Evaluate fast polynomial multiplications for PQC schemes via Radix-2^n in Software

Advisor: **Florian Hirner**

DATE: June 26, 2023

Motivation

Data privacy is a critical topic in today's digital world since nobody wants to have their data leaked. However, in certain cases, like medical image evaluation, these data need to be given in an unencrypted format to perform these evaluations. Homomorphic encryption (HE) enables computations on encrypted data to mitigate leakage.

HE requires certain operations like polynomial multiplications with large polynomials. Yet, it is relatively costly in terms of latency to perform one. A more advanced multiplication algorithm like the Fast-Fourier Transformation (FFT) can be used to reduce the latency from $O(n^2)$ to $O(n \cdot logn)$. There are different approaches to perform NTT, like Radix-2^n NTT.

The goal of this project/thesis is to implement a software-based solution to perform FFT via different Radix-2^n. Another goal is to find potential improvements within different Radix-2^n versions to make them more efficient.

Goals and Tasks

- Get familiar with the Fast Fourier Transformation. [2-Weeks]
- A quick research of existing Radix-2^n architectures. [2-Weeks]
- Implement a base version of Radix-$2^n \rightarrow$ Radix-2 [2-Weeks]
- Extend your code to support higher degrees of Radix-2^n , like Radix-4, Radix-8, ..., Radix-32 [1/2-Month]
- Suggest ways to accelerate these computations. [1-Month]

Literature

- Matthias J. Kannwischer
  Polynomial Multiplication for Post-Quantum Cryptography
  https://kannwischer.eu/thesis/phd-thesis-print-version.pdf
- H. J. Nussbaumer
  The Fast Fourier Transform
  https://doi.org/10.1007/978-3-662-00551-4_4
- M. Garrido
  A Survey on Pipelined FFT Hardware Architectures
  https://doi.org/10.1007/s11265-021-01655-1

Courses & Deliverables

- ☑ **Introduction to Scientific Working**
  Short report on background
  Short presentation
- ☑ **Bachelor Project**
  Project code and documentation
- ☑ **Bachelor's Thesis**
  Project code
  Thesis
  Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in the topic area
- Basic knowledge of programming in C/C++, or python

The Hybrid Encryption Paradigm

Advisor: **Anisha Mukherjee**

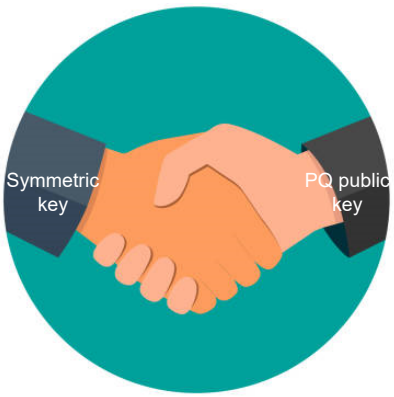
Motivation

As quantum computers began to pose challenges to the security of traditional cryptographic algorithms like RSA and ECC, the research community shifted attention to post-quantum cryptographic solutions. One promising field that has emerged is quantum-safe hybrid encryption. Quantum-safe hybrid encryption combines the strengths of classical encryption algorithms with quantum-resistant primitives to fortify existing systems and protocols, such as TLS/SSL, VPNs, or blockchain against potential quantum attacks.

First, you will start with familiarising yourself with the symmetric and post-quantum public-key algorithms that can be used for hybrid encryption. Next, you will move on to work on a proof-of-concept implementation with the help of already existing resources. Towards the end of the thesis, you will be able to do a brief analysis of the pros and cons of such an encryption protocol in real-world deployment.

Goals and Tasks

- Get familiar with existing literature [3 weeks]
- Implement a proof-of-concept protocol [8-9 weeks]
- Investigate the efficiency and practicality of such a protocol [3 weeks]



Courses & Deliverables

- ☑ **Introduction to Scientific Working**
  Short report on background
  Short presentation
- ☑ **Bachelor Project**
  Project code and documentation
- ☑ **Bachelor's Thesis**
  Project code
  Thesis
  Final presentation

Recommended if you're studying

☑ CS ☑ SEM ☑ MATH

Prerequisites

- Interest in post-quantum cryptography
- Programming (Python/Sage)

Advisor Contact

anisha.mukherjee@iaik.tugraz.at

Designing approximated Machine Learning models in Python for Homomorphic evaluation.

Advisor: **Aikata**

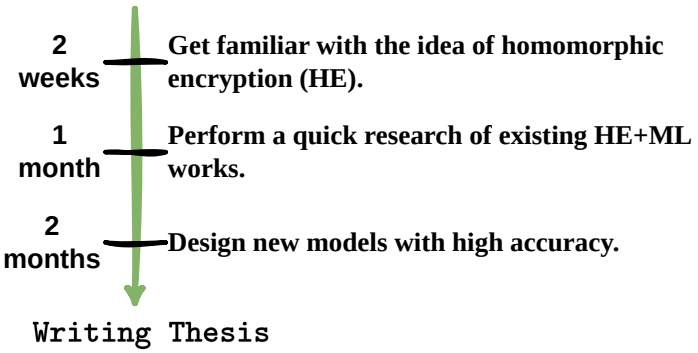
DATE: June 15, 2023

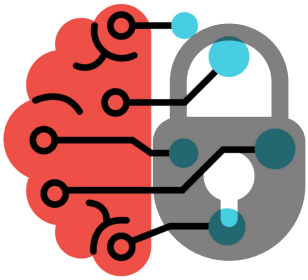
Motivation

Homomorphic encryption is the holy grail of privacy. It allows privacy-preserving data storage and computation. These computations include statistical analysis and several machine-learning applications. The non-linear components in machine-learning models, like ReLU or Max-Pool, cannot be computed using fast homomorphic encryption schemes. Thus, they need to be replaced by functions like a quadratic-ReLU or Average-Pool. This often results in a loss of accuracy.

The purpose of this thesis would be to approximate the existing ML models such that they can be homomorphically evaluated. Approaching the highest possible accuracy would help differentiate this work from naive approximations. In conclusion, this work would analyze the cost of such approximation in terms of runtime and accuracy for training as well as inference.

Goals and Tasks





Literature

- Alessandro Falcetta, Manuel Roveri
  Privacy-Preserving Deep Learning With Homomorphic Encryption: An Introduction
- Joon-Woo Lee, Hyungchul Kang, Yongwoo Lee, et. al.
  Privacy-Preserving Machine Learning With Fully Homomorphic Encryption for Deep Neural Network

Courses & Deliverables

- ☑ **Introduction to Scientific Working**
  Short report on background
  Short presentation
- ☑ **Bachelor Project**
  Project code and documentation
- ☑ **Bachelor's Thesis**
  Project code
  Thesis
  Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in the topic area, and basic knowledge of programming in Python

Advisor Contact

aikata@iaik.tugraz.at

Metrics for analyzing Homomorphic Encryption acceleration works.

Advisor: **Aikata**

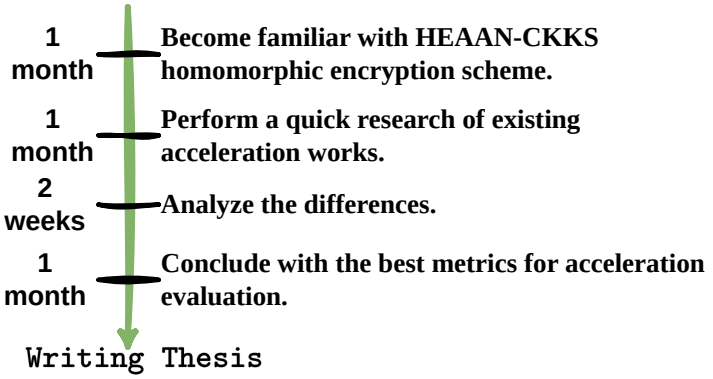
DATE: June 15, 2023

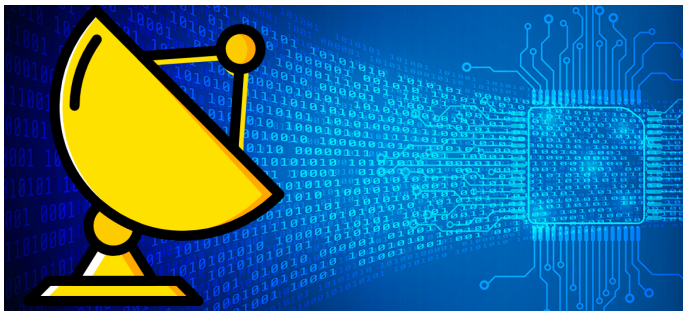
Motivation

Homomorphic encryption is the holy grail of privacy. It allows privacy-preserving data storage and computation. However, this powerful algorithm suffers from impracticality. This is because homomorphic computations are almost a million times slower than plain computations. To bridge this gap several implementations exist in the literature. Now the problem the community faces is how to analyze who is better. Since there are no standards, these implementations choose their own parameters and give acceleration results.

Hence, the goal of this thesis would be to analyze these works and come up with metrics that can help evaluate the acceleration potential of different works. Several such metrics exist, but they lack complete coverage. This thesis would converge to the best metric for the evaluation of acceleration potential.

Goals and Tasks





Literature

- www.openfhe.org/community/
  OpenFHE
  www.openfhe.org/
- Ahmet Can Mert, Aikata, Sunmin Kwon, Youngsam Shin, Donghoon Yoo, Yongwoo Lee, and Sujoy Sinha Roy
  Medha: Microcoded Hardware Accelerator for computing on Encrypted Data
  eprint.iacr.org/2022/480.pdf

Courses & Deliverables

- ☑ **Introduction to Scientific Working**
  Short report on background
  Short presentation
- ☑ **Bachelor Project**
  Project code and documentation
- ☑ **Bachelor's Thesis**
  Project code
  Thesis
  Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in the topic area, and basic knowledge of programming in C/C++

Advisor Contact

aikata@iaik.tugraz.at

Analysis of Side-channel protections for polynomial multiplication.

Advisor: **Aikata**

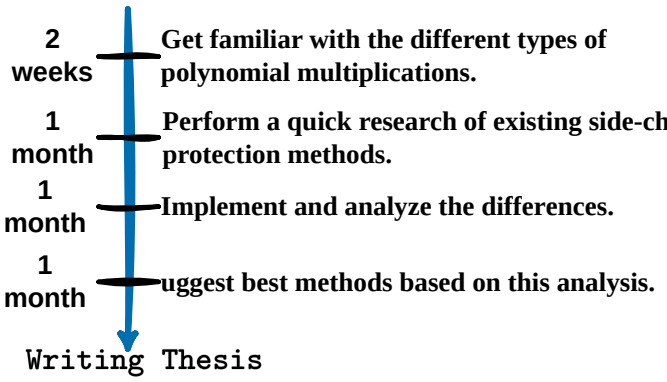
DATE: June 15, 2023

Motivation

The lattice-based post-quantum schemes (PQC) consist of two giant building blocks, Keccak and polynomial multiplier. They deal with security-critical components and therefore require side-channel protections. There are various methods to protect Keccak, however very few ingenious ways for the polynomial multiplier based on scheme specifications.

Thus, this thesis would aim at analyzing the naive methods and compare them with the newly proposed scheme-specific optimized methods. This analysis would be performed for multiple lattice-based PQC schemes in Software. Depending on the interest it can further be extended to Hardware. The icing on the cake would be a new method that can surpass the existing methods.

Goals and Tasks



Literature

- Aikata Aikata, Andrea Basso, Gaetan Cassiers, Ahmet Can Mert, and Sujoy Sinha Roy
  Kavach: Lightweight masking techniques for polynomial arithmetic in lattice-based cryptography
  https://eprint.iacr.org/2023/517

Courses & Deliverables

- ☑ **Introduction to Scientific Working**
  Short report on background
  Short presentation
- ☑ **Bachelor Project**
  Project code and documentation
- ☑ **Bachelor's Thesis**
  Project code
  Thesis
  Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in the topic area
- Basic knowledge of programming in C/C++ (for SW) or Verilog/VHDL (for HW)

Advisor Contact

aikata@iaik.tugraz.at

Analysis of polynomial multipliers for Post-quantum schemes in Software

Advisor: **Aikata**

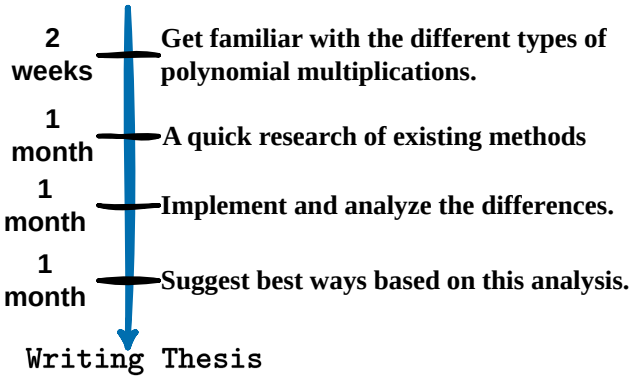
DATE: June 15, 2023

Motivation

Polynomial multiplication is the major building block in all lattice-based Post-quantum schemes. The literature presents several methods to perform this, however, it is difficult to gaze at the advantage or disadvantages of one approach over the other. This, not only depends on the scheme specification but also the environment under consideration.

The purpose of this thesis would be to pick distinct lattice-based schemes and analyze different multiplication methods. In conclusion, the best methods should be presented in software along the dimension of lightweight, and high-speed designs.

Goals and Tasks



Literature

- Matthias J. Kannwischer
  Polynomial Multiplication for Post-Quantum Cryptography
  https://kannwischer.eu/thesis/phd-thesis-print-version.pdf

Courses & Deliverables

- ☑ **Introduction to Scientific Working**
  Short report on background
  Short presentation
- ☑ **Bachelor Project**
  Project code and documentation
- ☑ **Bachelor's Thesis**
  Project code
  Thesis
  Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in the topic area
- Basic knowledge of programming in C/C++

Advisor Contact

aikata@iaik.tugraz.at