On Lattices for Cryptography

Jheyne N. Ortiz[1] Robson R. Araujo[2] Sueli I.R. Costa[2]
Ricardo Dahab[1] Diego F. Aranha[1]
[1] - *IC/Unicamp*
[2] - *Imecc/Unicamp*

July 25, 2018
LAWCI - Latin American Week on Coding and Information
Unicamp, Campinas - SP

Outline

- Post-quantum Cryptography
  - Conventional Cryptography
  - Quantum Computing
  - Post-quantum Cryptography
- Lattices
- Lattice-based cryptography
- Aspects of algebraic number theory
- Choosing lattice parameters

Conventional Cryptography

Cryptography consists in protocols and algorithms for providing

- integrity;
- confidentiality;
- authenticity; and
- non-repudiation.

Conventional Cryptography

Cryptography consists in protocols and algorithms for providing

- integrity;
- confidentiality;
- authenticity; and
- non-repudiation.

These properties can be obtained by adopting a combination of encryption schemes, key-encapsulation mechanisms, digital signatures, key-exchange protocols, and hash functions.

Keywords: TLS protocol, RSA, ECDSA, SHA-2, AES.

Post-quantum Cryptography
Quantum Computing, Bristlecone

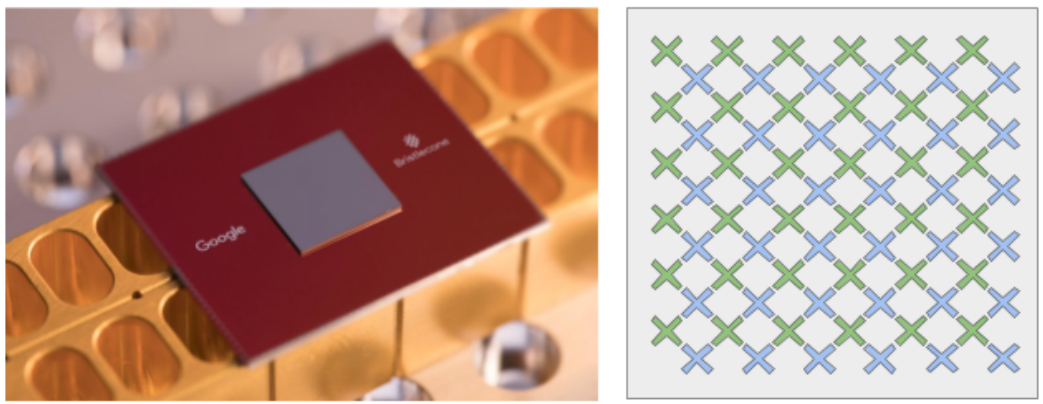
A Preview of Bristlecone, Google's New Quantum Processor

Monday, March 05, 2018

Posted by Julian Kelly, Research Scientist, Quantum AI Lab

The goal of the Google Quantum AI lab is to build a quantum computer that can be used to solve real-world problems. Our strategy is to explore near-term applications using systems that are forward compatible to a large-scale universal error-corrected quantum computer. In order for a quantum processor to be able to run algorithms beyond the scope of classical simulations, it requires not only a large number of qubits. Crucially, the processor must also have low error rates on readout and logical operations, such as single and two-qubit gates.

Today we presented Bristlecone, our new quantum processor, at the annual American Physical Society meeting in Los Angeles. The purpose of this gate-based superconducting system is to provide a testbed for research into system error rates and scalability of our qubit technology, as well as applications in quantum simulation, optimization, and machine learning.



Bristlecone is Google's newest quantum processor (left). On the right is a cartoon of the device: each "X" represents a qubit, with nearest neighbor connectivity.

Figure 1: New Google's quantum computer with 72 qubits.

Quantum Computing

Quantum computers are an imminent threat to **public-key cryptography**.

Shor's quantum algorithm can be used to solve integer factorization and discrete logarithm problems [Sho97]. It implies the end of RSA- and ECC-based cryptographic schemes.

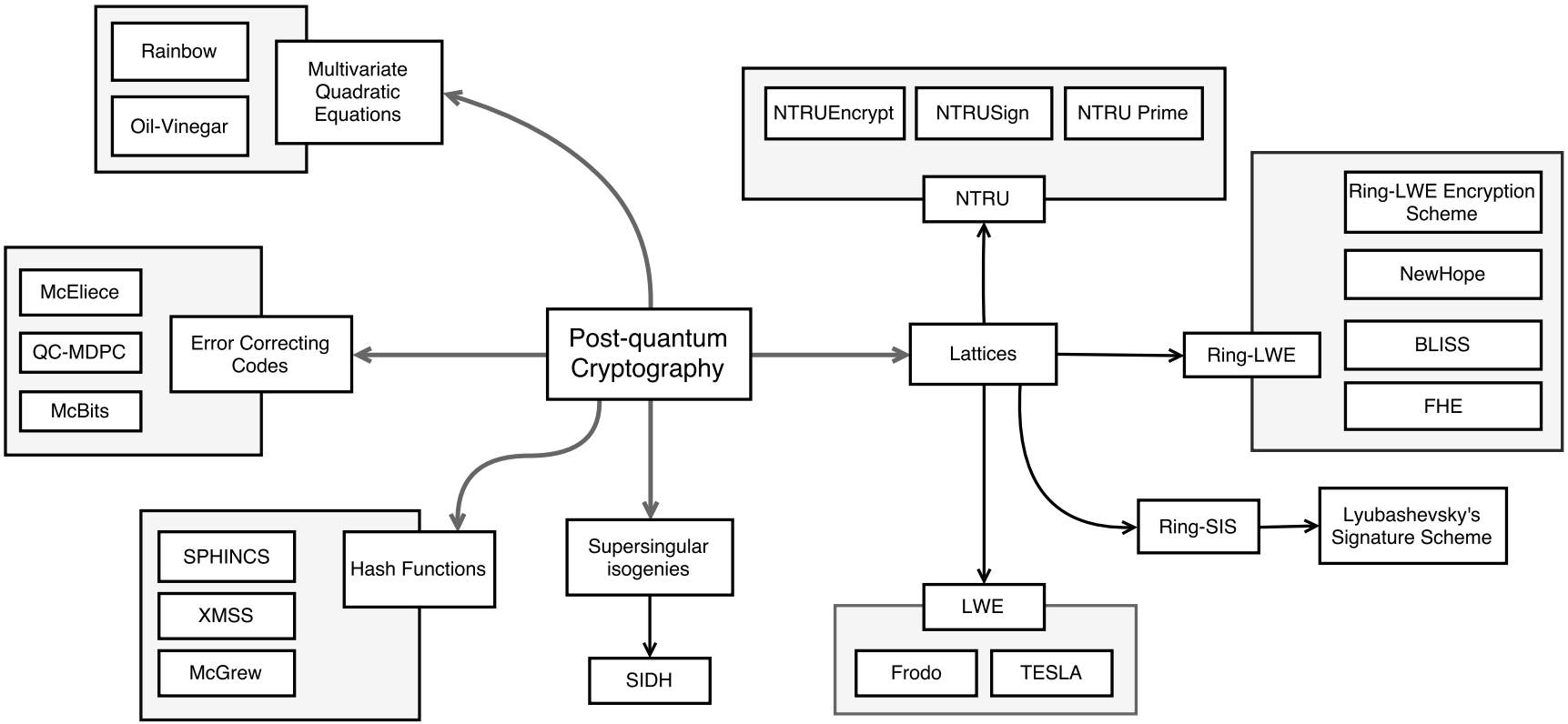
Quantum Computing

Quantum computers are an imminent threat to **public-key cryptography**.

Shor's quantum algorithm can be used to solve integer factorization and discrete logarithm problems [Sho97]. It implies the end of RSA- and ECC-based cryptographic schemes.

Problem: A large amount of past and present personal data unprotected from *future* quantum computational power.

Post-quantum Cryptography



Classes of **hard computational problems** that support new cryptographic primitives for which efficient quantum algorithms are still **unknown**.

NIST's Call for Post-quantum Standards

NIST

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

PROJECTS | POST-QUANTUM CRYPTOGRAPHY

Post-Quantum Cryptography

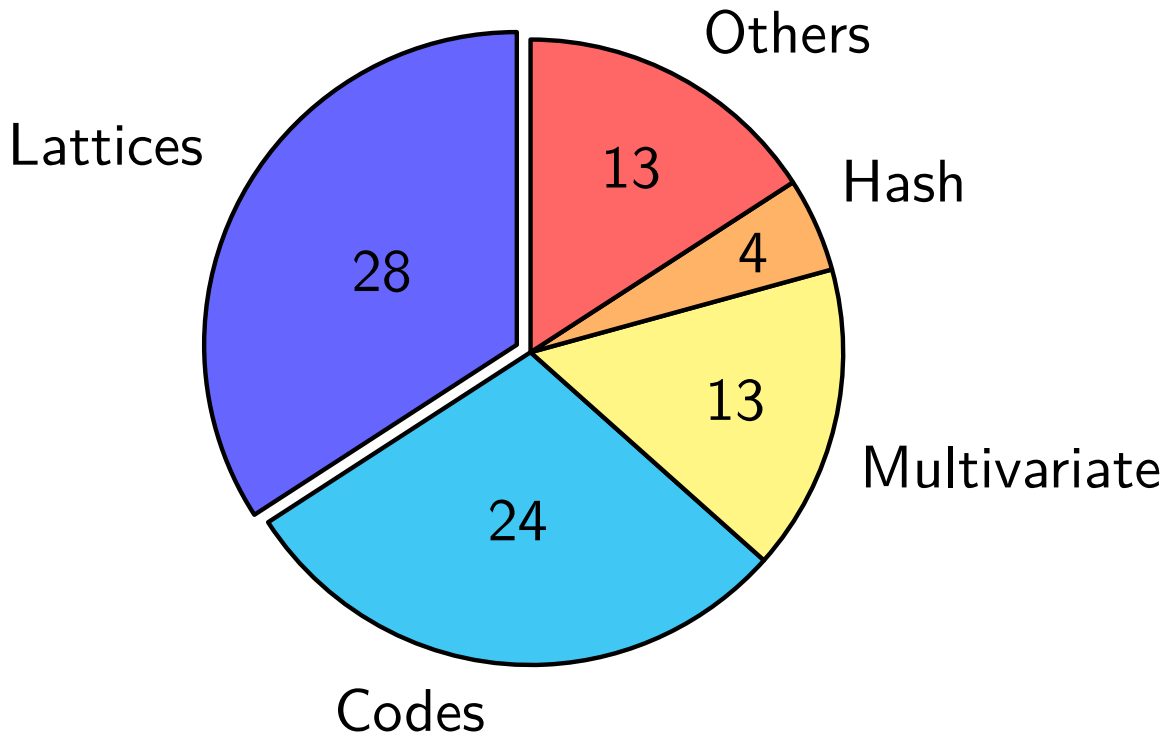
Post-Quantum Cryptography Standardization

The submission deadline of November 30, 2017 has passed. Please see the Round 1 Submissions for the listing of complete and proper submissions.

Call for Proposals Announcement

NIST has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. Currently, public-key cryptographic algorithms are specified in FIPS 186-4, *Digital Signature Standard*, as well as special publications SP 800-56A Revision 2, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography* and SP 800-56B Revision 1, *Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography*. However, these algorithms are vulnerable to attacks from large-scale quantum computers (see NISTIR 8105, *Report on Post Quantum Cryptography*).

Post-quantum Submissions



- Submissions include encryption schemes, digital signatures, and key-encapsulation mechanisms.
- Lattice-based cryptography already provides a whole **framework** of cryptographic primitives!

Definition of lattice

Let $\mathbf{B} = \{b_1, \ldots, b_m\} \subset \mathbb{R}^n$ be a set of m linearly independent vectors, $m \leq n$. The set

$$\Lambda = \Lambda(\mathbf{B}) = \left\{ \sum_{i=1}^{m} x_i b_i : x_i \in \mathbb{Z} \right\}$$

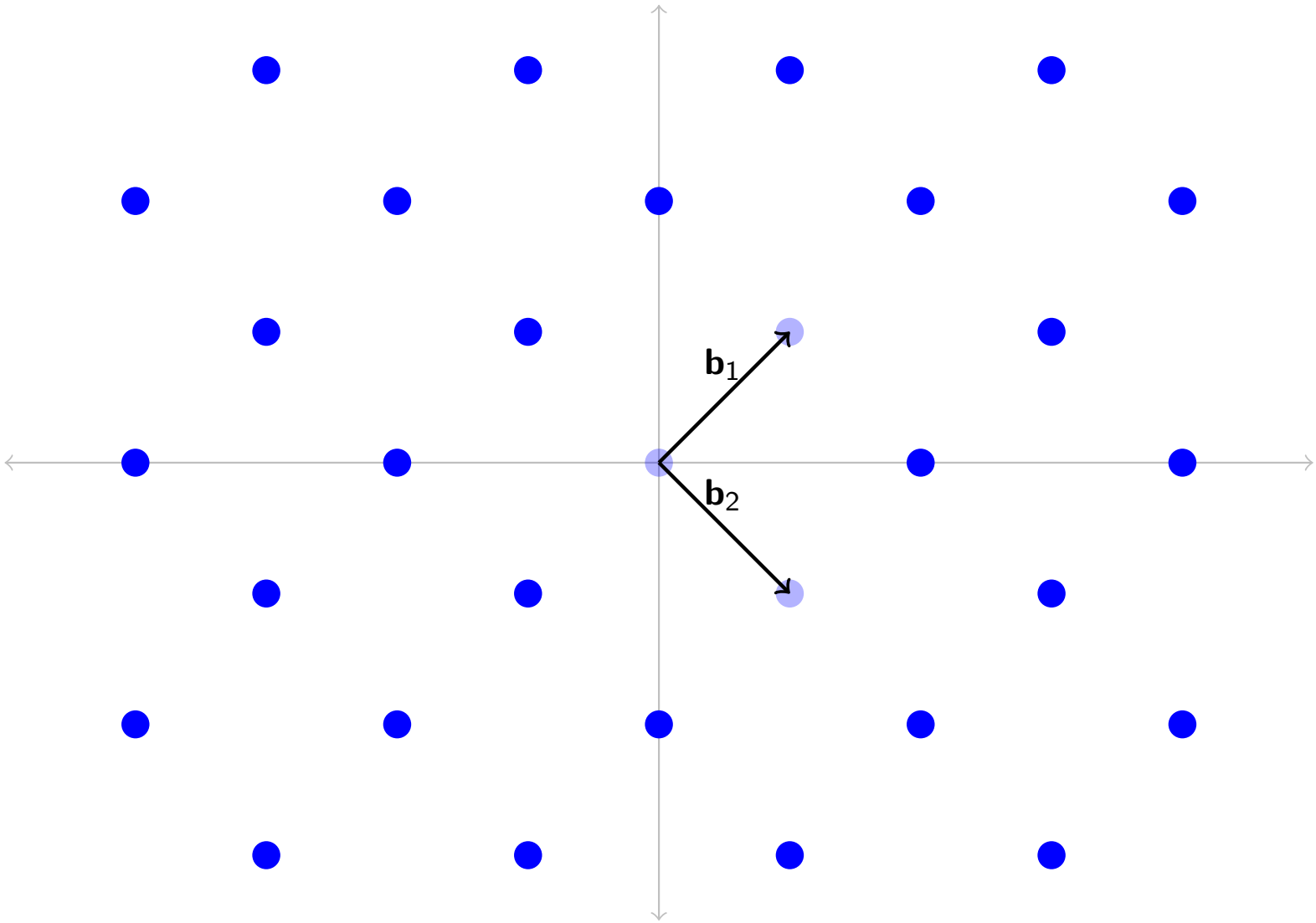
is called *lattice* of rank m in $\mathbb{R}^n$.

If $n = m$, the lattice $\Lambda(\mathbf{B})$ is called a full-rank lattice.

Remark 1: A lattice is an additive discrete subgroup of $\mathbb{R}^n$.
Remark 2: In this work we consider only full-rank lattices.

Example in $\mathbb{R}^2$

Example of the full-rank lattice $\Lambda(\mathbf{B}) \subset \mathbb{R}^2$ with basis $\mathbf{B} = \{(1, 1), (1, -1)\}$.



Some computational problem over lattices

Consider $\Lambda = \Lambda(\mathbf{B}) \subset \mathbb{R}^n$ a full-rank lattice and $\gamma = \gamma(n) \geq 1$ a real number which grows as a function of n, called *approximation factor*.

- **Shortest Vector Problem (SVP):** Find $\mathbf{c} \in \Lambda$ such that $\|\mathbf{c}\| = \lambda_1(\Lambda)$, where $\lambda_1(\Lambda) := \min_{\mathbf{0} \neq \mathbf{v} \in \Lambda} \|\mathbf{v}\|$ is called the *minimum distance* of Λ.
- **Approximate SVP (SVP$_\gamma$):** Find $\mathbf{c} \neq \mathbf{0}$ in Λ such that $\|\mathbf{c}\| \leq \gamma(n)\lambda_1(\Lambda)$.
- **Bounded Distance Decoding Problem (BDD$_\gamma$):** if $\mathbf{t} \in \mathbb{R}^n$ is a target point such that $\|\mathbf{t} - \mathbf{v}\| < \lambda_1(\Lambda)/(2\gamma(n))$, for all $\mathbf{v} \in \mathbb{R}^n$, the BDD$_\gamma$ consists in finding the unique $\mathbf{c} \in \Lambda$ such that $\|\mathbf{t} - \mathbf{c}\| < \lambda_1(\Lambda)/(2\gamma(n))$.

In general, these problems are very hard.

Foundations of Lattice-based Cryptography

Short Integer Solution [Ajt96]. Given m uniformly random vectors $\mathbf{a}_i \in \mathbb{Z}_q^n$, the SIS problem to find a nontrivial vector $\mathbf{z} = (z_1, \ldots, z_m) \in \mathbb{Z}^m$ of norm $\|\mathbf{z}\| \leq \beta$ such that $\sum_{i=1}^{m} \mathbf{a}_i \cdot z_i = \mathbf{0} \in \mathbb{Z}_q^n$, for β being a positive real, and n, q positive integer numbers.

Learning with Errors [Reg05]. The LWE problem defines a distribution over $\mathbb{Z}_q^n \times \mathbb{Z}_q$, where the samples are of the form $(\mathbf{a}, b = \langle \mathbf{s}, \mathbf{a} \rangle + e \mod q)$, for $\mathbf{s} \in \mathbb{Z}_q^n$ a fixed element called the *secret*, $\mathbf{a} \in \mathbb{Z}_q^n$ a uniformly random element, and $e \in \psi$ sampled from an error distribution ψ (q and n as in SIS problem).

Search version of LWE problem consists to find $\mathbf{s}$ given m independent samples $(\mathbf{a}_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ drawn from the LWE distribution for a uniformly random secret $\mathbf{s}$.

Number fields and ring of integers

A field $\mathbb{K}$ is said to be a **number field** if

$$\mathbb{K} \simeq \frac{\mathbb{Q}[x]}{\langle f(x) \rangle}$$

where $f(x) \in \mathbb{Q}[x]$ is a monic irreducible polynomial. The degree of $f(x)$ is called the **degree** of $\mathbb{K}$.

The set

$$R = \mathcal{O}_{\mathbb{K}} = \{a \in \mathbb{K} \ : \ \exists g(x) \in \mathbb{Z}[x] \ s.t. \ g(a) = 0\}$$

is a ring called the **ring of integers** of $\mathbb{K}$.

The number field $\mathbb{K}$ of degree n is said to be **totally complex** if there exists exaclty n monomorphisms $\sigma_i : \mathbb{K} \longrightarrow \mathbb{R}$ $(1 \leq i \leq n)$, where $\sigma_{i+n/2} = \overline{\sigma_i}$ for $1 \leq i \leq n/2$.
From now on, suppose that $\mathbb{K}$ is a totally complex number field.

The map $\sigma : \mathbb{K} \longrightarrow \mathbb{R}^n$ defined as

$$\sigma(a) = \Big(\mathfrak{Re}(\sigma_1(a)), \mathfrak{Im}(\sigma_1(a)), \ldots, \mathfrak{Re}(\sigma_{n/2}(a)), \mathfrak{Im}(\sigma_{n/2}(a))\Big)$$

is known as **canonical embedding**.
If $\alpha \in R = \mathcal{O}_{\mathbb{K}}$ satisfies $a_i := \sigma_i(\alpha) \in \mathbb{R}_{>0}$, α is called *totally positive* and we define the map $\sigma_\alpha : \mathbb{K} \longrightarrow \mathbb{R}^n$ as

$$\sigma_\alpha(a) = \Big(\sqrt{2a_1}\mathfrak{Re}(\sigma_1(a)), \sqrt{2a_1}\mathfrak{Im}(\sigma_1(a)), \ldots, \sqrt{2a_{n/2}}\mathfrak{Im}(\sigma_{n/2}(a))\Big)$$

is called **twisted embedding**.

If I is an ideal of R then $\sigma(I)$ and $\sigma_\alpha(I)$ are full-rank lattices in $\mathbb{R}^n$.

Learning with Errors over Rings

Consider $J^\vee = \{a \in \mathbb{K} \ : \ Tr_{\mathbb{K}/\mathbb{Q}}(a) \subset \mathbb{Z}\}$ the *dual* of an ideal $J \subset R$, $R_q = R/qR$, where $q \geq 2$ is an integer number, $\mathbb{K}_\mathbb{R} = \mathbb{K} \otimes_\mathbb{Q} \mathbb{R}$ and $\mathbb{T} = \mathbb{K}_\mathbb{R}/R^\vee$.

Learning with Errors over rings (Ring-LWE) [LPR10]
The *distribution Ring-LWE* outputs samples of the form

$$(a, b = (a \cdot s)/q + e \mod R^\vee) \in R_q \times \mathbb{T},$$

for the secret $s \in R_q^\vee$, where $a \leftarrow R_q$ is uniformly randomized and $e \leftarrow \psi$, where ψ is an error distribution over $\mathbb{K}_\mathbb{R}$.

Ring-LWE search version: for a family of distributions Ψ over $\mathbb{K}_\mathbb{R}$, it consists to the secret s given arbitrary many independent samples from the Ring-LWE distribution, for some arbitrary $s \in \mathcal{R}_q^\vee$ and $\psi \in \Psi$.

Twisted Ring-LWE

In usual Ring-LWE, the error e is randomized as an inverse image of $\tilde{e} \in \mathbb{R}^n$ via the canonical embedding:

$$e = \sigma^{-1}(\tilde{e}).$$

If we change σ by σ_α and choose e to be

$$e = \sigma_\alpha^{-1}(\tilde{e})$$

for some $\tilde{e} \in \mathbb{R}^n$ we have a new version of the Ring-LWE called α-**Ring-LWE**.

Hardness proof [OAD+18]

If $\alpha \in \mathcal{O}_\mathbb{K}$ is totally positive, the search version of Ring-LWE is reducible to the search version of α-Ring-LWE.

Efficiency versus security

- Encoding and decoding of cryptographic systems over LWE are usually done using the lattice $\mathbb{Z}^k$. Recently, [vP16] proposed change $\mathbb{Z}^k$ by Leech lattice Λ_{24} and obtained an improvement of more than 10% in bandwidth. In our opinion, the use of the twisted construction can provide similar analysis for Ring-LWE based cryptographic systems.
- Attacks have been made against some instances of Ring-LWE using good properties of specific number fields. Because of this, it had been suggested to change the number fields that have been used (cyclotomic, for example) by *non Galoisian* and/or *non monogenic* number fields.

References I

M. Ajtai.

Generating Hard Instances of Lattice Problems (Extended Abstract).

In *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing*, STOC '96, pages 99–108, New York, NY, USA, 1996. ACM.

Vadim Lyubashevsky, Chris Peikert, and Oded Regev.

On Ideal Lattices and Learning with Errors over Rings, pages 1–23.

Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.

Jheyne N. Ortiz, Robson R. Araujo, Ricardo Dahab, Diego F. Aranha, and Sueli I. R. Costa.

In praise of twisted canonical embedding.

Cryptology ePrint Archive, Report 2018/356, 2018.

`https://eprint.iacr.org/2018/356`.

References II

Oded Regev.

On Lattices, Learning with Errors, Random Linear Codes, and Cryptography.

In *Proceedings of the Thirty-seventh Annual ACM Symposium on Theory of Computing*, STOC '05, pages 84–93, New York, NY, USA, 2005. ACM.

Peter W. Shor.

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.

SIAM J. Comput., 26(5):1484–1509, October 1997.

Alex van Poppelen.

Cryptographic decoding of the Leech lattice.

Cryptology ePrint Archive, Report 2016/1050, 2016.

`http://eprint.iacr.org/2016/1050`.