

Secure Classification as a Service

Levelled Homomorphic, Post-Quantum Secure Machine Learning Inference
based on the CKKS Encryption Scheme

Peter Waldert

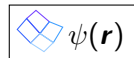
Bachelor Thesis Presentation, 01.08.2022

Outline

- 1 Introduction
- 2 Lattice Cryptography and RLWE
- 3 The CKKS Scheme
- 4 Implementation
- 5 Results

Privacy for Medical Applications

Post-Quantum Security



$$\psi(\mathbf{r})$$

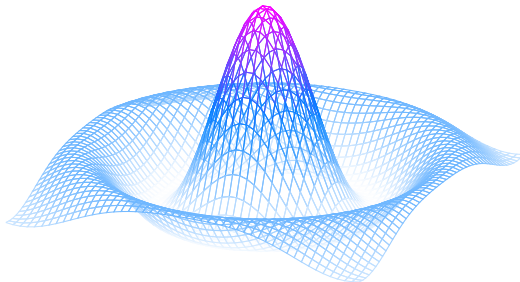


Figure: Illustration of a wave function ψ as commonly used in quantum mechanics.

The Rivest-Shamir-Adleman (RSA) Scheme

From the integers \mathbb{Z} , define the quotient ring $(\mathbb{Z}/q\mathbb{Z}, +, \cdot)$.

With unpadded RSA [2], some arithmetic can be performed on the ciphertext - looking at the encrypted ciphertext $\mathcal{E} : \mathbb{Z}/q\mathbb{Z} \mapsto \mathbb{Z}/q\mathbb{Z}$, $\mathcal{E}(m) := m^r \bmod q$ ($r, q \in \mathbb{N}$) of the message $m_1, m_2 \in \mathbb{Z}/q\mathbb{Z}$ respectively, the following holds:

$$\begin{aligned}\mathcal{E}(m_1) \cdot \mathcal{E}(m_2) &\equiv (m_1)^r (m_2)^r \bmod q \\ &\equiv (m_1 m_2)^r \bmod q \\ &\equiv \mathcal{E}(m_1 \cdot m_2) \bmod q\end{aligned}$$

Polynomial Rings

Definition (Cyclotomic Polynomial)

Given the n^{th} roots of unity $\{\xi_k\}$, define $\Phi_n \in \mathbb{Z}[X]$ as

$$\Phi_n(x) := \prod_{\substack{k=1 \\ \xi_k \text{ primitive}}}^n (x - \xi_k).$$

It is unique for each given $n \in \mathbb{N}$.

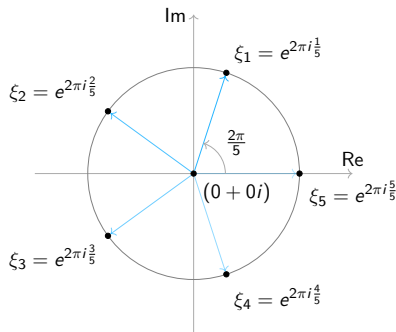


Figure: The 5th roots of unity

Some Notation

- $\mathbb{Z}[X] := \{p : \mathbb{C} \mapsto \mathbb{C}, p(x) = \sum_{k=0}^{\infty} a_k x^k, a_k \in \mathbb{Z} \forall k \geq 0\}$
- $\mathbb{Z}_q[X] := (\mathbb{Z}/q\mathbb{Z})[X]$
- $\mathbb{Z}_q[X]/\Phi_M(X)$
- $\mathbb{Z}_q[X]/(X^N + 1)$ for N a power of 2.

The Learning With Errors (LWE) Problem

Definition (LWE-Distribution $A_{\mathbf{s}, \chi_{\text{error}}}$)

Given a prime $q \in \mathbb{N}$ and $n \in \mathbb{N}$, we choose some secret $\mathbf{s} \in (\mathbb{Z}/q\mathbb{Z})^n$. In order to sample a value from the LWE distribution $A_{\mathbf{s}, \chi_{\text{error}}}$:

- Draw a random vector $\mathbf{a} \in (\mathbb{Z}/q\mathbb{Z})^n$ from the multivariate uniform distribution with its domain in the integers up to q .
- Given another probability distribution χ_{error} over the integers modulo q , sample a scalar 'error term' $\mu \in \mathbb{Z}/q\mathbb{Z}$ from it, often also referred to as noise.
- Set $b = \mathbf{s} \cdot \mathbf{a} + \mu$, with \cdot denoting the standard vector product.
- Output the pair $(\mathbf{a}, b) \in (\mathbb{Z}/q\mathbb{Z})^n \times (\mathbb{Z}/q\mathbb{Z})$.

Search-LWE-Problem: Given m independent samples $(\mathbf{a}_i, b_i)_{0 \leq i \leq m}$ from $A_{\mathbf{s}, \chi_{\text{error}}}$, find \mathbf{s} .

The Learning With Errors on Rings (RLWE) Problem

Corollary (RLWE-Distribution $B_{s, \chi_{\text{error}}}$)

Given a quotient $(R/qR, +, \cdot)$, we choose some secret $s \in R/qR$. In order to sample a value from the RLWE distribution $B_{s, \chi_{\text{error}}}$:

- *Uniformly randomly draw an element $a \in R/qR$*
- *Given another probability distribution χ_{error} over the ring elements, sample an 'error term' $\mu \in R/qR$ from it, also referred to as noise.*
- *Set $b = s \cdot a + \mu$, with \cdot denoting the ring multiplication operation.*
- *Output the pair $(a, b) \in R/qR \times R/qR$.*

Use it to construct a cryptosystem...

Overview of Cheon-Kim-Kim-Song (CKKS)

[1]

Encoding and Decoding

CKKS.

Encode(\mathbf{z}) For a given input vector \mathbf{z} , output

$$m = (\underline{\sigma}^{-1} \circ \underline{\rho}_{\delta}^{-1} \circ \underline{\pi}^{-1})(\mathbf{z}) = \underline{\sigma}^{-1}(\lfloor \delta \cdot \underline{\pi}^{-1}(\mathbf{z}) \rfloor_{\underline{\sigma}(R)}) \rightarrow m$$

Decode(m) Decode plaintext m as $\mathbf{z} = (\underline{\pi} \circ \underline{\rho}_{\delta} \circ \underline{\sigma})(m) = (\underline{\pi} \circ \underline{\sigma})(\delta^{-1}m) \rightarrow \mathbf{z}$

Encryption and Decryption

CKKS.

Encrypt(\mathbf{p}, m) Let $(b, a) = \mathbf{p}$, $u \leftarrow \chi_{enc}$, $\mu_1, \mu_2 \leftarrow \chi_{error}$, then the ciphertext is
 $\mathbf{c} = u \cdot \mathbf{p} + (m + \mu_1, \mu_2) = (m + bu + \mu_1, au + \mu_2) \rightarrow \mathbf{c}$

Decrypt(s, \mathbf{c}) Decrypt the ciphertext $\mathbf{c} = (c_0, c_1)$ as $m = [c_0 + c_1 s]_{q_L} \rightarrow m$

Homomorphic Addition

CKKS.

Add(c_1, c_2) Output $c_3 = c_1 + c_2 \quad \rightarrow c_3$

Demo: Secure Handwritten Digit Classification as a Service

Neural Networks

Matrix Multiplications

Confusion everywhere

Runtime Benchmarks

Ciphertext Visualisations

Conclusion

Crypto is good for us

Questions?

Glossary I

CKKS	Cheon-Kim-Kim-Song	10
LWE	Learning With Errors	8
RLWE	Learning With Errors on Rings	9
RSA	Rivest-Shamir-Adleman	5

Bibliography I

- [1] Jung Hee Cheon, Andrey Kim, Miran Kim and Yongsoo Song. **Homomorphic Encryption for Arithmetic of Approximate Numbers**. ASIACRYPT. 2017.
- [2] Ronald L Rivest, Adi Shamir and Leonard M Adleman. **Cryptographic communications system and method**. US Patent 4,405,829. Sept. 1983.