Yansong Feng

Website: https://www.fffmath.com
Github: https://github.com/fffmath

Email: fengyansong@amss.ac.cn
Mobile: +86-188-2203-2054

Summary

My research interests are primarily centered around cryptography and security, particularly in the domains of Lattice-based Cryptography and Succinct Zero-Knowledge Proofs.

Education

- **Chinese Academy of Sciences (CAS)** — Beijing, China
  Academy of Mathematics and Systems Science (AMSS) — *Sept. 2022 - Current*
  Ph.D. in Applied Mathematics (Expected) — *GPA: 3.76/4*
  Courses: *Modern Cryptography, Error Correcting Code, Computational Algebraic Geometry, Computer Algebra*

- **Nankai University** — Tianjin, China
  Bachelor of Science - Pure Mathematics and Applied Mathematics — *Sept. 2018 - Jun. 2022*
  *Chern Class (**Honor Class**), named after Shiing-Shen Chern* — *GPA: 3.56/4*
  Courses: *Abstract Algebra, Representation Theory of Finite Groups, Dynamical System, Associative Algebra*

Research Experience

- **Secure Multi-Party Computation from Post-quantum Cryptography** — Aarhus, Denmark
  Crypto Group, Aarhus University. — *Oct. 2024 - Sept. 2025*
  - **Hosted by**: Diego F. Aranha.
  - **Status**: TBD.
  - **Achievements**: TBD.

- **Trusted Collaboration of Identity and Data Based on ZKP** — HongKong, China
  Department of Computing, PolyU — *Jun. 2024 - Sept. 2023*
  - **Hosted by**: AU Man Ho Allen.
  - **Status**: Doing some research on a topic about Lattice based polynomial commitment scheme.
  - **Achievements**:
    * Read several chapters of A Graduate Course in Applied Cryptography.
    * Carefully read the papers on Lattice based polynomial commitment scheme.

Publications

- **Small Public Exponent Brings More: Improved Partial Key Exposure Attacks against RSA**: Yansong Feng, Abderrahmane Nitaj, Yanbin Pan, Communications in Cryptology (2024) https://eprint.iacr.org/2024/1329.pdf
- **Embedding Integer Lattices as Ideals into Polynomial Rings**: Yihang Cheng, Yansong Feng, Yanbin Pan, accepted by International Symposium on Symbolic and Algebraic Computation - 49th International Conference (ISSAC), 2024 https://arxiv.org/abs/2307.12497
- **Partial Prime Factor Exposure Attacks on Some RSA Variants**: Yansong Feng, Abderrahmane Nitaj, Yanbin Pan, Theoretical Computer Science (2024) https://doi.org/10.1016/j.tcs.2024.114549
- **Generalized Implicit Factorization Problem**: Yansong Feng, Abderrahmane Nitaj, Yanbin Pan, accepted by Selected Areas in Cryptography - 30th International Conference (SAC), 2023 https://eprint.iacr.org/2023/1562

Projects

- **Useful-Links**: It's a webpage designed to provide many useful links related to cryptography. https://link.fffmath.com
- **Identifying-Ideal-Lattice**: A toolkit for identifying whether the input lattice is an ideal lattice or not. https://github.com/fffmath/Identifying-Ideal-Lattice

Honors and Awards

- HUA Scholarship of AMSS (100,000 RMB) - Sept. 2024
- Top Prize of the 9th (2024) National College Cryptomath Challenge (60,000 RMB) - Aug. 2024

Skills Summary

- **Programming**: Python (Sagemath, Pandas, NumPy, Scikit-learn. etc.), C++ (makefile, unit tests).
- **Tools**: Linux, Shell (Bash/Zsh), LaTeX(Overleaf), Microsoft Office, Git (version control).
- **Soft Skills**: Leadership, Event Management, Writing, Public Speaking, Time Management