Guo Yanpei

✉ gyp2847399255@gmail.com · ☎ (+86) 13693134669

Education

Beihang University (BUAA), Beijing, China 2019 – 2023

B.S. in School of Computer Science and Engineering, GPA: 3.78 / 4.00

Publication

Fast RS-IOP Multivariate Polynomial Commitments and Verifiable Secret Sharing

Zongyang Zhang*, Weihan Li*, **Yanpei Guo***, Kexin Shi, Sherman S. M. Chow, Ximeng Liu, Jin Dong

USENIX Security Symposium (Security), 2024, Co-first Author.

Achievements:

- Rolling-batch FRI technique, batch proving proximity of multiple vectors with Reed-Solomon codes of different length. **This technique has been applied in open-source zero-knowledge project Plonky3**.
- PolyFRIM, a multivariate polynomial commitment from RS code, leveraging rolling batch FRI, 5 times faster than prior work.
- One-to-many proof for proving multiple evaluations to multiple verifiers based on PolyFRIM, accelerating proving by 4 times.
- An asynchronous verifiable secret sharing (AVSS) scheme FRISS with a dealer complexity of $O(n^2 \log n)$.

My Duty: Protocol design and proof, experiments

Manuscript

Succinct Hash-based Arbitrary-Range Proofs

Zongyang Zhang, Weihan Li, **Yanpei Guo**, Sherman S. M. Chow, Zhiguo Wan

Submitted to *IEEE Transactions on Information Forensics and Security(TIFS)*

Achievements:

- A plausible post-quantum secure range proof (RP).
- A general bit-composition framework for ZK-RPs.

My Duty: Experiments

Doubly-Efficient Multilinear Polynomial Commitment from Reed-Solomon Code and Its Applications to Zero Knowledge Proof

Yanpei Guo, Kexi Huang, Tianyang Tao, Jiaheng Zhang

Submitted to *S&P, 2025*, First Author

Achievements:

- Deepfold, a multilinear polynomial commitment scheme that achieves nearly identical prover time, verifier time, and proof size as DEEP-FRI. It has about 3.5 times faster prover time or 3 times smaller proof size than prior work.
- A batch variant of Deepfold, reducing the prover time by half while adding no additional overhead to the proof size.

- A high-performance zero-knowledge argument system, by combining Deepfold with Libra.

My Duty: Protocol design and proof, experiments, paper writing

Skills

- Programming Languages: Rust, C++, Golang, Python, Vue, SQL
- Platform: Linux
- Development: Database, Back-end, Front-end

Honors and Awards

National Cryptographic technology Competition 2023, *First Prize*

Computer System Development Capability Competition, Operating System Kernel Design 2022, *First Prize, First Place*

Achievements:

- Developed a microkernel operating system in C, compatible with QEMU and SiFive FU740 platforms.
- Integrated support for Busybox, Lua, Redis, GCC, and Vim.
- Significantly enhanced the FAT32 file system with optimizations that improve performance by up to two times compared to Linux in certain benchmarks.

International Collegiate Programming Contest (ICPC) Asia Regional Contest Jinan Site 2020, *Silver Medal, the 54th Place*

The Chinese Mathematics Competitions for College Students (CMC) 2020, *First Prize*

TA experience

Computer Organization, Beijing, China 2022.07 – 2023.01

Superviaor: Xiaopeng Gao, School of Computer Science and Engineering, Beihang University

Operating System, Beijing, China 2021.01 – 2022.06

Superviaor: Lei Wang, School of Computer Science and Engineering, Beihang University

Computer Organization, Beijing, China 2021.07 – 2022.01

Superviaor: Xiaopeng Gao, School of Computer Science and Engineering, Beihang University

Language

TOEFL: Reading 28, Listening 23, Speaking 22, Writing 27 2024.04