subsection, we present some necessary notations and concepts of quantum computations as well as the quantum random oracle model, for the description of our results in Section 3 and Section 5.

In quantum computations, data is stored as quantum bits (called *qubits*) in quantum registers. In general, a state of n qubits is written as

$$|\phi\rangle = \sum_{\mathbf{x} \in \{0,1\}^n} a_{\mathbf{x}} |\mathbf{x}\rangle \quad (1)$$

where $a_{\mathbf{x}} \in \mathbb{C}$ such that $\sum_{\mathbf{x} \in \{0,1\}^n} |a_{\mathbf{x}}|^2 = 1$. The same state $|\phi\rangle$ can be represented differently, e.g., as follows:

$$|\phi\rangle = \sum_{\mathbf{x}' \in S} a'_{\mathbf{x}'} |\mathbf{x}'\rangle,$$

for any finite set S that can be mapped (by some function g) to a set of independent vectors in the Hermitian space $\mathbb{C}^{\#S}$. We call the set $\{ |g(\mathbf{x}')\rangle \}_{\mathbf{x}' \in S}$ a basis of the state. For example, the basis of the state $\phi_1 = (1/\sqrt{2})(|0\rangle + |1\rangle)$ can be $(\mathbf{b}_1, \mathbf{b}_2)$, where $\mathbf{b}_1 = (1, 0)^T$ and $\mathbf{b}_2 = (0, 1)^T$. Typically, we let $|x\rangle |y\rangle$ (or $|x, y\rangle$) denote the tensor product $|x\rangle \otimes |y\rangle$ of the two states $|x\rangle$ and $|y\rangle$. To measure the difference between two quantum states, we use the trace distance.

In classical computations, we are allowed to apply an irreversible gates to data: $x \mapsto f(x)$ for a possibly non-injective function f . It is also well-known that all the classical circuits can be transformed into corresponding quantum circuits with similar functionalities with the following map [Ben73]:

$$\sum_{x \in S} a_x |x, y\rangle \mapsto \sum_{x \in S} a_x |x, y \oplus f(x)\rangle.$$

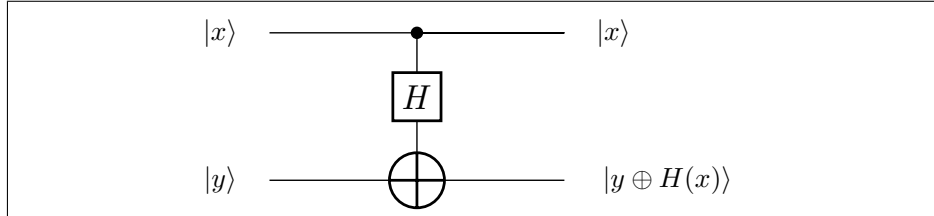


Figure 2: Quantum circuit for accessing random oracle H with input $|x\rangle$.

Quantum random-oracle model. As considered in [BDF+11], the quantum random-oracle model (QROM) is similar to their counterparts in the classical random-oracle model [BR93], with the difference that we consider quantum adversaries that are given quantum access to the random oracles involved. Also refer to Figure 2 as an illustration of quantum access to random oracle H .

For completeness, we also recall the continuous hidden subgroup problem (HSP) [EHKS14] as follows.

Definition 26 (Continuous HSP) Let $m \geq 1$, $H \subset \mathbb{R}^m$ a hidden discrete subgroup. Given quantum access to a function $f: \mathbb{R}^m \rightarrow \mathcal{S}$ as a H -periodic function for some set \mathcal{S} (i.e., $|x\rangle \mapsto |f(x)\rangle$), the continuous hidden subgroup problem is to find the hidden subgroup H .

2.5 Lattice reduction

In this section, we recall some well-known definitions of lattice reductions. Among them, the BKZ reduction is one of the most important tools for assessing the security of lattice-based cryptographic scheme.

2.5.1 Size reduction

First, we define the size-reduction conditions. If we view the GSO procedure as a QR decomposition, then the size-reduction conditions can be seen as a requirement on the upper triangular matrix.

Definition 27 (Size-reduction) A matrix $\mathbf{B} \in \mathbb{R}^{m \times n}$ is called size-reduced, if it satisfies:

$$|\mu_{i,j}| \leq \frac{1}{2}, \quad 1 \leq j < i \leq n,$$

where $\mu_{i,j} = \langle \mathbf{b}_i, \mathbf{b}_j^* \rangle / \langle \mathbf{b}_j^*, \mathbf{b}_j^* \rangle$.

If $\mathbf{b}_j^* = \mathbf{0}$, we let $\mu_{i,j} = 0$ for any $i \geq j$.

Algorithm 1 for achieving the size reduction condition.

Algorithm 1 Size-reduction algorithm

Require: A basis $\mathbf{B} = \{\mathbf{b}_1, \dots, \mathbf{b}_n\}$.

Ensure: A size-reduced basis of $\Lambda(\mathbf{B})$.

```

1: Compute the GSO basis  $\mathbf{b}_1^*, \dots, \mathbf{b}_n^*$ 
2: for  $i = 2$  to  $n$  do
3:   for  $j = i - 1$  down to  $1$  do
4:      $\mathbf{b}_i \leftarrow \mathbf{b}_i - \lceil \mu_{i,j} \rceil \mathbf{b}_j$ 
5:     for  $k = 1$  to  $j$  do
6:        $\mu_{i,k} \leftarrow \mu_{i,k} - \lceil \mu_{i,j} \rceil \mu_{j,k}$ 
7:     end for
8:   end for
9: end for

```

The size-reduction condition should be understood more clearly if we consider the GSO (or QR-decomposition). Suppose that we start from any basis $\mathbf{B} = \mathbf{Q}\mathbf{R}$ with an orthogonal matrix \mathbf{Q} and an upper triangular matrix

$$\mathbf{R} = \begin{pmatrix} \ddots & \vdots & \dots & \vdots & \dots \\ & \|\mathbf{b}_i^*\| & \dots & \mu_{ij} \|\mathbf{b}_i^*\| & \dots \\ & & \ddots & \vdots & \dots \\ & & & \|\mathbf{b}_j^*\| & \dots \\ & & & & \ddots \end{pmatrix}.$$

In particular, to achieve the size-reduction condition for a specific μ_{ji} with $i < j$,

it suffices to construct a unimodular matrix \mathbf{U}_{ij} and apply it on \mathbf{R} as follows

$$\mathbf{R} \cdot \mathbf{U}_{ij} = \begin{pmatrix} \ddots & \vdots & \cdots & \vdots & \cdots \\ & \|\mathbf{b}_i^*\| & \cdots & \mu_{ji}\|\mathbf{b}_i^*\| & \cdots \\ & & \ddots & \vdots & \cdots \\ & & & \|\mathbf{b}_j^*\| & \cdots \\ & & & & \ddots \end{pmatrix} \begin{pmatrix} \ddots & & & & \\ & 1 & -\lfloor \mu_{ji} \rfloor & & \\ & & \ddots & & \\ & & & 1 & \\ & & & & \ddots \end{pmatrix} = \begin{pmatrix} \ddots & \vdots & \cdots & \vdots & \cdots \\ & \|\mathbf{b}_i^*\| & \cdots & \widehat{\mu}_{ji}\|\mathbf{b}_i^*\| & \cdots \\ & & \ddots & \vdots & \cdots \\ & & & \|\mathbf{b}_j^*\| & \cdots \\ & & & & \ddots \end{pmatrix},$$

where we have $|\widehat{\mu}_{ji}| \leq 1/2$. This step is exactly corresponding to Line 4 of Algorithm 1. Notice that such an operation $\mathbf{R} \cdot \mathbf{U}_{ij}$ for some $i < j$ may also change the values μ_{ik} for $k < i$. Thus we can proceed to apply these specific unimodular matrices \mathbf{U}_{ij} to \mathbf{R} from bottom ($i = j$) to up ($i = 1$) (see Algorithm 1 for a full procedure).

Given a basis $\mathbf{B} = \mathbf{QR}$, the product $\prod_i \|\mathbf{b}_i^*\|$ of the diagonal components of \mathbf{R} is fixed and equal to the determinant of the lattice associated with the basis \mathbf{B} . Intuitively, to obtain a good basis, we aim to make the $\|\mathbf{b}_i^*\|$'s have limited decrease.

2.5.2 LLL reduction

The LLL-reduction can be computed in polynomial-time (see [LLL82]).

Definition 28 (LLL-reduction) For $\delta \in (1/4, 1)$, a matrix $\mathbf{B} \in \mathbb{R}^{m \times n}$ is called LLL_δ reduced, if it is size-reduced and satisfies the Lovász condition:

$$\delta \|\mathbf{b}_i^*\|^2 \leq \|\mu_{i+1,i}\mathbf{b}_i^* + \mathbf{b}_{i+1}^*\|^2$$

for $1 \leq i < n$.

Furthermore, the LLL-reduction condition can be achieved efficiently in polynomial-time by the LLL-reduction algorithm proposed by Lenstra *et al* [LLL82].

Algorithm 2 LLL-reduction algorithm

Require: A basis $\mathbf{B} = \{\mathbf{b}_1, \dots, \mathbf{b}_n\}$ and parameter δ .

Ensure: A δ -LLL-reduced basis of $\Lambda(\mathbf{B})$.

- 1: Size-reduce(\mathbf{B}).
 - 2: Swap:
 - 3: **if** $\exists i$ such that $\|\mu_{i+1,i}\mathbf{b}_i^* + \mathbf{b}_{i+1}^*\|^2 < \delta \|\mathbf{b}_i^*\|^2$ **then**
 - 4: swap($\mathbf{b}_i, \mathbf{b}_{i+1}$)
 - 5: goto Step 1
 - 6: **end if**
-

2.5.3 HKZ reduction

The Hermite-Korkine-Zolotarev (HKZ) reduction is more promising for approaching the successive minima, even though an HKZ-reduced basis does not necessarily reach them.

Definition 29 (HKZ-reduction) A matrix $\mathbf{B} \in \mathbb{R}^{m \times n}$ is called HKZ-reduced, if it is size-reduced and satisfies:

$$\|\mathbf{b}_i^*\| = \lambda_1(\Lambda_{[i,n]})$$

for all $i \in \{1, \dots, n\}$.

Here, we recall a result on the relation between the norms of HKZ-reduced basis vectors and the successive minima of the lattice.

Lemma 2.7 ([LLS90, Theorem 2.1]) *Let $\mathbf{B} = (\mathbf{b}_1, \dots, \mathbf{b}_n)$ be an HKZ-reduced basis of a lattice Λ . We have*

$$\frac{4}{i+3} \lambda_i(\Lambda)^2 \leq \|\mathbf{b}_i\|^2 \leq \frac{i+3}{4} \lambda_i(\Lambda)^2$$

for all $i \in [n]$.

For an n -dimensional HKZ-reduced basis, we can also quantify the relations among its Gram–Schmidt norms $\|\mathbf{b}_i^*\|$'s in the worst case as follows.

Lemma 2.8 *For any HKZ-reduced basis $\mathbf{B} = \mathbf{QR}$ of an n -dimensional lattice, we have, for all $i < n$,*

$$\|\mathbf{b}_i^*\| \leq \sqrt{\gamma_{n-i+1}} \cdot \left(\prod_{j=i}^n \|\mathbf{b}_j^*\| \right)^{\frac{1}{n-i+1}}. \quad (2)$$

This worst-case result is obtained by considering the Minkowski's first theorem. If we take equalities in the inequalities above, when we fix $\|\mathbf{b}_n^*\|$, all the remaining $\|\mathbf{b}_i^*\|$'s are also fixed. Equation (2) can be rewritten as

$$x_i = \frac{1}{2} \log \gamma_{n-i+1} + \frac{1}{n-i+1} \sum_{j=i}^n x_j$$

for all $i < n$, where $x_i = \log \|\mathbf{b}_i^*\|$. The x_i 's are also known as the worst-case HKZ profile.

To obtain an HKZ-reduced basis, one is needed to find a shortest vector in each projected lattice, with dimension from n to 1. As we have already discussed in Section 2.2, the currently best known SVP solvers take time exponential in dimension n , which becomes very costly when n grows.

Algorithm 3 HKZ-reduction algorithm

Require: A basis $\mathbf{B} = \{\mathbf{b}_1, \dots, \mathbf{b}_n\}$.

Ensure: A HKZ-reduced basis of $\Lambda(\mathbf{B})$.

- 1: **for** $k = 1$ **to** $n - 1$ **do**
 - 2: Find any \mathbf{b} such that $\|\pi_k(\mathbf{b})\| = \lambda_1(\Lambda_{[k,n]})$
 - 3: $\mathbf{B} \leftarrow \text{LLL-reduce}(\mathbf{b}_1, \dots, \mathbf{b}_{k-1}, \mathbf{b}, \mathbf{b}_k, \dots, \mathbf{b}_n)$
 - 4: Size-reduce(\mathbf{B})
 - 5: **end for**
-

Note that in Step 3 of Algorithm 3, the LLL-reduction is used to remove the linear dependency between \mathbf{b} and $\{\mathbf{b}_k, \dots, \mathbf{b}_n\}$ (in this case, the input is a generating set instead of a basis). Further, the inserted vector \mathbf{b} will not be exchanged with any of $\{\mathbf{b}_1, \dots, \mathbf{b}_{k-1}\}$ because the Lovász condition is always satisfied.

2.5.4 BKZ reduction

Later, Schnorr [Sch87] gave a block-wise lattice reduction for trade-off between the LLL-reduction and HKZ-reduction. It was also made more practical by Schnorr and Euchner [SE91, SE94], whose variant is known as the Block Korkine-Zolotarev (BKZ) reduction algorithm.

Definition 30 (BKZ-reduction) A matrix $\mathbf{B} \in \mathbb{R}^{m \times n}$ is said to be BKZ_β reduced for block size $\beta \geq 2$, if it is size-reduced and satisfies:

$$\|\mathbf{b}_i^*\| \leq \lambda_1(\Lambda_{[i, \min(i+\beta-1, n)]})$$

for all $i \in \{1, \dots, n-1\}$.

The BKZ reduction condition can be seen as a run-time/quality trade-off between LLL-reduction and HKZ-reduction. Next, we will first review the (practical) BKZ reduction algorithm [SE91, SE94] for (almost) achieving BKZ-reduction.

The BKZ algorithm. The Schnorr-Euchner BKZ algorithm [SE94] takes as inputs a block-size β and a basis $\mathbf{B} = \{\mathbf{b}_1, \dots, \mathbf{b}_n\}$ of a lattice Λ , and outputs a basis which is ‘close’ to being BKZ_β -reduced (up to numerical inaccuracies, as the underlying Gram–Schmidt orthogonalization is computed in floating-point arithmetic, and up to the progress parameter $\delta < 1$). BKZ starts by LLL-reducing the input basis, then calls an SVP-solver on consecutive local blocks $\mathbf{B}_{[k, \min(k+\beta-1, n)]}$ for $k = 1, \dots, n-1$. This is called a *BKZ tour*. After each execution of the SVP-solver, if we have $\lambda_1(\Lambda_{[k, \min(k+\beta-1, n)]}) < \delta \cdot \|\mathbf{b}_k^*\|$, then BKZ updates the block $\mathbf{B}_{[k, \min(k+\beta-1, n)]}$ by inserting the vector found by the SVP-solver between indices $k-1$ and k , and LLL reduce the block from the first index to the last index of current block (in this case, the input is a generating set instead of a basis). Otherwise, we LLL-reduce the block from first index to the last index of current block directly, without any insertion. The procedure terminates when no change occurs at all during a tour. We refer to Algorithm 4 for a complete description of the BKZ algorithm.

Algorithm 4 The Schnorr and Euchner BKZ algorithm

Require: A basis $\mathbf{B} = \{\mathbf{b}_1, \dots, \mathbf{b}_n\}$, a block size $\beta \geq 2$ and a constant $\delta < 1$.

Ensure: A BKZ_β -reduced basis of $\Lambda(\mathbf{B})$.

```

1: repeat
2:   for  $k = 1$  to  $n - 1$  do
3:     Find any  $\mathbf{b}$  such that  $\|\pi_k(\mathbf{b})\| = \lambda_1(\Lambda_{[k, \min(k+\beta-1, n)]})$ 
4:     if  $\delta \cdot \|\mathbf{b}_k^*\| > \|\mathbf{b}\|$  then
5:        $\mathbf{B} \leftarrow \text{LLL-reduce}(\mathbf{b}_1, \dots, \mathbf{b}_{k-1}, \mathbf{b}, \mathbf{b}_k, \dots, \mathbf{b}_{\min(k+\beta, n)})$ .
6:     else
7:        $\mathbf{B} \leftarrow \text{LLL-reduce}(\mathbf{b}_1, \dots, \mathbf{b}_{\min(k+\beta, n)})$ .
8:     end if
9:   end for
10: until no change occurs.
```

2.6 Basic cryptosystems

In this subsection, we will remind some necessary basic cryptosystems for the need of presenting our results in Section 5 and Section 6.

2.6.1 The AJPS Mersenne-based cryptosystem

First, we recall the AJPS cryptosystem (See Construction 1), which was known to be a candidate for first-round NIST PQC standardization.

Construction 1. AJPS cryptosystem.

Key Generation: Let n be a prime number. Randomly choose two elements $f, g \in R = \mathbb{Z}/N\mathbb{Z}$ of Hamming weight w , where g is invertible in R and $N = 2^n - 1$. Set $h = f/g$. The public key is h , and the secret key is g .

Encryption: To encrypt a bit s , pick random $p, q \in R$ of Hamming weight at most w . Output the ciphertext $c = (-1)^s(ph + q) \in R$.

Decryption: To decrypt c , compute $cg = (-1)^s(phg + qg) = (-1)^s(pf + qg)$. Since p, q, f and g all have Hamming weight $\leq w$, the n -bit string $pf + qg$ has Hamming weight $\leq 2w^2 < n/2$. Thus if $s = 0$, then $|cg| < n/2$. On the other hand, if $s = 1$, then $|-cg| < n/2$, as a result, $|cg| > n - n/2 = n/2$. Thus, to decrypt c , output 0 if $|cg| < n/2$, and 1 otherwise.

2.6.2 The GGH signature scheme

Next, we recall the GGH signature in a high level (see Construction 2). The first-round NIST PQC candidate: DRS signature can be seen as a variant following the same design paradigm of GGH signature. We refer the reader to [PSDS] for a detailed description for DRS signature.

Construction 2. GGH signature.

Key Generation: Let n be a prime number, $H : \mathbb{Z}^n \rightarrow \mathbb{Z}^n$ be a hash function. Choose a short basis \mathbf{B} for a full rank lattice $\Lambda \subset \mathbb{Z}^n$ and compute a public basis $\mathbf{B}' = \mathbf{U}\mathbf{B}$ with \mathbf{U} a randomly chosen unimodular matrix. The signing key is: \mathbf{B} , and the verification key is \mathbf{B}' .

Sign: To sign a message $\mathbf{m} \in \mathbb{Z}^n$, first use H to hash it to $\mathbf{u} = H(\mathbf{m}) \in \mathbb{Z}^n$, then use the short basis \mathbf{B} to compute a lattice vector \mathbf{s} close to $H(\mathbf{m})$. Output the signature (\mathbf{m}, \mathbf{s}) .

Verify: To verify a signature (\mathbf{m}, \mathbf{s}) , first check \mathbf{s} is indeed in the lattice $\Lambda(\mathbf{B}') = \Lambda(\mathbf{B})$, then verify if $\|\mathbf{s} - H(\mathbf{m})\|$ is small, return 0 if either of the test fails, return 1 otherwise.

2.6.3 The GPV and Lyubashevsky’s signature schemes

Other than the GGH-style signature, there are mainly two types of lattice-based signatures: GPV signature [GPV08] with trapdoor (see Construction 3) and Schnorr-like signature without trapdoor [Lyu12] (see Construction 4). The NIST PQC second-round candidate Falcon [PFH⁺19] and its simpler predecessor DLP [DLP14] can be seen as efficient variants of GPV signature scheme over NTRU lattices, thus achieving great speed-ups compared to the original one over general lattice setting. On the other hand, there are also numerous follow-up works of Lyubashevsky’s signature without trapdoor, which include an efficient variant with bimodel Gaussians called BLISS [DDLL13] and its adaptation for embedded system called GLP [GLP12], as well as the second-round NIST candidate Dilithium [DKL⁺18].

Construction 3. GPV signature.

Key Generation: Let $n, m \geq 1, q \geq 2, H : \mathbb{Z}^n \rightarrow \mathbb{Z}^n$ be a hash function. Apply the Alwen and Peikert trapdoor generation algorithm (refer to Lemma 2.6) to generate a pair $(\mathbf{A}, \mathbf{T}) \in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}^{m \times m}$. The signing key is: \mathbf{T} and the verification key is: \mathbf{A} .

Sign: To sign a message $\mathbf{m} \in \mathcal{M}$, first use H to hash it to $\mathbf{u} = H(\mathbf{m}) \in \mathbb{Z}^n$, then use the trapdoor \mathbf{T} to compute a short solution \mathbf{x} to the ISIS instance (\mathbf{A}, \mathbf{u}) . Output the signature (\mathbf{m}, \mathbf{x}) .

Verify: To verify a signature (\mathbf{m}, \mathbf{x}) , check if $\mathbf{x}^T \mathbf{A} = H(\mathbf{m}) \pmod q$ and \mathbf{x} has small norm, return 0 if either of the test fails, return 1 otherwise.

Construction 4. Lyubashevsky's signature.

Key Generation: Let $d, k, n, m, M \geq 1, q \geq 2, H : \{0, 1\}^* \rightarrow \{\mathbf{v} : \mathbf{v} \in \{-1, 0, 1\}^k, \mathbf{v} \text{ has small norm}\}$ be a hash function. The signing key is: $\mathbf{S} \leftarrow \{-d, \dots, 0, \dots, d\}^{m \times k}$ and the verification key is: $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}, \mathbf{T} = \mathbf{AS}$.

Sign: To sign a message $\mathbf{m} \in \mathcal{M}$, first select $\mathbf{y} \leftarrow \mathcal{D}_{\mathbb{Z}^m, \sigma, 0}$ with large enough $\sigma > 0$, then compute $\mathbf{c} = H(\mathbf{A}\mathbf{y}, m)$ and $\mathbf{z} = \mathbf{S}\mathbf{c} + \mathbf{y}$. Output the signature $(\mathbf{m}, \mathbf{z}, \mathbf{c})$ with probability $\min\left(\frac{\mathcal{D}_{\mathbb{Z}^m, \sigma, 0}(\mathbf{z})}{M \mathcal{D}_{\mathbb{Z}^m, \sigma, \mathbf{S}\mathbf{c}}(\mathbf{z})}, 1\right)$.

Verify: To verify a signature $(\mathbf{m}, \mathbf{z}, \mathbf{c})$, check if $\mathbf{c} = H(\mathbf{A}\mathbf{z} - \mathbf{T}\mathbf{c}, m)$ and \mathbf{z} has small norm, return 0 if either of the test fails, return 1 otherwise.

2.7 Side-channel attacks and countermeasures

In this subsection, we will recall some necessary preliminaries about side-channel attacks and countermeasures for presenting our results mainly in Section 6.

2.7.1 Implementation attacks

We note that an extensive introduction on side-channel attacks is well given in deliverable D.3.1. For the sake of completeness, we recall the same content from there as a necessary preliminaries for current results, which include fault attack and timing attack.

Fault attacks. The idea of fault attacks is to induce a fault into a circuit and use the faulty output to get information about the secret key. This can be achieved by high temperature, unsupported supply voltage or current, excessively high overclocking, strong electric or magnetic fields, or even ionizing radiation. Fault attacks are usually non-invasive as the induced fault is only temporary and the device is not permanently damaged.

Timing attacks. When implementing cryptographic algorithms, the developer has to make sure that the execution time is independent of the secret data that is processed. Otherwise an attacker might be able to exploit the information about the execution time. Such attacks should not only be considered for embedded devices for which the attacker has physical access to, but also remote timing attacks are a threat that must be considered as shown by Brumley and Boneh [BB03]. Timing information can be leaked by conditional branches, instructions with non-constant execution time, and memory accesses that trigger cache hits or misses [Ber05].

2.7.2 Countermeasures

Again, we note that a fairly detailed overview of countermeasure for side-channel attacks is described in the deliverable D.3.1. For the sake of completeness, we recall two countermeasures: masking and constant-time implementation.

Masking The idea behind masking is to split a secret value into several shares. The secret value can only be reconstructed with the knowledge of all shares. The splitting of the secret value can be performed in a Boolean way or in an arithmetic way. Boolean masking means that the XOR-sum of all shares results in the secret value and arithmetic masking means that the arithmetic sum or difference of the shares results in the secret value. There are conversion approaches to switch between arithmetic and Boolean masking [CGTV15]. The major advantage of masking schemes is that they allow to prove the side-channel security of an algorithm. Nevertheless, there are still implementation challenges that have to be taken care of. Otherwise, a provably secure algorithm might still have a side-channel leakage. To achieve higher-order security, it is necessary to split the secret value into more shares.

Constant-time implementation. To prevent timing attacks and simple power analysis it is crucial to develop an implementation that has an execution time independent from the secrets. Some pitfalls that should be avoided are:

- Comparison of secret strings: Such a comparison must not stop at the first unequal character.
- Branches: Branches must not be dependent on secret data. Ideally the same branches are taken for every run of the implementation.
- Table look-ups: On platforms with a cache, table look-ups can have varying access times. Thus the index must not depend on secret data for such platforms. In some cases it might be necessary to completely disable caches.
- Compiler optimization: A developer must take care that the compiler does not remove instructions that are critical for the security of the implementation but irrelevant for its functionality.

3 TASK 3.1: Quantum assumptions and reductions

Here, we will review the targets of TASK 3.1 and summarize the results obtained so far.

3.1 Review of the targets

Table 2 describes the targets of TASK 3.1. The main objective is to provide good candidates for the underlying assumptions and security models for the building blocks in WP4 and the privacy-preserving schemes in WP5. We first aim at investigating how the security model should be, assuming the existence of quantum computer. There are mainly three directions to work for this. At the beginning, we need to adapt our current proof technique with respect to the QROM. Next, we need to further make sure the QROM-secure protocol can be efficiently implemented. Finally, we need to search for possible relaxations of QROM to propose more efficient solutions. Second, we want to have a better understanding of the hardness of lattice problems as well as their related computational problems. To start, we need to try to improve current reduction, which will hopefully give us more efficient parameters for lattice-based cryptography. To continue, we would like to search for new reductions for existing hard problems, which will bring us new relations and hopefully new hardness results on known lattice problems or related computational problems.

Targets	Concrete contents
Investigate secure models for post-quantum cryptographic scheme	Develop new proof techniques needed for QROM
	Assess/improve practicality of QROM-secure schemes
	Understand relevance of the QROM, find possible relaxations
Study the hardness of lattice problems	Improve tightness of known reductions
	Find new reductions between lattice problems

Table 2: Concrete targets within TASK 3.1.

3.2 Overview of current results

An overview of the results obtained in TASK 3.1 can be found in Table 3. We give more details in the following subsections.

3.3 Current results on quantum assumptions

Within the scope of quantum assumptions, we have 3 publications: 2 in conferences and 1 in preprint. The question of the quantum security of the Fiat-Shamir transform (which allows the construction of signature schemes) has been greatly elucidated with two results [KLS18, DFMS19]. The first result [KLS18] gives a tight security proof, and comes at small cost on schemes such as Dilithium [DKL⁺18]. The second [DFMS19] gives a non-tight proof, but requires no extra properties from the scheme, and therefore comes with no impact on efficiency. Recently the result [HKSU18] also gives an

Category	Work	Status
Quantum assumptions	A Concrete Treatment of Fiat-Shamir Signatures in the Quantum Random-Oracle Model [KLS18]	Eurocrypt 2018
	Security of the Fiat-Shamir Transformation in the Quantum Random-Oracle Model [DFMS19]	Crypto 2019
	Generic Authenticated Key Exchange in the Quantum Random Oracle Model [HKSU18]	Preprint
Reductions	On the Ring-LWE and Polynomial-LWE Problems [RSW18]	Eurocrypt 2018
	Order-LWE and the Hardness of Ring-LWE with Entropic Secrets [BP18]	Asiacrypt 2019
	Middle-Product Learning with Rounding Problem and its Applications [BBD ⁺ 19]	Asiacrypt 2019
	Worst-Case Hardness for LPN and Cryptographic Hashing via Code Smoothing [BLVW19]	Eurocrypt 2019

Table 3: Current (intermediate) results on TASK 3.1.

investigation on a simpler generic transformation for authenticated key exchange in QROM.

A Concrete Treatment of Fiat-Shamir Signatures in the Quantum Random-Oracle Model. The Fiat-Shamir transform is a technique for combining a hash function and an identification scheme to produce a digital signature scheme. The resulting scheme is known to be secure in the random oracle model, which does not, however, imply security in the scenario where the adversary has also quantum access to the oracle.

In this work, a generic framework is proposed for constructing tight reductions in the QROM from underlying hard problems to Fiat-Shamir signatures. The proposed generic reduction is composed of two results whose proofs are believed to be simple and natural. First, a security notion (UF-NMA) is considered in which the adversary obtains the public key and attempts to create a valid signature without accessing a signing oracle. Second, a tight reduction is given to show that deterministic signatures (i.e., ones in which the randomness is derived from the message and the secret key) that are UF-NMA secure are also secure under the standard chosen message attack (UF-CMA) security definition. The second result is showing that if the identification scheme is “lossy”, as defined in [AFLT12] by Abdalla et al, then the security of the UF-NMA scheme is tightly based on the hardness of distinguishing regular and lossy public keys of the identification scheme. The latter distinguishing problem is normally exactly the definition of some presumably-hard mathematical problem. The combination of these components gives the main result.

As a concrete instantiation of this framework, the recent lattice-based Dilithium

digital signature scheme [DKL⁺18] by Ducas et al., is modified, so that its underlying identification scheme admits lossy public keys. The original Dilithium scheme, which is proven secure in the classical ROM based on standard lattice assumptions, has 1.5KB public keys and 2.7KB signatures. The new scheme, which is tightly based on the hardness of the Module-LWE problem in the QROM using the generic reductions, has 7.7KB public keys and 5.7KB signatures for the same security level. Furthermore, due to the proof of equivalence shown in this work between the UF-NMA and UF-CMA security notions of deterministic signature schemes, one can formulate a new non-interactive assumption under which the original Dilithium signature scheme is also tightly secure in the QROM.

Security of the Fiat-Shamir Transformation in the Quantum Random-Oracle Model. The famous Fiat-Shamir transformation turns any public-coin three-round interactive proof, i.e., any so-called sigma-protocol, into a non-interactive proof in the random-oracle model.

In this work, this transformation is studied in the setting of a quantum adversary that in particular may query the random oracle with quantum superpositions. The main result is a generic reduction that transforms any quantum dishonest prover attacking the Fiat-Shamir transformation in the quantum random-oracle model into a similarly successful quantum dishonest prover attacking the underlying sigma-protocol (in the standard model). Applied to the standard soundness and proof-of-knowledge definitions, this reduction implies that both these security properties, in both the computational and the statistical variant, are preserved under the Fiat-Shamir transformation even when allowing quantum attacks. This result improves and completes the partial results that have been known so far, but it also proves wrong certain claims made in the literature.

In the context of post-quantum secure signature schemes, this results imply that for any sigma-protocol that is a proof-of-knowledge against quantum dishonest provers (and that satisfies some additional natural properties), the corresponding Fiat-Shamir signature scheme is secure in the quantum random-oracle model.

Generic Authenticated Key Exchange in the Quantum Random Oracle Model.

In this work, FO_{AKE} , as a generic construction of two-message authenticated key exchange (AKE) from any passively secure public key encryption (PKE) in the QROM, is proposed. Whereas previous AKE constructions relied on a Diffie-Hellman key exchange or required the underlying PKE scheme to be perfectly correct, this transformation allows arbitrary PKE schemes with non-perfect correctness. Dealing with imperfect schemes is one of the major difficulties in a setting involving active attacks. This direct construction, when applied to schemes such as the submissions to the recent NIST post-quantum competition, is more natural than previous AKE transformations. Furthermore, this work avoids the use of (quantum-secure) digital signature schemes which are considerably less efficient than their PKE counterparts. As a consequence, one can instantiate this AKE transformation with any of the submissions to the recent NIST competition, e.g., ones based on codes and lattices. FO_{AKE} can be seen as a generalization of the Fujisaki-Okamoto transformation [FO99] (for building actively secure PKE from passively secure PKE) to the AKE setting. As a helper result, a security proof is also provided for the Fujisaki-Okamoto transformation in the QROM for PKE with non-perfect correctness. This work fixes several gaps in a previous proof in [JZC⁺18] by Jiang et al, is tighter, and tolerates a larger correctness error.

3.4 Current results on reductions

In the aspect of reduction among lattice problems and related computational problems, we have 4 publications in top-tier conferences. The work [RSW18] studies variants of the ring and polynomial LWE problems, and exhibits reductions to show equivalence between them for many cases. Later the result [BP18] further generalizes RLWE problem and propose the Order-LWE problem, to study the hardness of RLWE with secret from different distributions. Motivated by gaining security as well as efficiency, the work [BBD⁺19] proposes a variant of LWE without Gaussian noise but with potential more hardness (called MPCLWR, short for middle-product computational learning with rounding), and prove its usability by constructing a public key encryption based on it. Last the work [BLVW19] successfully provides a worst-case to average-case reduction for LPN with some specific parameters.

On the Ring-LWE and Polynomial-LWE Problems. The RLWE problem comes in various forms. Vanilla RLWE is the decision dual-RLWE variant, consisting in distinguishing from uniform a distribution depending on a secret belonging to the dual \mathcal{O}_K^\vee of the ring of integers \mathcal{O}_K of a specified number field K . In primal-RLWE, the secret instead belongs to \mathcal{O}_K . Both decision dual-RLWE and primal-RLWE enjoy search counterparts. Also widely used is (search/decision) PLWE, which is not defined using a ring of integers \mathcal{O}_K of a number field K but a polynomial ring $\mathbb{Z}[x]/f$ for a monic irreducible $f \in \mathbb{Z}[x]$.

In this work, it is shown that there exist reductions between all of these six problems that incur limited parameter losses (also refer to Figure 3 for an illustration of their relations as well as the connections between these six problems with other computational problems such as MP-LWE and lattice problems such as ApproxSVP in ideal lattices). More precisely, this work: first shows that the (decision/search) dual to primal reduction from Lyubashevsky et al [LPR10] and Peikert [Pei16] can be implemented with a small error rate growth for all rings (the resulting reduction is non-uniform polynomial time); then extends it to polynomial-time reductions between (decision/search) primal RLWE and PLWE that work for a family of polynomials f that is exponentially large as a function of $\deg f$ (the resulting reduction is also non-uniform polynomial time); lastly exploits the recent technique from Peikert et al [PRS17a] to obtain a search to decision reduction for RLWE for arbitrary number fields. The reductions incur error rate increases that depend on intrinsic quantities related to K and f .

Order-LWE and the Hardness of Ring-LWE with Entropic Secrets. In this work, a generalization of the celebrated RLWE problem [LPR10] is proposed, wherein the ambient ring is not the ring of integers of a number field, but rather an order (a full rank subring). This work shows that Order-LWE problem enjoys worst-case hardness with respect to short vector problems in invertible ideal lattices of the order. The definition allows us to provide a new analysis for the hardness of the abundantly used PLWE problem [SSTX09], different from the one recently proposed by Rosca, Stehlé and Wallet [RSW18]. This result suggests that Order-LWE may be used to analyze and possibly design useful relaxations of RLWE. This work shows that Order-LWE can naturally be harnessed to prove security for RLWE instances where the “RLWE secret” (which often corresponds to the secret-key of a cryptosystem) is not sampled uniformly as required for RLWE hardness. Concretely, in this work, the worst-case hardness is shown even if the secret is sampled from a subring of the sample space.

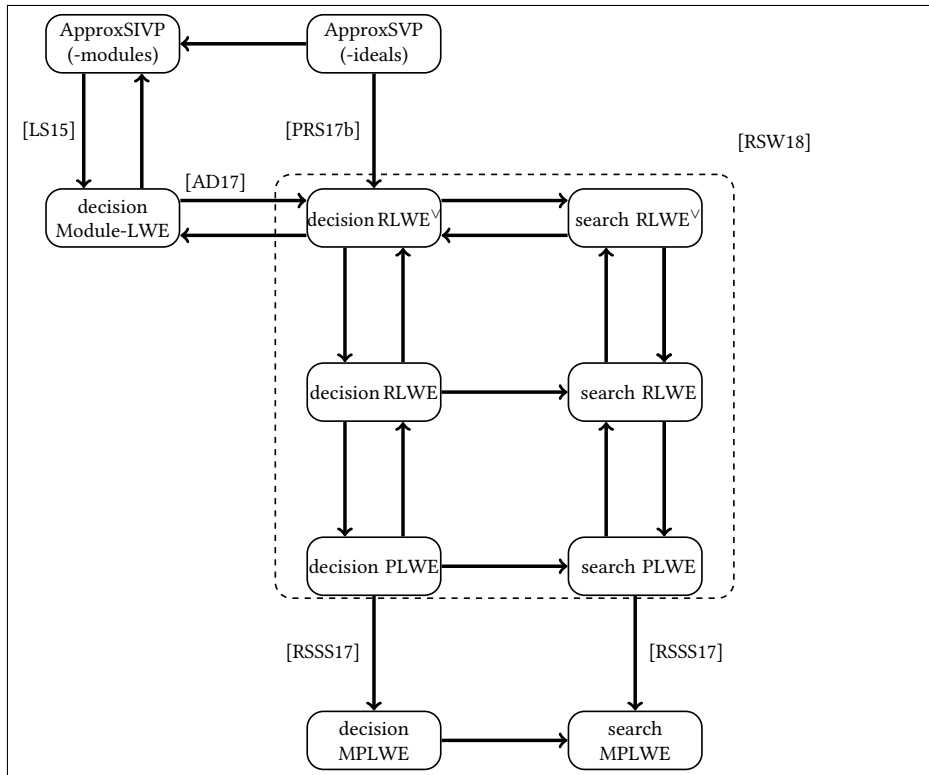


Figure 3: Relationships between variants of RLWE and PLWE. The dotted box contains the problems studied in this work. Each arrow may hide a noise rate degradation (and module rank - modulus magnitude transfer in the case of [AD17]). The top to bottom arrows in the dotted box correspond to non-uniform reductions. The reductions involving PLWE are analyzed for limited family of defining polynomials. The arrows without references correspond to trivial reductions.

Then, the case where the secret is sampled from an ideal of the sample space or a coset thereof (equivalently, some of its CRT coordinates are fixed or leaked), is well studied. for the latter, an interesting threshold phenomenon is presented, where the amount of RLWE noise determines whether the problem is tractable. Lastly, the long standing question of whether high-entropy secret is sufficient for RLWE to be intractable, is addressed. This result on sampling from ideals shows that simply requiring high entropy is insufficient. Finally, a broad class of distributions is proposed where we conjecture that hardness should hold, and provides evidence via reduction to a concrete lattice problem.

Middle-Product Learning with Rounding Problem and its Applications. At CRYPTO 2017, Rosca et al. introduce a new variant of the LWE problem, called the MP-LWE. The hardness of this new assumption is based on the hardness of the PLWE problem parameterized by a set of polynomials, making it more secure against the possible weakness of a single defining polynomial. As a cryptographic application, they also provide an encryption scheme based on the MP-LWE problem.

In this work, a deterministic variant of their encryption scheme is proposed, which does not need Gaussian sampling and is thus simpler than the original one. Still, it has

the same quasi-optimal asymptotic key and ciphertext sizes. The main ingredient for this purpose is the LWR problem which has already been used to derandomize LWE type encryption. The hardness of this new scheme is based on a new assumption called MPCLWR, an adaptation of the computational LWR problem over rings, introduced by Chen et al [CZZ18]. Finally, this new assumption is proved to be as hard as the decisional version of MP-LWE and thus benefits from worst-case to average-case hardness guarantees.

Worst-Case Hardness for LPN and Cryptographic Hashing via Code Smoothing. In this work, a worst-case decoding problem is proposed, whose hardness reduces to that of solving the LPN problem, in some parameter regime. Prior to this work, no worst case hardness result was known for LPN (as opposed to syntactically similar problems such as LWE). The caveat is that this worst case problem is only mildly hard and in particular admits a quasi-polynomial time algorithm, whereas the LPN variant used in the reduction requires extremely high noise rate of $1/2 - 1/\text{poly}(n)$. Thus this work can only show that “very hard” LPN is harder than some “very mildly hard” worst case problem. Specifically, this work considers the (n, m, w) -nearest codeword problem ((n, m, w) -NCP) which takes as input a generating matrix for a binary linear code in m dimensions and rank n , and a target vector which is very close to the code (Hamming distance at most w), and asks to find the codeword nearest to the target vector. This work shows that for balanced (unbiased) codes and for relative error $w/m \approx \log^2 n/n$, (n, m, w) -NCP can be solved given oracle access to an LPN distinguisher with noise ratio $1/2 - 1/\text{poly}(n)$. The proof in this work relies on a smoothing lemma for codes which has further implications: (n, m, w) -NCP with the aforementioned parameters lies in the complexity class Search-BPPSZK (i.e. reducible to a problem that has a statistical zero knowledge protocol) implying that it is unlikely to be NP-hard. Eventually, this work shows that LPN with very low noise rate $\log^2(n)/n$ implies the existence of collision resistant hash functions (in this parameter regime LPN is also in BPPSZK).

3.5 Conclusion

With respect to the concrete targets within TASK 3.1, we have a fairly good progress and numerous results. Within this subtask, we already have an extensive study on the underlying hardness assumptions as well as the security model under both classical and quantum computation. First, with respect to the security model, we have efficiently transformed prior schemes with security under classical model to the ones with almost the same security level, but now under the quantum setting. These transformations will eventually be used for our design of either building blocks in WP4 or privacy-preserving protocols in WP5. Second for the underlying hardness assumptions, we have established and improved the relations between known presumed hard problems and proposed new ones with better properties.

4 TASK 3.2: Algorithm design and implementation of lattice trapdoors

We will now review the targets and summarize the results obtained within TASK 3.2.

4.1 Review of the targets

Table 4 presents the targets of TASK 3.2. The main objective is to provide highly efficient solutions for our building blocks in WP4 and related privacy preserving schemes in WP5 and their implementation. First, we want to improve the parameters of lattice-based schemes. One of the starting point would be to try more efficient underlying structured lattice or apply other metrics such as Rényi divergence for lattice-based cryptography [BLL⁺15]. Next, we need to optimize the lattice trapdoor, i.e., resort to partial trapdoor whenever it is possible. Second, we also need to find other possible enhancement on both efficiency and security. For efficiency, we would like to remove or mitigate the floating-point arithmetic in Gaussian sampling. To do more, it is also more desirable to take security with respect to side-channel attacks into consideration within the design paradigm of Gaussian sampling.

Targets	Concrete contents
Investigate improvement for setting parameters	Tighten parameters using more structured lattices and statistical tools
	Resort to partial trapdoors when possible
Study on other enhancement	Remove or mitigate Floating-Point arithmetic in Gaussian sampling
	Enhanced security (e.g., against side-channel attacks) together with high efficiency

Table 4: Concrete targets within TASK 3.2.

4.2 Overview of current results

An overview of the results obtained in TASK 3.2 can be found in Table 5.

4.3 Current results on applying more efficient structures

In the scope of applying more efficient structure, we have 2 publications in conferences. The work [BFRS18] proposes an efficient implementation of lattice-based signature and IBE based on the RLWE and RSIS problems in the standard model, while other schemes used the NTRU assumption for efficiency reasons. Then another contribution [PP19] works out a recursive algorithm for NTRU key generation by exploiting the tower of subfields in cyclotomic fields. This work substantially improves the performance of the trapdoor generation of the Falcon scheme (second-round PQC NIST candidate).

Practical Implementation of Ring-SIS/LWE Based Signature and IBE. Lattice-based signature and Identity-Based Encryption (IBE) are well-known cryptographic schemes, and having both efficient and provably secure schemes in the standard model is still a challenging task in light of the current NIST post-quantum competition.

Category	Work	Status
More efficient structures	Practical Implementation of Ring-SIS/LWE Based Signature and IBE [BFRS18]	PQCrypto 2018
	More Efficient Algorithms for the NTRU Key Generation using the Field Norm [PP19]	PKC 2019
Gaussian sampling	CDT-Based Gaussian Sampling: From Multi to Double Precision [MR18]	IEEE TC
	Integral Matrix Gram Root and Lattice Gaussian Sampling without Floats [DGPY19]	Preprint
	GALACTICS: Gaussian Sampling for Lattice-Based Constant-Time Implementation of Cryptographic Signatures, Revisited [BBE ⁺ 19]	ACM CCS

Table 5: Current (intermediate) results on TASK 3.2.

In this work, provably secure (in the standard model) and efficient signature and IBE are constructed, by mixing standard IBE scheme, à la ABB (EUROCRYPT 2010) on RSIS/RLWE assumptions with the efficient trapdoor of Micciancio and Peikert [MP12] to provide an efficient implementation. The proposed IBE scheme is more efficient than the IBE scheme [DLP14] by Ducas, Lyubashevsky and Prest based on NTRU assumption and is based on more standard assumptions. Finally, an efficient implementation together with a formal proof in the standard model is also given for the underlying signature scheme.

More Efficient Algorithms for the NTRU Key Generation using the Field Norm.

NTRU lattices [HPS98] are a class of polynomial rings which allow for compact and efficient representations of the lattice basis, thereby offering very good performance characteristics for the asymmetric algorithms that use them. Signature algorithms based on NTRU lattices have fast signature generation and verification, and relatively small signatures, public keys and private keys. A few lattice-based cryptographic schemes entail, generally during the key generation, solving the NTRU equation:

$$fG - gF = q \text{ mod } x^n + 1,$$

where f and g are fixed. The goal is to compute solutions F and G to the equation, and all the polynomials are in $\mathbb{Z}[x]/(x^n + 1)$. The existing methods for solving this equation are quite cumbersome: their time and space complexities are at least cubic and quadratic in the dimension n , and for typical parameters they therefore require several megabytes of RAM and take more than a second on a typical laptop, precluding onboard key generation in embedded systems such as smart cards.

In this work, two new algorithms are presented for solving the NTRU equation. Both algorithms make a repeated use of the field norm in tower of fields; it allows them to be faster and more compact than existing algorithms by factors $\tilde{O}(n)$. For lattice-based schemes considered in practice, this reduces both the computation time and RAM usage by factors at least 100, making key pair generation within range of smart card abilities.

4.4 Current results on Gaussian sampling

Concerning the optimization of Gaussian sampling algorithms, we achieved 3 publications: 1 in conference, 1 in journal and 2 in preprints. Further work on Rényi divergence [MR18] shows that doubling the precision is sufficient for usual lattice-based signatures by using a modified cumulative distribution table (CDT). Further the work [DGPY19] proposes new techniques to avoid floating point computation during the linear algebra step of lattice trapdoor sampling. These techniques are based on a generalization of the 4-square theorem to matrices. Eventually in [BBE⁺19], we propose new techniques for approximating Gaussian sampling achieving constant time and without floating points arithmetic (FPA), by resorting to lattice reduction for approximating transcendental functions by integral polynomials. This work also permits masked implementation of BLISS [DDLL13].

CDT-Based Gaussian Sampling: From Multi to Double Precision. The Rényi divergence is a measure of closeness of two probability distributions which has found several applications over the last years as an alternative to the statistical distance in lattice-based cryptography. A tight bound has recently been presented for the Rényi divergence of distributions that have a bounded relative error.

In this work, the Rényi divergence is used to bound the precision requirement in Gaussian sampling to the IEEE 754 floating-point standard double precision for usual lattice-based signature parameters by using a modified cumulative distribution table (CDT), which reduces the memory needed by CDT-based algorithms and, makes their constant time implementation faster and simpler. Then, this approach is applied to a variable-center variant of the CDT algorithm which occasionally requires the online computation of the cumulative distribution function. As a result, the amount of floating-point operations is drastically decreased, which makes the constant-time and cache-resistant variants of this algorithm viable and efficient. Finally, some experimental results are provided to indicate that comparing to rejection sampling, the proposed approach increases the GPV signature rate by a factor 4 to 8 depending on the security parameter.

Integral Matrix Gram Root and Lattice Gaussian Sampling without Floats. Many advanced lattice based cryptosystems require to sample lattice points from Gaussian distributions. One challenge for this task is that all current algorithms resort to floating-point arithmetic (FPA) at some point, which has numerous drawbacks in practice: it requires numerical stability analysis, extra storage for high-precision, lazy/backtracking techniques for efficiency, and may suffer from weak determinism which can completely break certain schemes.

In this work, techniques are given to implement Gaussian sampling over general lattices without using FPA. To this end, the approach of Peikert is also revisited, using perturbation sampling. Peikert's approach uses the Cholesky decomposition $\Sigma = \mathbf{A}\mathbf{A}^t$

of the target covariance matrix Σ , giving rise to a square matrix \mathbf{A} with real (not integer) entries. The new proposed idea, in a nutshell, is to replace this decomposition by an integral one. While there is in general no integer solution if one restricts \mathbf{A} to being a square matrix, it is shown that such a decomposition can be efficiently found by allowing \mathbf{A} to be wider (say $n \times 9n$). This can be viewed as an extension of Lagrange’s four-square theorem to matrices. In addition, the proposed integral decomposition algorithm is further adapted to the ring setting: for power-of-2 cyclotomics, the tower of rings structure can be exploited to improve the complexity and compactness.

GALACTICS: Gaussian Sampling for Lattice-Based Constant-Time Implementation of Cryptographic Signatures, Revisited. In this work, a constant-time implementation is proposed for the BLISS lattice-based signature scheme [DDL13]. BLISS is possibly the most efficient lattice-based signature scheme proposed so far, with a level of performance on par with widely used pre-quantum primitives like ECDSA. It is one of the few postquantum signatures to have seen real-world deployment, as part of the strongSwan VPN software suite.

The outstanding performance of the BLISS signature scheme stems in large part from its reliance on discrete Gaussian distributions, which allow for better parameters and security reductions. However, that advantage has also proved to be its Achilles’ heel, as discrete Gaussians pose serious challenges in terms of secure implementations. Implementations of BLISS so far have included secret-dependent branches and memory accesses, both as part of the discrete Gaussian sampling and of the essential rejection sampling step in signature generation. These defects have led to multiple devastating timing attacks, and were a key reason why BLISS was not submitted to the NIST postquantum standardization effort. In fact, almost all of the actual candidates chose to stay away from Gaussians despite their efficiency advantage, due to the serious concerns surrounding implementation security. Moreover, naive countermeasures will often not cut it: it is shown that a reasonable-looking countermeasure suggested in previous work to protect the BLISS rejection sampling can again be defeated using novel timing attacks, in which the timing information is fed to phase retrieval machine learning algorithm in order to achieve a full key recovery. Fortunately, careful implementation techniques are also presented that allow to describe an implementation of BLISS with complete timing attack protection, achieving the same level of efficiency as the original unprotected code, without resorting on floating point arithmetic or platform-specific optimizations like AVX intrinsics. These techniques, including a new approach to the polynomial approximation of transcendental function, can also be applied to the masking of the BLISS signature scheme, and will hopefully make more efficient and secure implementations of lattice-based cryptography possible going forward.

4.5 Conclusion

With respect to our concrete targets within TASK 3.2, we have progressed well and obtained many results so far. Within this subtask, we have investigated many directions to achieve more efficient lattice-based cryptographic schemes, which will eventually serve for our purpose in this project. First, we have tried to apply more efficient structures in the implementation of lattice-based schemes. These more efficient structures can serve as important candidates for our need in WP4 and 5. Second, we have performed an extensive study for optimizing the Gaussian sampling by either reducing or removing the need of floating-point arithmetic. Hopefully, the basic tools

developed can be used to greatly improve the efficiency of our building blocks as well as privacy-preserving schemes.

5 TASK 3.3: Classical and quantum cryptanalysis

We will first recall the targets and summarize the results obtained so far within TASK 3.3.

5.1 Review of the targets

Table 6 presents the targets of TASK 3.3. The main objective is to investigate and improve the state-of-the-art (quantum and classical) algorithms for cryptanalysis, which will be used to choose parameters in the building blocks in WP4 and the privacy-preserving protocols in WP5. From the quantum cryptanalysis point of view, it is important to extend currently known attacks for hard problems in ideal lattices to more general structured lattice, such as module lattices. Next, as it will always increase the physical difficulty of maintaining a larger entanglement of qubits, it is also important to evaluate or improve the concrete number of qubits required in the quantum algorithms. We also need to investigate the quantum version of best classical algorithms and their quantum implementations. From classical cryptanalysis aspect, we have a large family of cryptanalysis algorithms (the sieve, the enumeration and the BKZ algorithm). The first question is whether we can improve or hybridize them. So far, the cost model for the cryptanalysis algorithm is based on the arithmetic operations count. To have a more exact cost model, one may need to consider more realistic factor in real implementation such as the size of RAM and circuit needed. The final target is to derive security models for reliable security estimates and to develop automated tools for generating parameters.

Targets	Concrete contents
Cryptanalysis with quantum computation	Extend known attacks to more structured lattices
	Evaluate and improve number of required qubits
	Generalize classical algorithm to quantum setting
Cryptanalysis with classical computation	Improve and hybridize known algorithms (Sieve, Enum, BKZ)
	Use more realistic cost models (RAM, Circuit)
	Reliable security estimates, automated parameter selection
Cryptanalysis on NIST candidates	They include both first and second round candidates

Table 6: Concrete targets within TASK 3.3.

5.2 Overview of current results

An overview of the results obtained in TASK 3.3 can be found in Table 7.

Category	Work	Status
Quantum cryptanalysis	Quantum Algorithms for the Approximate k -List Problem and their Application to Lattice Sieving [KMPM19]	Eurocrypt 2019
	Quantum speedups for lattice sieves are tenuous at best [AGPS19]	Preprint
	On the Quantum Complexity of the Continuous Hidden Subgroup Problem [dBDF19]	Preprint
	On the Shortness of Vectors to be found by the Ideal-SVP Quantum Algorithm [DPW19]	Crypto 2019
	Approx-SVP in Ideal Lattices with Pre-processing [PHS19]	Eurocrypt 2019
	An LLL Algorithm for Module Lattices [LPSW19]	Asiacrypt 2019
Classical cryptanalysis	Measuring, simulating and exploiting the head concavity phenomenon in BKZ [BSW18]	Asiacrypt 2018
	Shortest Vector from Lattice Sieving: a Few Dimensions for Free [Duc18]	Eurocrypt 2018
	The General Sieve Kernel and New Records in Lattice Reduction [ADH ⁺ 19]	Eurocrypt 2019
	Exploring Trade-offs in Batch Bounded Distance Decoding [ACW19]	Preprint
	A refined analysis of the cost for solving LWE via uSVP [BMW19]	Africacrypt 2019
Cryptanalysis on NIST candidates	Estimate all the LWE, NTRU schemes! [ACD ⁺ 18]	SCN 2018
	Attacks on the AJPS Mersenne-based cryptosystem [dBDJdW18]	PQCrypto 2018
	Learning Strikes Again: the Case of the DRS Signature Scheme [YD18]	Asiacrypt 2018

Table 7: Current (intermediate) results on TASK 3.3.

5.3 Current results on quantum cryptanalysis

We got 6 publications on quantum cryptanalysis: 4 in top-tier conferences and 2 preprints. First, we try to generalize classical algorithms for cryptanalysis to the quantum setting. The result [KMPM19] generalizes the classical k -list algorithm [HKL18] to the quantum setting, to get an improvement on both time and space cost for solving SVP, together with a detailed analysis of the size of quantum circuit needed. To

have a better understanding on the quantum version of sieve for solving SVP, the work [AGPS19], shows that the performance of quantum implementation of the near neighbor search algorithm, as a core part for sieve algorithm, does not differ a lot from the classical implementation, with a non-asymptotic analysis. Second, we tried to have a better understanding on the state-of-the-art algorithms for solving SVP over ideal lattices under quantum computation. In [dBDF19], the authors give a complete proof for the correctness and efficiency of the polynomial-time quantum algorithm for solving the continuous HSP [EHKS14], which is a core component of the state-of-the-art solver for SVP over ideal lattices [CDPR16]. Furthermore in [DPW19], the expected output quality of the same quantum algorithm [CDW17] above for finding short vectors in cyclotomic ideal lattices is formally quantified. The work also concludes on when to expect those algorithms to become relevant compared to standard LLL and BKZ. Moreover, we also make an improvement over the state-of-the-art SVP solver algorithm over ideal lattices. The work [PHS19] generalizes the above quantum attack to all number fields, and provides new trade-offs between time and approximation factor. The algorithm requires some preprocessing depending on the field only, and up to this preprocessing, it outperforms prior algorithms [CDPR16, CDW17] for diverse parameters. Last, we also extend algorithms for Euclidean lattices with less structure to lattices with more structure. In [LPSW19], the authors propose a way to compute an LLL algorithm over module lattices in a cyclotomic number field. The main drawback is the need for an exact-CVP oracle.

Quantum Algorithms for the Approximate k -List Problem and their Application to Lattice Sieving. The SVP is one of the mathematical foundations of lattice based cryptography. Lattice sieve algorithms are among the foremost methods for solving SVP. The asymptotically fastest known classical and quantum sieves solve SVP in a d -dimensional lattice in $2^{cd+o(d)}$ time steps with $2^{c'd+o(d)}$ memory for small constants c, c' .

In this work, various quantum sieving algorithms are given that trade computational steps for memory. First, a quantum analogue of the classical k -Sieve algorithm [HKL18] is given, in the Quantum Random Access Memory (QRAM) model, achieving an algorithm that heuristically solves SVP in $2^{0.2989d+o(d)}$ time steps using $2^{0.1395d+o(d)}$ memory. This should be compared to the state-of-the-art algorithm [Laa15], which, in the same model, solves SVP in $2^{0.2653d+o(d)}$ time steps and memory. In the QRAM model these algorithms can be implemented using $poly(d)$ width quantum circuits. Secondly, the k -Sieve is framed as the problem of k -clique listing in a graph and apply quantum k -clique finding techniques to the k -Sieve. Finally, the large quantum memory regime is explored by adapting parallel quantum search [BBG⁺13] by Beals et al to the 2-Sieve and giving an analysis in the quantum circuit model. It is also shown how to heuristically solve SVP in $2^{0.1037d+o(d)}$ time steps using $2^{0.2075d+o(d)}$ quantum memory.

Quantum speedups for lattice sieves are tenuous at best. Quantum variants of lattice sieve algorithms are often used to assess the security of lattice based cryptographic constructions.

In this work, a heuristic and non-asymptotic analysis of the cost of several algorithms for near neighbor search on high dimensional spheres, is provided. These algorithms are used in lattice sieves. First, quantum circuits are designed for near neighbor algorithms and software is provided that numerically optimises algorithm

parameters according to various cost metrics. Then, using this software, an estimate is obtained for the cost of classical and quantum near neighbor search on spheres. Finally, it is found that quantum search may provide a small speedup in dimensions of cryptanalytic interest, but only under exceedingly optimistic physical and algorithmic assumptions.

On the Quantum Complexity of the Continuous Hidden Subgroup Problem.

The Hidden Subgroup Problem (HSP) aims at capturing all problems that are susceptible to be solvable in quantum polynomial time following the blueprints of Shor’s celebrated algorithm. Successful solutions to these problems over various commutative groups allow to efficiently perform number-theoretic tasks such as factoring or finding discrete logarithms. The latest successful generalization by Eisentrager et al [EHKS14] considers the problem of finding a full-rank lattice as the hidden subgroup of the continuous vector space \mathbb{R}^m , even for large dimensions m . It unlocked new cryptanalytic algorithms by Biasse and Song [BS16], Cramer et al [CDPR16, CDW17], in particular to find mildly short vectors in ideal lattices. The cryptanalytic relevance of such a problem raises the question of a more refined and quantitative complexity analysis. In the light of the increasing physical difficulty of maintaining a large entanglement of qubits, the degree of concern may be different whether the above algorithm requires only linearly many qubits or a much larger polynomial amount of qubits.

In this work, a detailed analysis of (a variation of) the aforementioned HSP algorithm is given, together with a conclusion on its complexity as a function of all the relevant parameters. Incidentally, this work also clarifies certain claims from the extended abstract of Eisentrager et al.

On the Shortness of Vectors to be found by the Ideal-SVP Quantum Algorithm.

The hardness of finding short vectors in ideals of cyclotomic number fields (hereafter, Ideal-SVP) can serve as a worst-case assumption for numerous efficient cryptosystems, via the average-case problems RSIS and RLWE. For a while, it could be assumed the Ideal-SVP problem was as hard as the analog problem for general lattices (SVP), even when considering quantum algorithms. But in the last few years, a series of works has lead to a quantum algorithm for Ideal-SVP that outperforms what can be done for general SVP in certain regimes. More precisely, it was demonstrated (under certain hypotheses) that one can find in quantum polynomial time a vector longer by a factor at most $\alpha = \exp(\tilde{O}(n^{1/2}))$ than the shortest non-zero vector in a cyclotomic ideal lattice, where n is the dimension.

In this work, the constants hidden behind this asymptotic claim are explored. While these algorithms have quantum steps, the steps that impact the approximation factor α are entirely classical, which allows us to estimate it experimentally using only classical computing. Moreover, heuristic improvements are designed for those steps that significantly decrease the hidden factors in practice. Finally, new provable effective lower bounds are derived based on volumetric arguments. This study allows to predict the crossover point with classical lattice reduction algorithms, and thereby determine the relevance of this quantum algorithm in any cryptanalytic context. For example, this result predicts that this quantum algorithm provides shorter vectors than BKZ-300 (roughly the weakest security level of NIST lattice-based candidates) for cyclotomic rings of rank larger than about 24000.

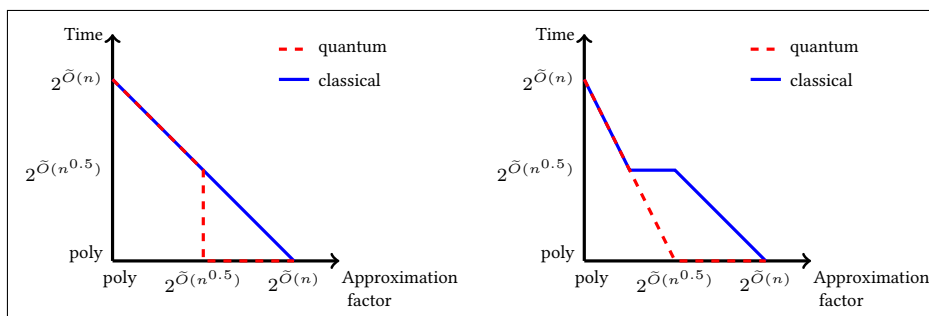


Figure 4: Prior (left) and new (right) trade-offs for ideal approx-SVP in the same fields (with a pre-processing of cost $\exp(\tilde{O}(n))$).

Approx-SVP in Ideal Lattices with Pre-processing. In this work, an algorithm to solve the approximate SVP for lattices corresponding to ideals of the ring of integers of an arbitrary number field K is described. This algorithm has a pre-processing phase, whose run-time is exponential in $\log |\Delta|$ with Δ the discriminant of K . Importantly, this pre-processing phase depends only on K . The pre-processing phase outputs an advice, whose bit-size is no more than the run-time of the query phase. Given this advice, the query phase of the algorithm takes as input any ideal I of the ring of integers, and outputs an element of I which is at most $\exp(\tilde{O}((\log |\Delta|)^{\alpha+1}/n))$ times longer than a shortest non-zero element of I (with respect to the Euclidean norm of its canonical embedding). This query phase runs in time and space $\exp(\tilde{O}((\log |\Delta|)^{\max(2/3, 1-2\alpha)}))$ in the classical setting, and $\exp(\tilde{O}((\log |\Delta|)^{1-2\alpha}))$ in the quantum setting. The parameter α can be chosen arbitrarily in $[0, 1/2]$. Both correctness and cost analyses rely on heuristic assumptions, whose validity is consistent with experiments. The algorithm builds upon the algorithms from Cramer et al [CDPR16] and Cramer et al [CDW17]. It relies on the framework from Buchmann [Rog88], which allows to merge them and to extend their applicability from prime-power cyclotomic fields to all number fields. The cost improvements are obtained by allowing precomputations that depend on the field only (also see Figure 4 for an illustration of the improvement).

An LLL Algorithm for Module Lattices. The LLL algorithm [DDL13] takes as input a basis of a Euclidean lattice, and, within a polynomial number of operations, it outputs another basis of the same lattice but consisting of rather short vectors.

In this work, a generalization to R -modules contained in K^n for arbitrary number fields K and dimension n is provided, with R denoting the ring of integers of K . Concretely, an algorithm is introduced which efficiently finds short vectors in rank- n modules when given access to an oracle that finds short vectors in rank-2 modules, and an algorithm that efficiently finds short vectors in rank-2 modules given access to a CVP oracle for a lattice that depends only on K . The second algorithm relies on quantum computations and its analysis is heuristic.

5.4 Current results on classical cryptanalysis

We got 5 articles about classical cryptanalysis: 4 in conferences and 1 preprint. As for the first part, we try to have a better understanding of classical lattice reduction algorithms. In [BSW18], the authors give a probabilistic simulator that better fits the practical behavior of the BKZ algorithm. Furthermore, we try to improve classical

algorithms. As one of the big news in 2018, in [Duc18], a sub-exponential speed-up for finding the shortest vector via sieving has been achieved, which greatly enlarge the cross-over point with the enumeration algorithm. Based on the breakthrough works such as [Duc18] and [LM18], the work [ADH⁺19] represents another major news in the area from 2019, by achieving new SVP records (up to dimension around 150) using an open source sieving implementation [dt16]. Then we also study the capability of enumeration and sieving algorithms for concrete applications. The work [ACW19] shows that when dealing with a batch of BDD instances for a given lattice, the enumeration algorithm is more efficient than sieving algorithms. Finally, in order to have a better understanding on the state-of-the-art cost estimator for solving LWE [ADPS16, AGVW17] (that helps for parameter selection), [BMW19] provides many experiments to evaluate the accuracy of this cost estimator, together with more evidence confirming the assumptions used.

Measuring, simulating and exploiting the head concavity phenomenon in BKZ. The BKZ lattice reduction algorithm is central in cryptanalysis, in particular for lattice-based cryptography. A precise understanding of its practical behavior in terms of run-time and output quality is necessary for parameter selection in cryptographic design. As the provable worst-case bounds poorly reflect the practical behavior, cryptanalysts rely instead on the heuristic BKZ simulator of Chen and Nguyen [CN11]. It fits better with practical experiments, but not entirely. In particular, it over-estimates the norm of the first few vectors in the output basis. In a nutshell, BKZ performs better than its Chen-Nguyen simulation, which is a bad news for parameter selection.

In this work, first, experiments are reported for providing more insight on this shorter-than-expected phenomenon. Second, a refined BKZ simulator is proposed by taking the distribution of short vectors in random lattices into consideration. Third, according to the experiments, this refined simulator more accurately predicts the concrete behavior of BKZ. Furthermore, a new BKZ variant is designed to exploit the shorter-than-expected phenomenon. For the same cost assigned to the underlying SVP-solver, the new BKZ variant produces bases of better quality. Its potential impact is also further illustrated by testing it on the SVP-120 instance of the Darmstadt lattice challenge.

Shortest Vector from Lattice Sieving: a Few Dimensions for Free. Asymptotically, the best known algorithms for solving the SVP in a lattice of dimension n are sieve algorithms, which have heuristic complexity estimates ranging from $(4/3)^{n+o(n)}$ to $(3/2)^{n/2+o(n)}$ when Locality Sensitive Hashing techniques are used. Sieve algorithms are however outperformed by pruned enumeration algorithms in practice by several orders of magnitude, despite the larger super-exponential asymptotical complexity $2^{\theta(n \log n)}$ of the latter.

In this work, a concrete improvement of sieve-type algorithms is shown. Precisely, it is shown that a few calls to the sieve algorithm in lattices of dimension less than $n - d$ solves SVP in dimension n , where $d = \theta(n/\log n)$. Although the improvement is only sub-exponential, its practical effect in relevant dimensions is quite significant. An implementation is given for it over a simple sieve algorithm with $(4/3)^{n+o(n)}$ complexity, and it outperforms the best sieve algorithms from the literature by a factor of 10 in dimensions 70-80. It performs less than an order of magnitude slower than pruned enumeration in the same range. By design, this improvement can also be applied to most other variants of sieve algorithms, including LSH sieve algorithms and

tuple-sieve algorithms. In this light, one may expect sieve-techniques to outperform pruned enumeration in practice in the near future.

The General Sieve Kernel and New Records in Lattice Reduction. In this work, the General Sieve Kernel (G6K) is proposed, as an abstract stateful machine supporting a wide variety of lattice reduction strategies based on sieving algorithms. Using the basic instruction set of this abstract stateful machine, first, concise formulations are given for previous sieving strategies from the literature and then new ones are also proposed. Then, a light variant of BKZ is given for exploiting the features of the proposed abstract stateful machine. This encapsulates several recent suggestions (Ducas at Eurocrypt 2018 [Duc18]; Laarhoven and Mariano at PQCrypto 2018 [LM18]) to move beyond treating sieving as a blackbox SVP oracle and to utilise strong lattice reduction as preprocessing for sieving. Furthermore, new tricks are proposed to minimise the sieving computation required for a given reduction quality with mechanisms such as recycling vectors between sieves, on-the-fly lifting and flexible insertions akin to Deep LLL and recent variants of Random Sampling Reduction. Moreover, a highly optimized, multi-threaded and tweakable implementation of this machine is provided, which we make open-source. Then, an illustration is given for the performance of this implementation of the proposed sieving strategies by applying G6K to various lattice challenges. In particular, our approach allows us to solve previously unsolved instances of the Darmstadt SVP (151, 153, 155) and LWE (e.g. (75, 0.005)) challenges. Our solution for the SVP-151 challenge was found 400 times faster than the time reported for the SVP-150 challenge, the previous record. For exact SVP, a performance crossover is observed between G6K and FPLLL’s state of the art implementation of enumeration at dimension 70.

Exploring Trade-offs in Batch Bounded Distance Decoding. Algorithms for solving the BDD are used for estimating the security of lattice-based cryptographic primitives, since these algorithms can be employed to solve variants of the LWE problem. In certain parameter regimes where the target vector is small and/or sparse, batches of BDD instances emerge from a combinatorial approach where several components of the target vector are guessed before decoding.

In this work, trade-offs are explored in solving “Batch-BDD”, and the proposed techniques are applied to the small-secret LWE problem. Then, the proposed techniques are also compared to previous works which solve batches of BDD instances, such as the hybrid lattice-reduction and meet-in-the-middle attack. Our results are a mixed bag. It is shown that, in the “enumeration setting” and with BKZ reduction, the proposed techniques outperform a variant of the hybrid attack which does not consider time-memory trade-offs in the guessing phase for certain Round5 (17-bits out of 466), Round5-IoT (19-bits out of 240), and NTRU LPrime (23-bits out of 385) parameter sets. On the other hand, the proposed techniques do not outperform the Hybrid Attack under standard, albeit unrealistic, assumptions. Finally, as expected, our techniques do not improve on previous works in the “sieving setting” (under standard assumptions) where combinatorial attacks in general do not perform well.

A refined analysis of the cost for solving LWE via uSVP. The LWE problem [Reg05] introduced by Regev is one of the fundamental problems in lattice-based cryptography. One standard strategy to solve the LWE problem is to reduce it to a uSVP problem via Kannan’s embedding and then apply a lattice reduction to solve the uSVP problem.

There are two methods for estimating the cost for solving LWE via this strategy: the first method considers the largeness of the gap in the uSVP problem [GN08] by Gama and Nguyen, and the second method [ADPS16] by Alkim et al., considers the shortness of the projection of the shortest vector to the Gram-Schmidt vectors. These two estimates have been investigated by Albrecht et al. [AGVW17] who present a sound analysis and show that the lattice reduction experiments fit more consistently with the second estimate. They also observe that in some cases the lattice reduction even behaves better than the second estimate perhaps due to the second intersection of the projected vector with the Gram-Schmidt vectors.

In this work, the work of Alkim et al. [ADPS16] and Albrecht et al. [AGVW17] are revisited. First, further experiments are reported for providing more comparisons and suggesting that the second estimate leads to a more accurate prediction in practice. Second, empirical evidence is presented for confirming the assumptions used in the second estimate. Furthermore, the gaps in uSVP derived from the embedded lattice is examined and used to explain why it is preferable to use $\mu = 1$ for the embedded lattice. This shows there is a coherent relation between the second estimate and the gaps in uSVP. Finally, it has been conjectured by Albrecht et al. that the second intersection will not happen for large parameters. It is shown in this work that this is indeed the case: there is no second intersection as $\beta \rightarrow \infty$.

5.5 Current results on cryptanalysis of NIST candidates

In 3 published papers, we propose cryptanalysis on some NIST candidates. As an important start, the work [ACD⁺18] provides a cross comparison of *all* lattice-based schemes submitted to the NIST PQC competition process under the assumptions in the respective submissions. On the other hand, we investigate the security of specific NIST candidates by exploiting their concrete structures, which eventually leads to reparametrization of those schemes. The work [dBDJdW18] shows that the first-round NIST candidate AJPS cryptosystem is not secure by proposing a quantum combinatorial attack and a classical lattice attack. In [YD18], the authors give an attack on the first-round NIST DRS signature scheme by exploiting the weakness of not having a Gaussian sampling for its key generation.

Estimate all the {LWE, NTRU} schemes! In this work, all LWE- and NTRU-based NIST PQC candidate schemes are considered, which include encryption, key encapsulation, and digital signature schemes. In particular, the impact is investigated that different estimates for the asymptotic runtime of (block-wise) lattice reduction have on the predicted security of these schemes. Relying on the “LWE estimator” of Albrecht et al., the cost is estimated for running primal and dual lattice attacks against every LWE-based scheme, using every cost model proposed as part of a submission. Furthermore, the security of the proposed NTRU-based schemes is also estimated against the same primal attack under all cost models for lattice reduction.

Attacks on the AJPS Mersenne-based cryptosystem. Aggarwal, Joux, Prakash and Santha recently introduced a new potentially quantum-safe public-key cryptosystem [AJPS18], and suggested that a brute-force attack is essentially optimal against it. They consider but then dismiss both Meet-in-the-Middle attacks and LLL-based attacks. Very soon after their paper appeared, Beunardeau et al. proposed a practical LLL-based technique that seemed to significantly reduce the security of the AJPS system.

In this work, there are two main results. First, it is shown that a Meet-in-the-Middle attack can also be made to work against the AJPS system, using locality-sensitive hashing to overcome the difficulty that Aggarwal et al. saw for such attacks. A quantum version of this attack is also provided. Second, a more precise analysis is given for the attack of Beunardeau et al., confirming and refining their results.

Learning Strikes Again: the Case of the DRS Signature Scheme. Lattice signature schemes generally require particular care when it comes to preventing secret information from leaking through signature transcript. For example, the NTRUSign scheme [HHP⁺03] and the Goldreich-Goldwasser-Halevi (GGH) signature scheme [GGH97] were completely broken by the parallelepiped-learning attack of Nguyen and Regev [NR06]. Several heuristic countermeasures were also shown vulnerable to similar statistical attacks. At PKC 2008, Plantard, Susilo and Win [PSW08] proposed a new variant of GGH, informally arguing resistance to such attacks. Based on this variant, Plantard, Sipasseuth, Dumondelle and Susilo proposed a concrete signature scheme, called DRS [PSDS], that has been accepted in the round 1 of the NIST post-quantum competition.

In this work, another statistical attack is proposed to demonstrate a weakness of the DRS scheme: one can recover some partial information of the secret key from sufficiently many signatures. One difficulty is that, due to the DRS reduction algorithm, the relation between the statistical leak and the secret seems more intricate. This difficulty is worked around by training a statistical model, using a few features that are designed according to a simple heuristic analysis. While partial information is recovered on the secret key, this information is easily exploited by lattice attacks, significantly decreasing their complexity. Concretely, it is shown that, provided that 100 000 signatures are available, the secret key may be recovered using BKZ-138 for the first set of DRS parameters submitted to the NIST. This puts the security level of this parameter set below 80-bit (maybe even 70-bit), to be compared to an original claim of 128 bits.

5.6 Conclusion

With respect to our concrete targets within TASK 3.3, we obtained numerous results. Namely, we improved state-of-the-art algorithms under both classical and quantum settings. First, we improved state-of-the-art quantum algorithms for both Euclidean and ideal lattice and module lattice. These results can be used for selecting parameters given concrete needs for security and efficiency. Second, we have a better understanding on some classical algorithms for solving lattice-based cryptosystems. These works will help to determine parameters for being secure in a world without large-scale quantum computers. Finally, we investigated the security of many lattice-based NIST candidates, which we successfully produced an automated tool for generating parameters given desirable security level and efficiency.

6 TASK 3.4: Side-channel attacks

In the following, we will review our targets as well as summarize our results obtained so far within TASK 3.4.

6.1 Review of the targets

We first recall the targets of TASK 3.4 in Table 8. The main objective is to have a better understanding of the impact of side-channel attacks on lattice-based cryptographic implementations (both software and hardware). Then, we want to propose secure implementations against side-channel attacks by using countermeasures. The final target is to avoid insecure designs and to provide solutions for having secure implementation against side-channel attacks for the building blocks in WP4 as well as the privacy-preserving protocols in WP5. On one hand, from the attack point of view, we need to study and apply possible side-channel attacks on lattice-based schemes by exploiting any side-channel leakage or fault attacks against them. Specifically, we need to evaluate the resistance of the publicly proposed implementations of the NIST candidates, as they are also potential candidates for the building blocks for designing our privacy-preserving schemes in WP5. On the other hand, with respect to these attacks, we aim at finding efficient countermeasures. Out of many issues, there are two important questions: the first one is to improve the efficiency of applying masking tools to Gaussian sampling algorithm over lattices and the second one is to find efficient solutions to thwart cache attacks.

Targets	Concrete contents
Investigate side-channel attacks on software/hardware implementation	Apply side-channel attacks (e.g., timing attacks) and fault attacks etc
	Evaluate the resistance of NIST candidates against them
Study on the countermeasure	Apply masking tools efficiently to sampling algorithm over lattice
	Resistance to cache attacks

Table 8: Concrete targets within TASK 3.4.

6.2 Overview of current results

An overview of the results obtained in TASK 3.4 can be found in Table 9.

6.3 Current results on side-channel attacks

For side-channel cryptanalysis, we have 5 publications: 4 in conferences, 1 in journal and 1 in preprint. So far, we performed side-channel cryptanalysis on numerous existent lattice-based cryptographic schemes. In [EFGT18], the authors give a generic security analysis of implementations for lattice-based cryptosystems. Namely, it is shown that using fault attacks, one can break two main lattice-based signatures: GPV and Fiat-Shamir with Aborts signature schemes, as well as some key encapsulation mechanisms. Further in [ADP18], cold boot attacks on all RLWE/MLWE-based schemes have been studied by exploiting the weakness of storing the secret key in NTT form (number theoretic transform). On the other hand, we also look into the weakness of specific schemes against side-channel leakage. The result [BDE⁺18] exposes a weakness of the Fiat-Shamir type signature: BLISS signature against power analysis attacks and timing attacks. Notably, this work proposes a secure constant-time implementation to thwart the attacks. Then for the first time, the work [FKT⁺19] analyzes the

Category	Work	Status
Side-channel attacks	Loop-Abort Faults on Lattice-Based Signature Schemes and Key Exchange Protocols [EFGT18]	IEEE TC
	Cold Boot Attacks on Ring and Module LWE Keys Under the NTT [ADP18]	CHES 2019
	LWE Without Modular Reduction and Improved Side-Channel Attacks Against BLISS [BDE ⁺ 18]	Asiacrypt 2018
	Uprooting the Falcon Tree? [FKT ⁺ 19]	Preprint
	Assessment of the Key-Reuse Resilience of NewHope [BGRR19]	CT-RSA 2019
Countermeasures	Masking the GLP Lattice-Based Signature Scheme at Any Order [BBE ⁺ 18]	Eurocrypt 2018
	Masking Dilithium: Efficient Implementation and Side-Channel Evaluation [MGTF19]	ACNS 2019
	An Efficient and Provable Masked Implementation of qTESLA [GR19]	Preprint

Table 9: Current (intermediate) results on TASK 3.4.

security of hash-and-sign signature (e.g., GPV signature) under side-channel attacks. It is shown that the implementation of the DLP scheme as proposed by its designers, a predecessor of the second-round NIST candidate FALCON, is not secure, which also draws attention on the similar security issue for FALCON. Recently in [BGRR19], the authors show that the NewHope scheme with key reuse is not secure against side channels attacks or fault attacks.

Loop-Abort Faults on Lattice-Based Signature Schemes and Key Exchange Protocols. As the advent of general-purpose quantum computers appears to be drawing closer, agencies and advisory bodies have started recommending that we prepare the transition away from factoring and discrete logarithm-based cryptography, and towards postquantum secure constructions, such as lattice-based schemes. Almost all primitives of classical cryptography (and more!) can be realized with lattices, and the efficiency of primitives like encryption and signatures has gradually improved to the point that key sizes are competitive with RSA at similar security levels, and fast performance can be achieved both in software and hardware. However, little research has been conducted on physical attacks targeting concrete implementations of postquantum cryptography in general and lattice-based schemes in particular, and such research is essential if lattices are going to replace RSA and elliptic curves in our devices and smart cards. In this paper, we look in particular at fault attacks against implementations of lattice-based signature schemes, looking both at Fiat-Shamir type constructions (particularly BLISS, but also GLP, PASSSing and Ring-TESLA) and at hash-and-sign schemes (particularly the GPV-based scheme of Ducas-Prest-Lyubashevsky).

These schemes include essentially all practical lattice-based signatures, and achieve the best efficiency to date in both software and hardware. We present several fault attacks against those schemes yielding a full key recovery with only a few or even a single faulty signature, and discuss possible countermeasures to protect against these attacks.

Cold Boot Attacks on Ring and Module LWE Keys Under the NTT. In this work, cold boot attacks are investigated on cryptographic schemes based on the ring- and module- variants of the LWE problem, wherein an attacker is faced with the problem of recovering a scheme’s secret key from a noisy version of that key. The leakage resilience of cryptography based on the LWE problem has been studied before, but there are only limited results considering the parameters observed in cold boot attack scenarios. There are two main encodings for storing ring- and module-LWE keys, and, as shown in this work, the performance of cold boot attacks can be highly sensitive to the exact encoding used. The first encoding stores polynomial coefficients directly in memory. The second encoding performs a number theoretic transform (NTT) before storing the key, a commonly used method leading to more efficient implementations. First, estimates are given for a cold boot attack complexity on the first encoding method based on standard algorithms; this analysis confirms that this encoding method is vulnerable to cold boot attacks only at very low bit-flip rates. Then, it is shown that, for the second encoding method, the structure introduced by using an NTT is exploitable in the cold boot setting: a bespoke attack strategy can be developed that is much cheaper than the estimates for the first encoding when considering module-LWE keys. For example, at a 1% bit-flip rate (which corresponds roughly to what can be achieved in practice for cold boot attacks when applying cooling), a cold boot attack on Kyber KEM parameters has a cost of 2^{43} operations when the secret key is stored in NTT encoding, compared to 2^{70} operations with the first encoding. On the other hand, in the case of the ring-LWE-based KEM, New Hope, the cold boot attack complexities are similar for both encoding methods.

LWE Without Modular Reduction and Improved Side-Channel Attacks Against BLISS. This work is devoted to analyzing the variant of Regev’s LWE problem in which modular reduction is omitted: namely, the problem (ILWE) of recovering a vector $\mathbf{s} \in \mathbb{Z}^n$ given polynomially many samples of the form $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e) \in \mathbb{Z}^{n+1}$ where \mathbf{a} and e follow fixed distributions. Unsurprisingly, this problem is much easier than LWE: under mild conditions on the distributions.

In this work, it is shown that the problem can be solved efficiently as long as the variance of e is not super polynomially larger than that of \mathbf{a} . An almost tight bounds is provided on the number of samples needed to recover \mathbf{s} . The interest in studying this problem stems from the side-channel attack against the BLISS lattice-based signature scheme described by Espitau et al. [EFGT17]. The attack targets a quadratic function of the secret that leaks in the rejection sampling step of BLISS [DDLL13]. The same part of the algorithm also suffers from a linear leakage, but the authors claimed that this leakage could not be exploited due to signature compression: the linear system arising from it turns out to be noisy, and hence key recovery amounts to solving a high-dimensional problem analogous to LWE, which seemed infeasible. However, this noisy linear algebra problem does not involve any modular reduction: it is essentially an instance of ILWE, and can therefore be solved efficiently using the proposed techniques. This allows us to obtain an improved side-channel attack on BLISS, which applies to

100% of secret keys (as opposed to $\approx 7\%$ in [EFGT17]), and is also considerably faster.

Uprooting the Falcon Tree? In this work, the study of side-channel leakage in hash-and-sign lattice-based signatures is initiated, with particular emphasis on the two efficient implementations of the original GPV lattice trapdoor paradigm for signatures, namely NIST second-round candidate FALCON [PFH⁺19] and its simpler predecessor DLP [DLP14]. Both of these schemes implement the GPV signature scheme over NTRU lattices, achieving great speed-ups over the general lattice case. There are mainly three results as follows.

First, a specific source of side-channel leakage is identified in most implementations of those schemes. Signing in lattice-based hash-and-sign schemes involves sampling a lattice point according to a Gaussian distribution. This reduces to sampling several one-dimensional discrete Gaussian distributions with standard deviations determined by the Gram-Schmidt norms of the secret lattice basis. The observation is that those norms often leak through timing side-channels in the implementation of the one dimensional Gaussian samplers.

Second, the link between this leakage and the secret key is elucidated, by showing that the entire secret key can be efficiently reconstructed solely from those Gram-Schmidt norms. The result makes heavy use of the algebraic structure of the corresponding schemes, which work over a power-of-two cyclotomic field. To establish it, efficient algorithms are proposed, which, given the leading principal minors of the matrix associated to a totally positive field element (in the power basis for DLP and the bit-reversed order basis for FALCON), recover the element up to conjugation. In the case of those schemes, that element is $f\bar{f} + g\bar{g}$, where (f, g) is the NTRU-style secret key. Then it is shown that this element combined with the verification key suffices to recover the entire secret efficiently.

Third, the side-channel attack against DLP is concretely demonstrated. The challenge is that timing information only provides an approximation of the Gram-Schmidt norms (with an accuracy increasing with the number of traces), and the proposed algebraic recovery technique needs to be combined with pruned tree search in order to apply it to approximated values. Experimentally, it is shown that around 2^{35} DLP traces are enough to reconstruct the entire key with good probability. Carrying out a similar experiment against FALCON is left as an open problem, however, since the recursive nature of our bit-reversed order recovery algorithm does not accommodate approximate inputs easily. Nevertheless, our results do underscore the importance of constant time implementations particularly for schemes using Gaussian sampling.

Assessment of the Key-Reuse Resilience of NewHope NewHope [ADPS16] is a suite of two efficient RLWE based key encapsulation mechanisms (KEMs) that has been proposed to the NIST call for proposals for post-quantum standardization.

In this work, the security of NewHope is studied when an active adversary takes part in a key establishment protocol and is given access to an oracle, called key mismatch oracle, which indicates whether her guess of the shared key value derived by the party targeted by the attack is correct or not. This attack model turns out to be relevant in private key reuse situations since an attacker may then be able to access such an oracle repeatedly – either directly or using faults or side channels, depending on the considered instance of NewHope. Following this model, it is shown that, by using NewHope recommended parameters, several thousands of queries are sufficient to recover the full private key with high probability. This result has been

experimentally confirmed using Magma CAS implementation. While the presented key mismatch oracle attacks do not break any of the designers' security claims for the NewHope KEMs, they provide better insight into the resilience of these KEMs against key reuse. In the case of the CPA-KEM instance of NewHope, they confirm that key reuse (e.g. key caching at server side) should be strictly avoided, even for an extremely short duration. In the case of the CCA-KEM instance of NewHope, they allow to point out critical steps inside the CCA transform that should be carefully protected against faults or side channels in case of potential key reuse.

6.4 Current results on Countermeasures

Within the works about countermeasures against side-channel attacks, we have 3 publications: 2 in conference and another preprint. There are not many works known so far for securing lattice-based cryptographic schemes against side-channel attacks. We started some of them. Concretely, the result [BBE⁺18] gives a masking solution for the GLP lattice-based signature scheme [GLP12], which is an adaptation of Lyubashevsky's signature without trapdoor for embedded systems. The authors of [MGTF19] study in practice the resilience of the Dilithium lattice-based signature using the masking scheme proposed for GLP in the previous work. More recently the work [GR19] further proposes a provable and efficient masking for the second-round NIST candidate: qTELSA signature scheme.

Masking the GLP Lattice-Based Signature Scheme at Any Order. Recently, numerous physical attacks have been demonstrated against lattice-based schemes, often exploiting their unique properties such as the reliance on Gaussian distributions, rejection sampling and FFT-based polynomial multiplication. As the call for concrete implementations and deployment of postquantum cryptography becomes more pressing, protecting against those attacks is an important problem. However, few countermeasures have been proposed so far. In particular, masking has been applied to the decryption procedure of some lattice-based encryption schemes, but the much more difficult case of signatures (which are highly non-linear and typically involve randomness) has not been considered until now.

In this work, the first masked implementation of a lattice-based signature scheme is proposed. Since masking Gaussian sampling and other procedures involving contrived probability distribution would be prohibitively inefficient, this work focuses on the GLP scheme of Güneysu, Lyubashevsky and Pöppelmann [GLP12]. It is shown how to provably mask it in the Ishai–Sahai–Wagner model [ISW03] at any order in a relatively efficient manner, using extensions of the techniques of Coron et al for converting between arithmetic and Boolean masking. The proposed proof relies on a mild generalization of probing security that supports the notion of public outputs. Finally, a proof-of-concept implementation is also provided to assess the efficiency of the proposed countermeasure.

Although security against side-channel attacks is not an explicit design criterion of the NIST postquantum standardization effort, it is certainly a major concern for schemes that are meant for real-world deployment. In view of the numerous physical attacks that have been proposed against postquantum schemes in recent literature, it is in particular very important to evaluate the cost and effectiveness of side-channel countermeasures in that setting.

Masking Dilithium: Efficient Implementation and Side-Channel Evaluation.

For lattice-based signatures, this work was initiated by Barthe et al., who showed at EUROCRYPT 2018 how to apply arbitrary order masking to the GLP signature scheme presented at CHES 2012 by Güneysu, Lyubashevsky and Pöppelman. However, although Barthe et al.'s paper provides detailed proofs of security in the probing model of Ishai, Sahai and Wagner, it does not include practical side-channel evaluations, and its proof-of-concept implementation has limited efficiency. Moreover, the GLP scheme has historical significance but is not a NIST candidate, nor is it being considered for concrete deployment.

In this paper, we look instead at Dilithium, one of the most promising NIST candidates for postquantum signatures. This scheme, presented at CHES 2018 by Ducas et al. and based on module lattices, can be seen as an updated variant of both GLP and its more efficient sibling BLISS; it comes, in particular, with a careful implementation that is both efficient and constant-time.

Our analysis of Dilithium from a side-channel perspective is threefold. We first evaluate the side-channel resistance of an ARM Cortex M3 implementation of Dilithium without masking, and identify exploitable side-channel leakage. We then describe how to securely mask the scheme, and verify that the masked implementation no longer leaks. Finally, we show how a simple tweak to Dilithium (namely, replacing the prime modulus by a power of two) makes it possible to obtain a considerably more efficient masked scheme, by a factor of 7.3 to 9 for the most time-consuming masking operations, without affecting security.

An Efficient and Provable Masked Implementation of qTESLA. Now that the NIST's post-quantum cryptography standardization has entered in its second phase, the time has come to focus more closely on practical aspects of the candidates. While efficient implementations of the proposed schemes are somewhat included in the submission packages, certain issues like the threat of side-channel attacks are often lightly touched upon by the authors. Hence, the community is encouraged by the NIST to join the war effort to treat those peripheral, but nonetheless crucial, topics.

In this work, the lattice-based signature scheme qTESLA [ABB⁺19] is studied in the context of the masking countermeasure. Continuing a line of research opened by Barthe et al. [BBE⁺18] with the masking of the GLP signature scheme, this work extends and modifies their work to mask the qTESLA scheme. Based on the work of Migliore et al. [MGTF19], this work slightly modifies the parameters to improve the masked performance while keeping the same security. The masking can be done at any order and specialized gadgets are used to get maximal efficiency at order 1. Eventually, an implementation of the proposed countermeasure is given in the original code of the submission and performed tests at different orders to assess the feasibility of the proposed technique.

6.5 Conclusion

With respect to our concrete targets within TASK 3.4, we made substantial good progress and numerous publications. Concretely, we performed extensive side-channel cryptanalysis on existant lattice-based cryptographic schemes, especially on the NIST candidates. This effort should help to avoid problematic software/hardware implementations. Further, we also had a valuable try on possible countermeasure (e.g., masking) against side-channels attacks. This branch of work can be used to design a secure implementation of privacy-preserving scheme in work package 5. All the

environment-relevant attacks and countermeasure shown here can also guide for the design of use cases and demonstrators in work package 6.

7 Conclusion

We recall that the aims of WP3 in the PROMETHEUS project is to provide a firm support for subsequent work packages 4, 5 and 6. These mainly include providing: 1) reliable underlying algebraic structure, 2) reliable underlying hard problems, 3) appropriate parameters for implementation and 4) countermeasures for thwarting side-channel attacks. As presented in this report, we already made good contributions on most of the tasks contained in this work package. We note that there are also some works in progress on the rest of the tasks that we did not include in current report, which is to be completed in the next WP3 deliverable D3.3 (due in December 2021). Overall, works in this work package are progressing well so far and can assure its assumed firm support to other work packages.

References

- [ABB⁺19] Erdem Alkim, Paulo S. L. M. Barreto, Nina Bindel, Patrick Longa, and Jefferson E. Ricardini. The lattice-based digital signature scheme qtesla. *IACR Cryptology ePrint Archive*, 2019:85, 2019.
- [ACD⁺18] Martin R. Albrecht, Benjamin R. Curtis, Amit Deo, Alex Davidson, Rachel Player, Eamonn W. Postlethwaite, Fernando Virdia, and Thomas 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*, pages 351–367, 2018.
- [ACW19] Martin R. Albrecht, Benjamin R. Curtis, and Thomas Wunderer. Exploring trade-offs in batch bounded distance decoding. *Cryptology ePrint Archive*, Report 2019/1122, 2019. <https://eprint.iacr.org/2019/1122>.
- [AD17] Martin R. Albrecht and Amit Deo. Large modulus ring-LWE \geq module-LWE. In *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I*, pages 267–296, 2017.
- [ADH⁺19] Martin R. Albrecht, Léo Ducas, Gottfried Herold, Elena Kirshanova, Eamonn W. Postlethwaite, and Marc Stevens. The general sieve kernel and new records in lattice reduction. In *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part II*, pages 717–746, 2019.
- [ADP18] Martin R. Albrecht, Amit Deo, and Kenneth G. Paterson. Cold boot attacks on ring and module LWE keys under the NTT. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2018(3):173–213, 2018.

- [ADPS16] Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum key exchange - A new hope. In *25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016.*, pages 327–343, 2016.
- [ADRS15] Divesh Aggarwal, Daniel Dadush, Oded Regev, and Noah Stephens-Davidowitz. Solving the shortest vector problem in 2^n time using discrete gaussian sampling: Extended abstract. In *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing, STOC 2015, Portland, OR, USA, June 14-17, 2015*, pages 733–742, 2015.
- [AFLT12] Michel Abdalla, Pierre-Alain Fouque, Vadim Lyubashevsky, and Mehdi Tibouchi. Tightly-secure signatures from lossy identification schemes. In *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, pages 572–590, 2012.
- [AGPS19] Martin R. Albrecht, Vlad Gheorghiu, Eamonn W. Postlethwaite, and John M. Schanck. Quantum speedups for lattice sieves are tenuous at best. *Cryptology ePrint Archive*, Report 2019/1161, 2019. <https://eprint.iacr.org/2019/1161>.
- [AGVW17] Martin R. Albrecht, Florian Göpfert, Fernando Virdia, and Thomas Wunderer. Revisiting the expected cost of solving usvp and applications to LWE. In *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I*, pages 297–322, 2017.
- [AJPS18] Divesh Aggarwal, Antoine Joux, Anupam Prakash, and Miklos Santha. A new public-key cryptosystem via mersenne numbers. In *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part III*, pages 459–482, 2018.
- [Ajt96] Miklós 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*, pages 99–108, 1996.
- [AKS01] Miklós Ajtai, Ravi Kumar, and D. Sivakumar. A sieve algorithm for the shortest lattice vector problem. In *Proceedings on 33rd Annual ACM Symposium on Theory of Computing, July 6-8, 2001, Heraklion, Crete, Greece*, pages 601–610, 2001.
- [AP09] J. Alwen and C. Peikert. Generating shorter bases for hard random lattices. In *STACS 2009*, volume 3 of *LIPICs*, pages 75–86. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, Germany, 2009.
- [Ban93] W. Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen*, 296(4):625–635, 1993.

- [BB03] David Brumley and Dan Boneh. Remote timing attacks are practical. In *Proceedings of the 12th USENIX Security Symposium, Washington, D.C., USA, August 4-8, 2003*, 2003.
- [BBD⁺19] Shi Bai, Katharina Boudgoust, Dipayan Das, Adeline Roux-Langlois, Weiqiang Wen, and Zhenfei Zhang. Middle-product learning with rounding problem and its applications, 2019. To appear in the proc. of Asiacrypt.
- [BBE⁺18] Gilles Barthe, Sonia Belaïd, Thomas Espitau, Pierre-Alain Fouque, Benjamin Grégoire, Mélissa Rossi, and Mehdi Tibouchi. Masking the GLP lattice-based signature scheme at any order. In *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II*, pages 354–384, 2018.
- [BBE⁺19] Gilles Barthe, Sonia Belaïd, Thomas Espitau, Pierre-Alain Fouque, Mélissa Rossi, and Mehdi Tibouchi. Galactics: Gaussian sampling for lattice-based constant- time implementation of cryptographic signatures, revisited. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS '19*, pages 2147–2164, New York, NY, USA, 2019. ACM.
- [BBG⁺13] Robert Beals, Stephen Brierley, Oliver Gray, Aram W Harrow, Samuel Kutin, Noah Linden, Dan Shepherd, , and Mark Stather. Efficient distributed quantum computing. In *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 469(2153):20120686, 2013.
- [BDE⁺18] Jonathan Bootle, Claire Delaplace, Thomas Espitau, Pierre-Alain Fouque, and Mehdi Tibouchi. LWE without modular reduction and improved side-channel attacks against BLISS. In *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part I*, pages 494–524, 2018.
- [Ben73] Charles H. Bennett. Logical reversibility of computation. *IBM J. Res. Dev.*, 17(6):525–532, November 1973.
- [Ber05] Daniel J. Bernstein. Cache-timing attacks on aes. 2005.
- [BFRS18] Pauline Bert, Pierre-Alain Fouque, Adeline Roux-Langlois, and Mohamed Sabt. Practical implementation of ring-SIS/LWE based signature and IBE. In *Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings*, pages 271–291, 2018.
- [BGRR19] Aurélie Bauer, Henri Gilbert, Guénaël Renault, and Mélissa Rossi. Assessment of the key-reuse resilience of newhope. In *Topics in Cryptology - CT-RSA 2019 - The Cryptographers' Track at the RSA Conference 2019, San Francisco, CA, USA, March 4-8, 2019, Proceedings*, pages 272–292, 2019.

- [BLL⁺15] Shi Bai, Adeline Langlois, Tancrede Lepoint, Damien Stehlé, and Ron Steinfeld. Improved security proofs in lattice-based cryptography: Using the rényi divergence rather than the statistical distance. In *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part I*, pages 3–24, 2015.
- [BLP⁺13] Z. Brakerski, A. Langlois, C. Peikert, O. Regev, and D. Stehlé. On the classical hardness of learning with errors. In *STOC*, 2013.
- [BLS16] Shi Bai, Thijs Laarhoven, and Damien Stehlé. Tuple lattice sieving. *LMS Journal of Computation and Mathematics*, 19(A):146–162, 2016.
- [BLVW19] Zvika Brakerski, Vadim Lyubashevsky, Vinod Vaikuntanathan, and Daniel Wichs. Worst-case hardness for lpn and cryptographic hashing via code smoothing. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019*, pages 619–635, Cham, 2019. Springer International Publishing.
- [BMW19] Shi Bai, Shaun Miller, and Weiqiang Wen. A refined analysis of the cost for solving LWE via usvp. In *Progress in Cryptology - AFRICACRYPT 2019 - 11th International Conference on Cryptology in Africa, Rabat, Morocco, July 9-11, 2019, Proceedings*, pages 181–205, 2019.
- [BP18] Zvika Brakerski and Renen Perlman. Order-LWE and the hardness of ring-LWE with entropic secrets. *IACR Cryptology ePrint Archive*, 2018:494, 2018.
- [BS16] Jean-François Biasse and Fang Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. In *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2016, Arlington, VA, USA, January 10-12, 2016*, pages 893–902, 2016.
- [BSW18] Shi Bai, Damien Stehlé, and Weiqiang Wen. Measuring, simulating and exploiting the head concavity phenomenon in BKZ. In *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part I*, pages 369–404, 2018.
- [CDPR16] Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev. Recovering short generators of principal ideals in cyclotomic rings. In *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part II*, pages 559–585, 2016.
- [CDW17] Ronald Cramer, Léo Ducas, and Benjamin Wesolowski. Short stickelberger class relations and application to ideal-svp. In *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part I*, pages 324–348, 2017.

- [CGTV15] Jean-Sébastien Coron, Johann Großschädl, Mehdi Tibouchi, and Praveen Kumar Vadnala. Conversion from arithmetic to boolean masking with logarithmic complexity. In *Fast Software Encryption - 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers*, pages 130–149, 2015.
- [CN11] Yuanmi Chen and Phong Q. Nguyen. BKZ 2.0: Better lattice security estimates. In *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, pages 1–20, 2011.
- [CZZ18] Long Chen, Zhenfeng Zhang, and Zhenfei Zhang. On the hardness of the computational ring-LWR problem and its applications. In *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part I*, pages 435–464, 2018.
- [dBDF19] Koen de Boer, Léo Ducas, and Serge Fehr. On the quantum complexity of the continuous hidden subgroup problem. *IACR Cryptology ePrint Archive*, 2019:716, 2019.
- [dBdJdW18] Koen de Boer, Léo Ducas, Stacey Jeffery, and Ronald de Wolf. Attacks on the AJPS mersenne-based cryptosystem. In *Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings*, pages 101–120, 2018.
- [DDLL13] Léo Ducas, Alain Durmus, Tancrede Lepoint, and Vadim Lyubashevsky. Lattice signatures and bimodal gaussians. In *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I*, pages 40–56, 2013.
- [DFMS19] Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner. Security of the fiat-shamir transformation in the quantum random-oracle model. In *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II*, pages 356–383, 2019.
- [DGPY19] Léo Ducas, Steven Galbraith, Thomas Prest, and Yang Yu. Integral matrix gram root and lattice gaussian sampling without floats. *IACR Cryptology ePrint Archive*, 2019:320, 2019.
- [DKL⁺18] Léo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé. Crystals-dilithium: A lattice-based digital signature scheme. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2018(1):238–268, 2018.
- [DLP14] Léo Ducas, Vadim Lyubashevsky, and Thomas Prest. Efficient identity-based encryption over NTRU lattices. In *Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014, Proceedings, Part II*, pages 22–41, 2014.

- [DPW19] Léo Ducas, Maxime Plançon, and Benjamin Wesolowski. On the shortness of vectors to be found by the ideal-svp quantum algorithm. In *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part I*, pages 322–351, 2019.
- [dt16] The FPLLL development team. `fp111`, a lattice reduction library. <https://github.com/fp111/fp111>, 2016.
- [Duc18] Léo Ducas. Shortest vector from lattice sieving: A few dimensions for free. In *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part I*, pages 125–145, 2018.
- [EFGT17] Thomas Espitau, Pierre-Alain Fouque, Benoît Gérard, and Mehdi Tibouchi. Side-channel attacks on BLISS lattice-based signatures: Exploiting branch tracing against strongswan and electromagnetic emanations in microcontrollers. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017*, pages 1857–1874, 2017.
- [EFGT18] Thomas Espitau, Pierre-Alain Fouque, Benoît Gérard, and Mehdi Tibouchi. Loop-abort faults on lattice-based signature schemes and key exchange protocols. *IEEE Trans. Computers*, 67(11):1535–1549, 2018.
- [EHKS14] Kirsten Eisenträger, Sean Hallgren, Alexei Y. Kitaev, and Fang Song. A quantum algorithm for computing the unit group of an arbitrary degree number field. In *Symposium on Theory of Computing, STOC 2014, New York, NY, USA, May 31 - June 03, 2014*, pages 293–302, 2014.
- [FKT⁺19] Pierre-Alain Fouque, Paul Kirchner, Mehdi Tibouchi, Alexandre Wallet, and Yang Yu. Uprooting the falcon tree? *Cryptology ePrint Archive*, Report 2019/1180, 2019. <https://eprint.iacr.org/2019/1180>.
- [FO99] Eiichiro Fujisaki and Tatsuo Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, pages 537–554, 1999.
- [FP83] U. Fincke and Michael Pohst. A procedure for determining algebraic integers of given norm. In *Computer Algebra, EUROCAL '83, European Computer Algebra Conference, London, England, March 28-30, 1983, Proceedings*, pages 194–202, 1983.
- [GGH97] Oded Goldreich, Shafi Goldwasser, and Shai Halevi. Public-key cryptosystems from lattice reduction problems. In *Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings*, pages 112–131, 1997.

- [GLP12] Tim Güneysu, Vadim Lyubashevsky, and Thomas Pöppelmann. Practical lattice-based cryptography: A signature scheme for embedded systems. In *Cryptographic Hardware and Embedded Systems - CHES 2012 - 14th International Workshop, Leuven, Belgium, September 9-12, 2012. Proceedings*, pages 530–547, 2012.
- [GMSS99] Oded Goldreich, Daniele Micciancio, Shmuel Safra, and Jean-Pierre Seifert. Approximating shortest lattice vectors is not harder than approximating closest lattice vectors. *Inf. Process. Lett.*, 71(2):55–61, 1999.
- [GN08] Nicolas Gama and Phong 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*, pages 31–51, 2008.
- [GNR10] Nicolas Gama, Phong Q. Nguyen, and Oded Regev. Lattice enumeration using extreme pruning. 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*, pages 257–278, 2010.
- [GPV08] Craig Gentry, Chris Peikert, and Vinod 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*, pages 197–206, 2008.
- [GR19] François Gérard and Mélissa Rossi. An efficient and provable masked implementation of qtesla. *IACR Cryptology ePrint Archive*, 2019:606, 2019.
- [HHP⁺03] Jeffrey Hoffstein, Nick Howgrave-Graham, Jill Pipher, Joseph H. Silverman, and William Whyte. NTRUSIGN: digital signatures using the NTRU lattice. In *Topics in Cryptology - CT-RSA 2003, The Cryptographers' Track at the RSA Conference 2003, San Francisco, CA, USA, April 13-17, 2003, Proceedings*, pages 122–140, 2003.
- [HKL18] Gottfried Herold, Elena Kirshanova, and Thijs Laarhoven. Speed-ups and time-memory trade-offs for tuple lattice sieving. In *Public-Key Cryptography - PKC 2018 - 21st IACR International Conference on Practice and Theory of Public-Key Cryptography, Rio de Janeiro, Brazil, March 25-29, 2018, Proceedings, Part I*, pages 407–436, 2018.
- [HKSU18] Kathrin Hövelmanns, Eike Kiltz, Sven Schäge, and Dominique Unruh. Generic authenticated key exchange in the quantum random oracle model. *IACR Cryptology ePrint Archive*, 2018:928, 2018.
- [HPS98] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A ring-based public key cryptosystem. In *Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998, Proceedings*, pages 267–288, 1998.
- [HS07] Guillaume Hanrot and Damien Stehlé. Improved analysis of kannan's shortest lattice vector algorithm. In *Advances in Cryptology - CRYPTO*

- 2007, *27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007, Proceedings*, pages 170–186, 2007.
- [ISW03] Yuval Ishai, Amit Sahai, and David A. Wagner. Private circuits: Securing hardware against probing attacks. In *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, pages 463–481, 2003.
- [JZC⁺18] Haodong Jiang, Zhenfeng Zhang, Long Chen, Hong Wang, and Zhi Ma. Ind-cca-secure key encapsulation mechanism in the quantum random oracle model, revisited. In *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part III*, pages 96–125, 2018.
- [Kan83] Ravi Kannan. Improved algorithms for integer programming and related lattice problems. In *Proceedings of the 15th Annual ACM Symposium on Theory of Computing, 25-27 April, 1983, Boston, Massachusetts, USA*, pages 193–206, 1983.
- [KLS18] Eike Kiltz, Vadim Lyubashevsky, and Christian Schaffner. A concrete treatment of fiat-shamir signatures in the quantum random-oracle model. In *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part III*, pages 552–586, 2018.
- [KMPM19] Elena Kirshanova, Erik Mårtensson, Eamonn W. Postlethwaite, and Subhayan Roy Moulik. Quantum algorithms for the approximate k-list problem and their application to lattice sieving. *IACR Cryptology ePrint Archive*, 2019:1016, 2019.
- [Laa15] Thijs Laarhoven. *Search problems in cryptography*. PhD thesis, Eindhoven University of Technology, 2015.
- [LLL82] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261(4):515–534, 1982.
- [LLS90] J. C. Lagarias, W. H. Lenstra, and C. P. Schnorr. Korkine-Zolotarev bases and successive minimal of a lattice and its reciprocal lattice. *Combinatorica*, 10:333–348, 1990.
- [LM09] Vadim Lyubashevsky and Daniele 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*, pages 577–594, 2009.
- [LM18] Thijs Laarhoven and Artur Mariano. Progressive lattice sieving. In *Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings*, pages 292–311, 2018.

- [LPR10] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. 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*, pages 1–23, 2010.
- [LPSW19] Changmin Lee, Alice Pellet-Mary, Damien Stehlé, and Alexandre Wallet. An LLL algorithm for module lattices. *IACR Cryptology ePrint Archive*, 2019:1035, 2019.
- [LS15] A. Langlois and D. Stehlé. Worst-case to average-case reductions for module lattices. *Designs, Codes and Cryptography*, 75(3), 2015.
- [Lyu12] V. Lyubashevsky. Lattice signatures without trapdoors. In *Eurocrypt 2012*, volume 7237 of *LNCS*. Springer, 2012.
- [MGTF19] Vincent Migliore, Benoît Gérard, Mehdi Tibouchi, and Pierre-Alain Fouque. Masking dilithium - efficient implementation and side-channel evaluation. In *Applied Cryptography and Network Security - 17th International Conference, ACNS 2019, Bogota, Colombia, June 5-7, 2019, Proceedings*, pages 344–362, 2019.
- [Mic00] Daniele Micciancio. The shortest vector in a lattice is hard to approximate to within some constant. *SIAM J. Comput.*, 30(6):2008–2035, 2000.
- [MP12] Daniele Micciancio and Chris Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, pages 700–718, 2012.
- [MR18] Carlos Aguilar Melchor and Thomas Ricosset. Cdt-based gaussian sampling: From multi to double precision. *IEEE Trans. Computers*, 67(11):1610–1621, 2018.
- [MV10a] D. Micciancio and P. Voulgaris. Faster exponential time algorithms for the shortest vector problem. In *Proc. of SODA*. ACM, 2010.
- [MV10b] Daniele Micciancio and Panagiotis Voulgaris. A deterministic single exponential time algorithm for most lattice problems based on voronoi cell computations. In *Proceedings of the 42nd ACM Symposium on Theory of Computing, STOC 2010, Cambridge, Massachusetts, USA, 5-8 June 2010*, pages 351–358, 2010.
- [NR06] Phong Q. Nguyen and Oded Regev. Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures. In *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*, pages 271–288, 2006.
- [Pei16] Chris Peikert. How (not) to instantiate ring-LWE. In *Security and Cryptography for Networks - 10th International Conference, SCN 2016, Amalfi, Italy, August 31 - September 2, 2016, Proceedings*, pages 411–430, 2016.

- [PFH⁺19] Thomas Prest., Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. Falcon. tech. rep., national institute of standards and technology. available at <https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions>, 2019.
- [PHS19] Alice Pellet-Mary, Guillaume Hanrot, and Damien Stehlé. Approx-svp in ideal lattices with pre-processing. In *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part II*, pages 685–716, 2019.
- [PP19] Thomas Pornin and Thomas Prest. More efficient algorithms for the NTRU key generation using the field norm. In *Public-Key Cryptography - PKC 2019 - 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography, Beijing, China, April 14-17, 2019, Proceedings, Part II*, pages 504–533, 2019.
- [PRS17a] Chris Peikert, Oded Regev, and Noah Stephens-Davidowitz. Pseudorandomness of ring-LWE for any ring and modulus. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017*, pages 461–473, 2017.
- [PRS17b] Chris Peikert, Oded Regev, and Noah Stephens-Davidowitz. Pseudorandomness of ring-lwe for any ring and modulus. In Hamed Hatami, Pierre McKenzie, and Valerie King, editors, *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017*, pages 461–473. ACM, 2017.
- [PSDS] Thomas Plantard, Arnaud Sipasseuth, Cedric Dumondelle, and Willy Susilo. Drs : Diagonal dominant reduction for lattice-based signature. submitted to the NIST. Post-Quantum Cryptography Project <https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions>.
- [PSW08] Thomas Plantard, Willy Susilo, and Khin Than Win. A digital signature scheme based on cvp_{∞} . In *Public Key Cryptography - PKC 2008, 11th International Workshop on Practice and Theory in Public-Key Cryptography, Barcelona, Spain, March 9-12, 2008. Proceedings*, pages 288–307, 2008.
- [Reg05] Oded 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*, pages 84–93, 2005.
- [Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6):34:1–34:40, 2009.
- [Rog88] C. A. Rogers. A subexponential algorithm for the determination of class groups and regulators of algebraic number fields. *Séminaire de théorie des nombres*, 1989(1990):27–41, 1988.

- [RSSS17] Miruna Rosca, Amin Sakzad, Damien Stehlé, and Ron Steinfeld. Middle-product learning with errors. In *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part III*, pages 283–297, 2017.
- [RSW18] Miruna Rosca, Damien Stehlé, and Alexandre Wallet. On the ring-LWE and polynomial-LWE problems. In *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part I*, pages 146–173, 2018.
- [Sch86] Alexander Schrijver. *Theory of Linear and Integer Programming*. John Wiley & Sons, Inc., 1986.
- [Sch87] Claus-Peter Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. *Theor. Comput. Sci.*, 53:201–224, 1987.
- [SE91] Claus-Peter Schnorr and M. Euchner. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. In *Fundamentals of Computation Theory, 8th International Symposium, FCT '91, Gosen, Germany, September 9-13, 1991, Proceedings*, pages 68–85, 1991.
- [SE94] Claus-Peter Schnorr and M. Euchner. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. *Math. Program.*, 66:181–199, 1994.
- [SSTX09] Damien Stehlé, Ron Steinfeld, Keisuke Tanaka, and Keita Xagawa. Efficient public key encryption based on ideal lattices. In *Advances in Cryptology - ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009. Proceedings*, pages 617–635, 2009.
- [YD18] Yang Yu and Léo Ducas. Learning strikes again: The case of the DRS signature scheme. In *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part II*, pages 525–543, 2018.