A study of some practical impacts of twisted embeddings in lattice-based cryptography

Candidate: Laura Viglioni

Supervisor: Prof. Dr. Ricardo Dahab

March 12, 2021

Agenda for this presentation

Basic definitions

Learning problems

Twisted Ring-LWE cryptosystem

Objectives

Methodology and timeline

Basic definitions

Lattices

A **lattice** $\Lambda \subset \mathbb{R}^n$ is a subgroup of the additive group $\mathbb{R}^n$.

Lattices

In other words, given m linear independent vectors in $\mathbb{R}^n$, the set $\{v_1, v_2, ..., v_m\}$ is called a **basis** for Λ and the lattice may be defined by:

$$\Lambda := \left\{ x = \sum_{i=1}^{m} \lambda_i v_i \in \mathbb{R}^n \mid \lambda_i \in \mathbb{Z} \right\}.$$

That is, any $\lambda \in \Lambda$ can be written as $\lambda = Mv$, where M is the **generator matrix** of Λ where each row is a vector from the basis and $v \in \mathbb{Z}^n$.

Lattices and cryptography

In the last two decades, lattice-based cryptosystems have become an important field in the cryptography community, since these cryptosystems rely on mathematical problems we believe are hard and quantum-resistant, such as the Shortest Vector Problem and the Shortest Independent Vectors Problem.

Lattices problems

Gap Shortest Vector Problem
For an approximation factor $\gamma = \gamma(n) \geq 1$, the $GapSVP_\gamma$ is: given a lattice Λ and length $d > 0$, output **YES** if $\lambda_1(\Lambda) \leq d$ and **NO** if $\lambda_1(L) > \gamma d$.

Shortest Independent Vectors Problem
For an approximation factor $\gamma = \gamma(n) \geq 1$, the $SIVP_\gamma$ is: given a lattice Λ, output n linearly independent lattice vectors of length at most $\gamma(n) \cdot \lambda_n(\Lambda)$.

The H space

Let $r, s, n \in \mathbb{Z}_+$ such that $n = r + 2s > 0$. The space $H \subset \mathbb{C}^n$ is defined as:

$$H = \{(a_1, \dots, a_r, b_1, \dots, b_s, \overline{b_1}, \dots, \overline{b_s}) \in \mathbb{C}^n\},$$

where $a_i \in \mathbb{R}$, $\forall i \in \{1, \dots, r\}$ and $b_j \in \mathbb{C}$, $\forall\, j \in \{1, \dots, s\}$.

The H space

For all $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in H$ the space H is endowed with inner product $\langle x, y \rangle_H$ defined as:

$$\langle x, y \rangle_H = \sum_{i=1}^{n} x_i \overline{y_i} = \sum_{i=1}^{r} x_i y_i + \sum_{i=1}^{s} x_{i+r} \overline{y_{i+r}} + \sum_{i=1}^{s} \overline{x_{i+r}} y_{i+r}.$$

The ℓ_2-norm and infinity norm of any $x \in H$ are defined as $\|x\| = \sqrt{\langle x, x \rangle_H}$ and $\|x\|_\infty = \max \{|x_i|\}_{i=1}^{n}$.

Number Fields

For K, L two fields, we denote by L/K a **field extension** if $K \subseteq L$. Then L is said to be an **extension field** over K, or just an **extension** over K. In a field extension L/K, L has the structure of a vector space over K.

A field extension is called a **number field** when it is over the rational field $\mathbb{Q}$.

Twisted embeddings

Let K and L be two field extensions and a homomorphism $\phi : K \to L$. ϕ is said to be a $\mathbb{Q}$-**homomorphism** if $\phi(a) = a, ; \forall a \in \mathbb{Q}$.
A $\mathbb{Q}$-homomorphism $\phi : K \to \mathbb{C}$ is called an **embedding**.

Twisted embeddings

Theorem

If K is a number field with degree n then there are exactly n embeddings $\sigma_i : K \to \mathbb{C}$ where by $\sigma_i(\theta) = \theta_i$ where $\theta_i \in \mathbb{C}$ is a distinct zero of K's minimum polynomial.

Ian Stewart and David Tall.Algebraic number theory. A K Peters, 2002.

Twisted embeddings

The homomorphism $\sigma : K \to \mathbb{R}^r \times \mathbb{C}^s$, where (r, s) is the signature of K, is the **canonical embedding** and is defined by:

$$\sigma(x) = (\sigma_1(x), \ldots, \sigma_r(x), \sigma_{r+1}(x), \ldots, \sigma_{r+s}(x)) .$$

Note that we could rewrite the canonical embedding as $\sigma : K \to \mathbb{R}^n$,

$$\begin{aligned}\sigma(x) = (&\sigma_1(x), \ldots, \sigma_r(x), \\ &\Re(\sigma_{r+1}(x)), \Im(\sigma_{r+1}(x)), \ldots, \Re(\sigma_{r+s}(x)), \Im(\sigma_{r+s}(x))).\end{aligned}$$

Algebraic lattices

Let $\{\omega_1, ..., \omega_n\}$ be an integral basis of K. The n vectors $v_i = \sigma(\omega_i) \in \mathbb{R}^n$ are linearly independent, so they define a full rank algebraic lattice $\Lambda = \Lambda(\mathcal{O}_K) = \sigma(\mathcal{O}_K)$.

The generator matrix of $\Lambda = \sigma(\mathcal{O}_K)$ is defined by

$$\begin{pmatrix} \sigma_1(\omega_1) & \dots & \sigma_{r+2s}(\omega_1) \\ & \vdots & \\ \sigma_1(\omega_n) & \dots & \sigma_{r+2s}(\omega_n) \end{pmatrix}.$$

Twisted embeddings and number fields

An embedding creates the correspondence between a point $\lambda \in \Lambda \subset \mathbb{R}^n$ of an algebraic lattice.

$$\begin{aligned}\lambda &= (\lambda_1, \ldots, \lambda_{r+2s}) \in \Lambda \\ &= \left(\sum_{i=1}^{n} z_i \sigma_1(\omega_i), \ldots, \sum_{i=1}^{n} z_i \sigma_{r+2s}(\omega_i)\right) \\ &= \left(\sigma_1\left(\sum_{i=1}^{n} z_i \omega_i\right), \ldots, \sigma_{r+2s}\left(\sum_{i=1}^{n} z_i \omega_i\right)\right),\end{aligned}$$

where $z_i \in \mathbb{Z}$. Since any element $x \in \mathcal{O}_K$ has the form $x = \sum_{i=1}^{n} \lambda_i \omega_i$, we can conclude that

$$\lambda = (\sigma_1(x), \ldots, \sigma_{r+2s}(x)) = \sigma(x).$$

Learning problems

Learning from Parity

Given m vectors uniformly chosen $a_i \leftarrow \mathbb{Z}_2^n$ and some $\epsilon \in [0, 1]$, we define the problem **Learning from Parity (LFP)** as:

Find $s \in \mathbb{Z}_2^n$ such that, for $i \in \{1, \ldots, m\}$

$$\langle s, a_i \rangle \ \approx_\epsilon \ b_i \ \ (mod\ 2).$$

In other words, the equality holds with probability $1 - \epsilon$.

Learning with Errors

Learning with Errors (LWE) is a generalization of LFP with two new parameters $p \in \mathbb{P}$ and χ a probability distribution on $\mathbb{Z}_p$ so that we have:

$$< s, a_i > \approx_\chi \; b_i \pmod{p} \quad \text{or} \quad < s, a_i > + e_i = b_i \pmod{p},$$

where $a_i \leftarrow \mathbb{Z}_p^n$ uniformly and $e_i \leftarrow \mathbb{Z}$ according to χ.

Ring-LWE search

Let K be a number field, $R = \mathcal{O}_K$ its ring of integers and $R^\vee$ the codifferent ideal of K. Also let $K_\mathbb{R}$ be the tensor product $K \otimes_\mathbb{Q} \mathbb{R}$.

Let Ψ be a family of distributions over $K_\mathbb{R}$. The **search version of the** *ring* $-$ *LWE* **problem**, denoted $R - LWE_{q,\Psi}$, is defined as follows: given access to arbitrarily many independent samples from $A_{s,\psi}$ for some arbitrary $s \in R_q^\vee$ and $\psi \in \Psi$, find s.

Ring-LWE hardness

Theorem

Let K be the m^{th} cyclotomic number field having dimension $n = \phi(m)$ and $R = \mathcal{O}_K$ be its ring of integers. Let $\alpha < \sqrt{(\log n)/n}$, and let $q = q(n) \geq 2,\ q = 1\ (mod\ m)$ be a poly(n)-bounded prime such that $\alpha q \geq \omega(\sqrt{\log n})$. Then there is a polynomial-time quantum reduction from $\tilde{O}(n/\alpha)$-approximate SIVP (or SVP) on ideal lattices in K to $R - DLWE_{q,\Upsilon_\alpha}$.

Lyubashevsky, Peikert, and Regev. On ideal lattices and learning with errors over rings.

Twisted Ring-LWE

For a totally positive element $\tau \in F$, let ψ_τ denote an error distribution over the inner product $\langle \cdot, \cdot \rangle_\tau$ and $s \in R_q^\vee$ (the "secret") be an uniformly randomized element. The *Twisted Ring-LWE distribution* $\mathcal{A}_{s,\psi_\tau}$ produces samples of the form

$$a, b = a \cdot s + e \pmod{qR^\vee} \in R_q \times K_\mathbb{R}/qR^\vee.$$

Twisted Ring-LWE hardness

Solving the Twisted Ring-LWE is as hard as solving the usual Ring-LWE.

Theorem
Let K be an arbitrary number field, and let $\tau \in F$ be totally positive. Also, let (s, ψ) be randomly chosen from $(U(R_q^\vee) \times \Psi)$ in $(K_\mathbb{R}, \langle \cdot, \cdot \rangle_{\tau=1})$. Then there is a polynomial-time reduction from Ring-LWE$_{q,\psi}$ to Ring-LWE$^\tau_{q,\psi_\tau}$.

Ortiz, Araujo, Aranha, Costa, and Dahab. The Ring-LWE problem in lattice-based cryptography: in praise ofthe twisted embeddings.

Twisted Ring-LWE cryptosystem

Cryptosystem presented by Ortiz et al.

- Let R be an m-th cyclotomic ring and $p, q \in \mathbb{Z}$ coprime numbers.
- The message space is defined as R_p.
- Consider that ϕ_τ is an error distribution over $(K_\mathbb{R}, \langle \cdot, \cdot \rangle_\tau)$ and $\lfloor \cdot \rceil$ denotes a valid discretization to (cosets) of $R^\vee$ or $pR^\vee$.
- $\hat{m} = m/2$ if m is even, otherwise $\hat{m} = m$.
- For any $\overline{a} \in \mathbb{Z}_q$, let $[[\overline{a}]]$ denote the unique representative $a \in (\overline{a} + q\mathbb{Z}) \cap [-q/2, q/2)$, which is entry-wise extended to polynomials.

Cryptosystem presented by Ortiz et al.

- **Key generation**: choose a uniformly random $a \in R_q$. Choose $x \longleftarrow \lfloor \phi_\tau \rceil$ and $e \longleftarrow \lfloor p \cdot \phi_\tau \rceil_{pR^\vee}$. Output $(a, b = \hat{m} \cdot (a \cdot x + e) \mod qR) \in R_q \times R_q$ as the public key and x as the secret key.
- **Encryption**: choose $z \longleftarrow \lfloor \phi_\tau \rceil_R^\vee$, $e' \longleftarrow \lfloor p \cdot \phi_\tau \rceil_{pR^\vee}$ and $e'' \longleftarrow \lfloor p \cdot \phi_\tau \rceil_{t^{-1}\mu + pR^\vee}$, where $\mu \in R_p$ is the word to be encrypted. Let $u = \hat{m} \cdot (a \cdot z + e') \mod qR$ and $v = z \cdot b + e'' \in R_q^\vee$. Output $(u, v) \in R_q \times R_q^\vee$.
- **Decryption**: Given the encrypted message (u, v), compute $v - u \cdot x \mod qR^\vee$, and decode it to $d = [[v - u \cdot x]] \in R^\vee$. Output $\mu = t \cdot d \bmod pR$.

Objectives

Main goal

- Validate the idea of using twisted embeddings in cryptography
- Explore the theoretical and the practical aspects of this proposal

Practical aspects

- Compare implementations and instances of the Twisted Ring-LWE and Ring-LWE
- Maximum real subfield versus the cyclotomic power-of-two
- Search for proper sizes of keys and messages

Theoretical aspects

- Study the polynomial arithmetic of the maximal real subfield
- Study the relation between the orthonormal basis and the efficient conversion between lattice points and elements of number field
- Examine if it is possible to achieve a satisfactory efficiency with non-orthonormal basis

Methodology and timeline

Methodology

- **Literature Review:** review proposals of new cryptosystems, such as *NTTRU*.
- **Theoretical experiments:** perform experiments using algebra libraries to discover twist factors and to discover orthonormal bases.
- **Experimental outcome:** to calculate the expansion factor of the polynomial $f(x)$ that defines the ring $\mathbb{Z}[x]/f(x)$. Adapt or develop algorithms for polynomial multiplication.
- **Implementation:** implement a Twisted Ring-LWE based cryptosystem.
- **Practical experiments:** to estimate the cost in terms of clock cycles, also key and message sizes.

Timeline

- First and second semesters of 2021
  - Study the Twisted Ring LWE problem and implementation.
  - Perform theoretical experiments with number fields, twist factors and lattices.
  - Calculate the expansion factor and adapt/develop algorithms for polynomial multiplication.
- First and second semesters of 2022
  - Implement a Twisted Ring-LWE based cryptosystem.
  - Compare instances of Ring LWE and Twisted Ring LWE, *i.e.*, analyze the cryptosystem in both terms of clock cycles and key sizes.
  - Defense of dissertation.

Thank you!