IAIK

TU Graz

SCIENCE
PASSION
TECHNOLOGY

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

Post-Quantum Security

The Rivest-Shamir-Adleman (RSA) Scheme

Polynomial Rings

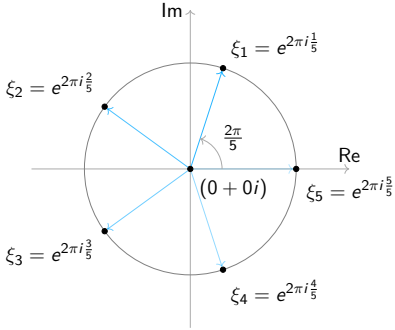

Figure: The 5^{th}roots of unity

The Learning With Errors (LWE) Problem

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

[1]

Encoding and Decoding

Encryption and Decryption

Homomorphic Addition

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	8
LWE	Learning With Errors	7
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.