

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

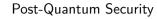
> iaik.tugraz.at



Outline

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

Privacy for Medical Applications





The Rivest-Shamir-Adleman (RSA) Scheme

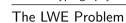


Lattice Cryptography Polynomial Rings



Lattice Cryptography

HAIK



Overview

[1]

Encoding and Decoding



Encryption and Decryption



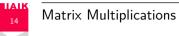
Homomorphic Addition

Demo: Secure MNIST Classification as a Service

Neural Networks



Implementation



$\frac{\text{Results}}{\text{Confusion everywhere}}$

Runtime Benchmarks



HAIK

vesuits



Ciphertext Visualisations

Conclusion

Crypto is good for us



Questions?

Glossary I

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.