Tianwei Zhang

tianwei.zhang@mpi-sp.org | +49 15753210347 | Bochum, Germany

Education

Ruhr University Bochum, Max Planck Institute for Security and Privacy, Ph.D. in Computer Science — Feb 2023 - Present

- **Supervisors**: Prof. Dr. Michael Walter (*RUB*), Prof. Dr. Giulio Malavolta (*Bocconi University*)
- **Research Area:** Lattice-based Cryptography and Quantum Cryptography

University of Bonn, M.Sc. in Mathematics — Oct 2020 - Jan 2023

- **Master Thesis**: Generalized High-Precision Fully Homomorphic Encryption Scheme (*sehr gut* 1.0)
- **Thesis Advisors**: Dr. Pieter Moree (*MPIM*), Prof. Dr. Jens Franke (*University of Bonn*)

Rutgers University, Undergraduate Exchange Program — Jan 2019 - May 2019

- **Graduate Courses taken**: Selected Topics in Geometry (Grade: A), Representation Theory (Grade: A), Abstract Algebra 2 (Grade: A), Lie Algebra (Grade: A)

Beijing Normal University, B.Sc. in Mathematics (LiYun Honors Program) — Sep 2016 - Jul 2020

- **GPA**: 3.88 / 4.0
- **Bachelor Thesis**: Moduli space of stable vector bundles over algebraic curve
- **Thesis Advisors**: Prof. Dr. Yao Yuan (*YMSC, Tsinghua University*), Prof. Dr. Zhiwei Wang (*BNU*)

Internship Experience

Research Intern in Privacy Enhancing Computing, *Clique* — Oct 2022 - Dec 2022

- Explore state-of-the-art zkSNARKs, with a focus on its application in Off-chain Data Availability problem.
- Deployed ZKP-based smart contracts for Web3 identity verification on the blockchain.

Algorithm Engineer Intern (Privacy Enhancing Computing), *Octa Information Technology Co., Ltd.* — Oct 2021 - Mar 2022

- Conducted advanced research in applied cryptography, specializing in Fully Homomorphic Encryption.
- Regularly shared cryptography expertise with engineering colleagues to enhance team knowledge and application of secure cryptographic methods within the company.

Research Assistant, *Yau Mathematical Sciences Center, Tsinghua University* — Sep 2020 - Sep 2021

- Organizer of weekly lattice-based cryptography seminar joint with several graduate students of University of Chinese Academy of Sciences.

Research Assistant, *Hong Kong University of Science and Technology* — July 2019 - Aug 2019

- Conducted an in-depth study of the Vafa-Witten Conjecture under the guidance of Prof. Dr. Weiping Li, gaining expertise in constructing moduli spaces of semi-stable coherent sheaves on ruled surfaces.

Publications

Time-Lock Puzzles from Lattices — 2024

Shweta Agrawal, Giulio Malavolta, ***Tianwei Zhang***. Crypto 2024

Registration-Based Encryption from Homomorphic Encodings — 2024

Nico Döttling, Xiuquan Ding, Giulio Malavolta, ***Tianwei Zhang***.

DEBPIR: Doubly Efficient Batched Private Information Retrieval — 2023

Xiuquan Ding, Giulio Malavolta, ***Tianwei Zhang***. ePrint

Projects

Lattice-based Registration-Based Encryption 2024

- Designed a novel Registration-Based Encryption (RBE) scheme from homomorphic encodings.
- Implemented the RBE in `C++` using the openFHE framework and conducted benchmarks against previous lattice-based RBE schemes.
- Achieved a 13.5-fold reduction in ciphertext size and a 20% increase in encryption speed compared to the best prior lattice-based RBE implementations.

Cryptography with Rust 2023

- Provides diverse implementations of lattice-based cryptographic schemes, constructions, and primitives, including the Kyber KEM scheme and an RNS-variant of the CKKS-FHE scheme, marking the first Rust port of the original `C++` code.
- Enable researchers and students in this area to efficiently prototype lattice-based cryptographic schemes.

Professional Activities and Service

Conference Reviewing

- EUROCRYPT 2025
- ASIACRYPT 2024
- TCC 2024

Teaching Assistant of *Ruhr University Bochum*

- Quantum Information and Computation – Winter 2023/2024
- Advanced Quantum Information and Computation – Summer 2024
- Quantum Information and Computation – Winter 2024/2025

Extracurricular Activities

Student Leader, *Sports Department, Beijing Normal University Student Union* Sep 2016 - May 2017

- Led the Sports Department in organizing and supporting numerous university sports events, including campus Badminton competitions.
- Captured exciting moments for each match with cameras.

Core Member, *Beijing Normal University Science Fiction Association* Sep 2016 - Aug 2018

- Participated in science fiction authors fans meetings, shared personal views on science fiction movies.

Professional Skills

Programming Languages: Proficient in `C++`, Rust; familiar with Python, Java.

Fully Homomorphic Encryption (FHE): BGV, BFV, GSW, TFHE, CKKS protocols, and their optimizations. Experience with OpenFHE library.

Secure Multi-Party Computation (MPC): Familiar with protocols such as GMW, GC, ABY 1.0, and SPDZ; knowledgeable in OT and OT extension technologies.

Zero-Knowledge Proof (ZKP): Proficient in zkSNARK protocols such as Groth16, Plonk, Bulletproof; skilled in Circom language.

Blockchain Technology: Familiar with Smart Contract development in Solidity and the Substrate framework.