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

Privacy for Medical Applications

- Development of new applications and solutions in health care, but: very sensitive data.
- For instance, RNA sequences, images of skin, lab data, medical records, etc.
- The results are even more volatile: Disease predictions
- $\Rightarrow$ Demand for privacy-preserving solutions in machine learning applications.

Post-Quantum Security

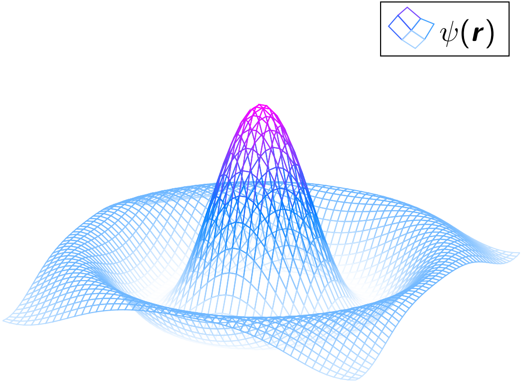


Figure: Illustration of a wave function ψ as commonly used in quantum mechanics.

The Rivest-Shamir-Adleman (RSA) Scheme

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

With unpadded RSA [5], some arithmetic can be performed on the ciphertext - looking at the encrypted ciphertext $\mathcal{E} : \mathbb{Z}/q\mathbb{Z} \mapsto \mathbb{Z}/q\mathbb{Z}$, $\mathcal{E}(m) := m^r \mod q$ $(r, q \in \mathbb{N})$ of the message $m_1, m_2 \in \mathbb{Z}/q\mathbb{Z}$ respectively, the following holds:

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

The Learning With Errors (LWE) Problem

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

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

- Draw a random vector $a \in (\mathbb{Z}/q\mathbb{Z})^n$ 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 $b = \boldsymbol{s} \cdot \boldsymbol{a} + \mu$, with $\cdot$ denoting the standard vector product.
- Output the pair $(\boldsymbol{a}, b) \in (\mathbb{Z}/q\mathbb{Z})^n \times (\mathbb{Z}/q\mathbb{Z})$.

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

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 $n \in \mathbb{N}$.

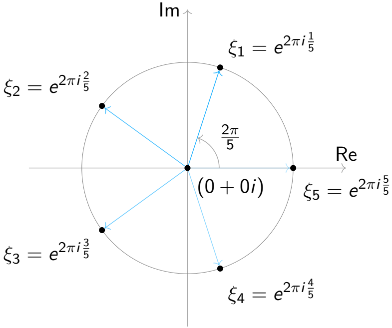


Figure: The 5^{th}roots of unity

Some Notation

- $\mathbb{Z}[X] := \{p : \mathbb{C} \mapsto \mathbb{C}, p(x) = \sum_{k=0}^{\infty} a_k x^k, a_k \in \mathbb{Z}\ \forall k \geq 0\}$
- $\mathbb{Z}_q[X] := (\mathbb{Z}/q\mathbb{Z})[X]$
- $\mathbb{Z}_q[X]/\Phi_M(X)$ using the M^{th}cyclotomic polynomial
- $\mathbb{Z}_q[X]/(X^N + 1)$ for N a power of 2.
  - Elements are polynomials of degree $N - 1$ with integer coefficients modulo q.

Some Notation

- $\mathbb{Z}[X] := \{p : \mathbb{C} \mapsto \mathbb{C}, p(x) = \sum_{k=0}^{\infty} a_k x^k, a_k \in \mathbb{Z}\ \forall k \geq 0\}$
- $\mathbb{Z}_q[X] := (\mathbb{Z}/q\mathbb{Z})[X]$
- $\mathbb{Z}_q[X]/\Phi_M(X)$ using the M^{th}cyclotomic polynomial
- $\mathbb{Z}_q[X]/(X^N + 1)$ for N a power of 2.
  - Elements are polynomials of degree $N - 1$ with integer coefficients modulo q.

The Learning With Errors on Rings (RLWE) Problem

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

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

- *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... Idea: Attacker needs to solve LWE given the ciphertext and public key.

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

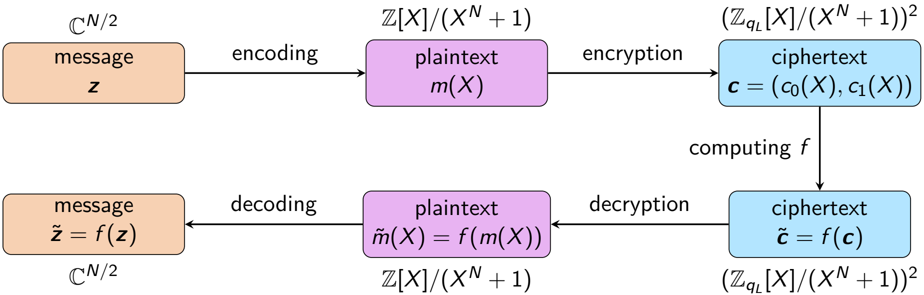


Figure: Schematic overview of CKKS, adapted from [2]. A plain vector $\boldsymbol{z} \in \mathbb{C}^{N/2}$ is encoded to $m = \text{CKKS.Encode}(\boldsymbol{z})$, encrypted to $\boldsymbol{c} = \text{CKKS.Encrypt}(\boldsymbol{p}, m)$, decrypted and decoded to a new $\tilde{\boldsymbol{z}} = \text{CKKS.Decode}(\text{CKKS.Decrypt}(s, \tilde{\boldsymbol{c}}))$.

Encoding and Decoding

CKKS.

Encode($\boldsymbol{z}$) For a given input vector $\boldsymbol{z}$, output
$m = (\underline{\sigma}^{-1} \circ \underline{\rho_\delta}^{-1} \circ \underline{\pi}^{-1})(\boldsymbol{z}) = \underline{\sigma}^{-1}(\lfloor \delta \cdot \underline{\pi}^{-1}(\boldsymbol{z}) \rceil_{\underline{\sigma}(R)}) \quad \to m$

Decode(m) Decode plaintext m as $\boldsymbol{z} = (\underline{\pi} \circ \underline{\rho_\delta} \circ \underline{\sigma})(m) = (\underline{\pi} \circ \underline{\sigma})(\delta^{-1} m) \quad \to \boldsymbol{z}$

- Three transformations: $\underline{\sigma}^{-1}$, $\underline{\rho_\delta}^{-1}$ and $\underline{\pi}^{-1}$.
- Key idea: Homomorphic property, they preserve additivity and multiplicativity.

Encryption and Decryption

CKKS.

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

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

- A public-key cryptosystem! Encrypt with $\boldsymbol{p}$, decrypt with s.
- Leaves the attacker with the RLWE problem.
- Decrypts correctly under certain conditions...

Homomorphic Addition

$\text{CKKS.Add}(\boldsymbol{c}_1, \boldsymbol{c}_2)$ Output $\boldsymbol{c}_3 = \boldsymbol{c}_1 + \boldsymbol{c}_2 \quad \rightarrow \boldsymbol{c}_3$

Decrypts correctly?

$$
\begin{aligned}
\text{BFV.Decrypt}(s, \overline{\boldsymbol{c}}) &= \lfloor \delta^{-1}[\overline{c_0} + \overline{c_1}s]_t \rceil \\
&= \lfloor \delta^{-1}[\delta\overline{m} + b\overline{u} + \overline{\mu_1} + (a\overline{u} + \overline{\mu_2})s]_t \rceil \\
&= \lfloor [(\delta^{-1}\delta)\overline{m} + \delta^{-1}b\overline{u} + \delta^{-1}\overline{\mu_1} + \delta^{-1}as\overline{u} + \delta^{-1}\overline{\mu_2}s]_t \rceil \\
&= \lfloor [\overline{m} - \cancel{\delta^{-1}as\overline{u}} - \delta^{-1}\tilde{\mu}\overline{u} + \delta^{-1}\overline{\mu_1} + \cancel{\delta^{-1}as\overline{u}} + \delta^{-1}\overline{\mu_2}s]_t \rceil \\
&= \lfloor [\overline{m} + \underbrace{\delta^{-1}(\overline{\mu_1} + \overline{\mu_2}s - \tilde{\mu}\overline{u})}_{:=\epsilon\,,||\epsilon||\ll 1}]_t \rceil \approx \lfloor [\overline{m}]_t \rceil = \lfloor \overline{m} \rceil \approx \overline{m}
\end{aligned}
$$

Goal: Classify MNIST

- Two main types of Machine Learning (ML): Supervised and Unsupervised Learning
- Popular dataset: Modified National Institute of Standards and Technology (MNIST). Encode as vector of 784 entries.

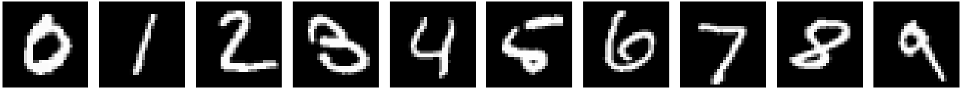


Figure: Sample images of the MNIST dataset of handwritten digits [4]. The dataset contains 70,000 images of 28×28 greyscale pixels valued from 0 to 255 as well as associated labels (as required for supervised learning).

Neural Networks

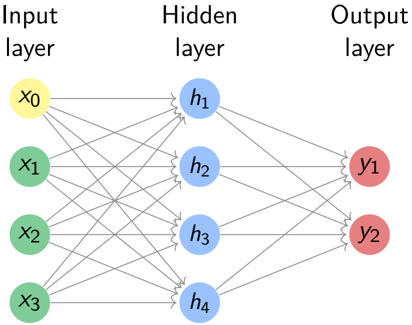


Figure: A simple neural network resembling the structure we use in our demonstrator with $\boldsymbol{h} = \text{relu}(M_1\boldsymbol{x} + \boldsymbol{b_1})$ and the output $\boldsymbol{y} = \text{softmax}(M_2\boldsymbol{h} + \boldsymbol{b_2})$.

Matrix Multiplication: The Naïve Method

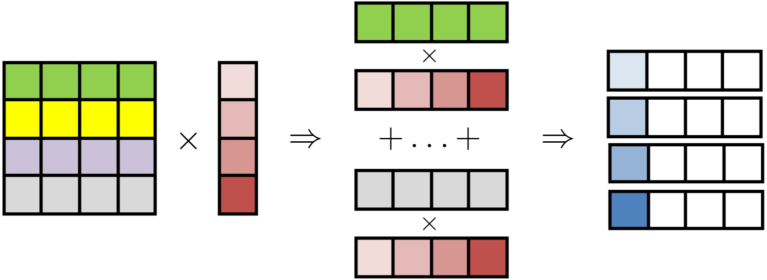


Figure: The naïve method to multiply a square matrix with a vector (adapted from [3]).

Matrix Multiplication: The Diagonal Method

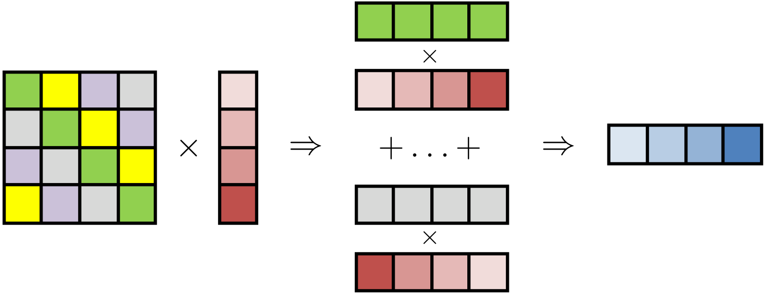


Figure: The diagonal method to multiply a square matrix with a vector (adapted from [3]).

Matrix Multiplication: The Hybrid Method

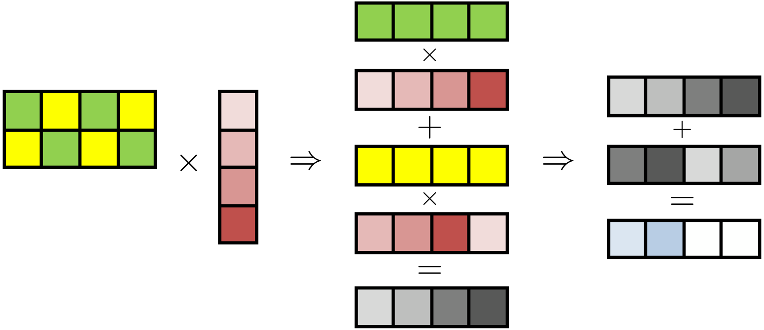


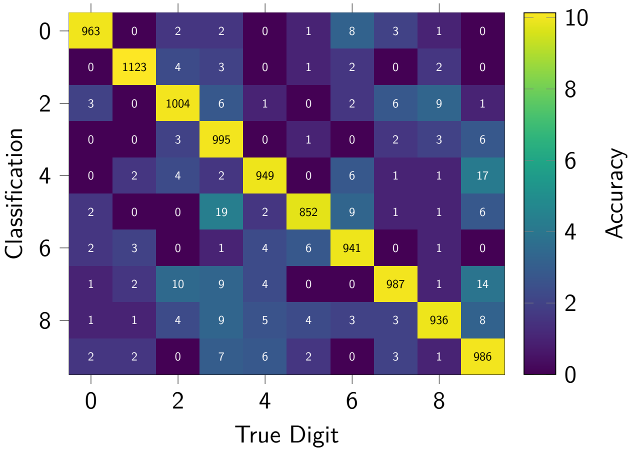
Figure: The hybrid method to multiply an arbitrarily sized matrix with a vector (adapted from [3]).

Similar performance: The BabyStep-Giantstep Method.

Demo: Secure Handwritten Digit Classification as a Service

https://secure-classification.peter.waldert.at/

Chaos everywhere: The Confusion Matrix



Runtime Benchmarks

Table: Performance benchmarks and communication overhead of the classification procedure on an Intel® i7-5600U CPU, including the encoding and decoding steps.

Mode	**SecLevel**	B_1	B_2	N	**MatMul**	T / s	M / MiB	Δ / 1
Release	tc128	34	25	8192	Diagonal	8.39	132.72	0.0364
					Hybrid	1.35	132.72	0.0362
					BSGS	1.66	132.72	0.1433
	tc128	60	40	16384	Diagonal	17.24	286.51	0.0363
					Hybrid	3.05	286.51	0.0364
					BSGS	3.66	286.51	0.1399
	tc256	60	40	32768	Diagonal	35.24	615.16	0.0363
					Hybrid	5.99	615.16	0.0364
					BSGS	7.34	615.16	0.1399

Ciphertext Visualisations

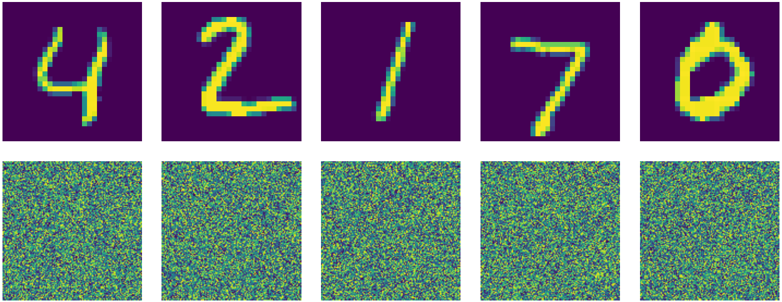


Figure: Ciphertext Visualisation: The first row corresponds to the images in plain, the second row depicts an encrypted version, namely the reconstructed polynomial coefficients a_k of the ciphertext polynomial.

Conclusion

Crypto is good for us

Questions?

Glossary I

CKKS	Cheon-Kim-Kim-Song	11
LWE	Learning With Errors	6
ML	Machine Learning	15
MNIST	Modified National Institute of Standards and Technology	15
RLWE	Learning With Errors on Rings	10
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] Daniel Huynh. **Cryptotree: fast and accurate predictions on encrypted structured data**. (2020). DOI: 10.48550/ARXIV.2006.08299. URL: https://arxiv.org/abs/2006.08299.

[3] Chiraag Juvekar, Vinod Vaikuntanathan and Anantha P. Chandrakasan. **Gazelle: A Low Latency Framework for Secure Neural Network Inference**. *CoRR* abs/1801.05507 (2018). arXiv: 1801.05507. URL: http://arxiv.org/abs/1801.05507.

[4] Yann LeCun and Corinna Cortes. **The MNIST database of handwritten digits**. 1998. URL: http://yann.lecun.com/exdb/mnist/.

[5] Ronald L Rivest, Adi Shamir and Leonard M Adleman. **Cryptographic communications system and method**. US Patent 4,405,829. Sept. 1983.