GUO YANPEI

✉ guo.yanpei@outlook.com · ☎ (+65) 80846903

🎓 EDUCATION

Beihang University (BUAA), Beijing, China   2019 – 2023
B.S. in School of Computer Science and Engineering, GPA: 3.78 / 4.00

National University of Singapore (NUS), Singapore   2024
Research Assistance in School of Computing

National University of Singapore (NUS), Singapore   2025 – 2029
Ph.D. in School of Computing

📕 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

Succinct Hash-based Arbitrary-Range Proofs

Zongyang Zhang, Weihan Li, **Yanpei Guo**, Sherman S. M. Chow, Zhiguo Wan
IEEE Transactions on Information Forensics and Security(TIFS)
My Duty: Experiments

DeepFold: Efficient Multilinear Polynomial Commitment from Reed-Solomon Code and Its Application to Zero-knowledge Proofs

Yanpei Guo, Xuanming Liu, Kexi Huang, Wenjie Qu, Tianyang Tao, Jiaheng Zhang
USENIX Security Symposium (Security), 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

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

Computer Security, CS3235, Singapore   2025.01 – 2025.05
Superviaor: Jiaheng Zhang, School of Computing, National University of Singapore

✹ LANGUAGE

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