

Yansong Feng

Website: <https://www.ffmpegath.com>
Github: <https://github.com/ffmpegath>

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

SUMMARY

My research interests primarily revolve around Algorithms & Theory, particularly in 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
- Aarhus University** Aarhus, Denmark
• *Visiting PhD Student* Oct. 2024 - Oct. 2025
- 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

- Yansong Feng, Abderrahmane Nitaj, Yanbin Pan. Newton Polytope-Based Strategy for Finding Roots of Multivariate Polynomials..** In submission. <https://eprint.iacr.org/2024/1330.pdf>
- Yansong Feng, Abderrahmane Nitaj, Yanbin Pan. Small Public Exponent Brings More: Improved Partial Key Exposure Attacks against RSA.** Communications in Cryptology (2024). <https://eprint.iacr.org/2024/1329.pdf>
- Yihang Cheng, **Yansong Feng**, Hengyi Luo, Yanbin Pan. **Solving γ -SVP in Order-Ideal Lattices.** In submission.
- Yihang Cheng, **Yansong Feng**, Yanbin Pan. **Embedding Integer Lattices as Ideals into Polynomial Rings.** ISSAC'24. <https://eprint.iacr.org/2024/1041>
- Yansong Feng, Abderrahmane Nitaj, Yanbin Pan. Partial Prime Factor Exposure Attacks on Some RSA Variants.** Theoretical Computer Science (2024). <https://doi.org/10.1016/j.tcs.2024.114549>
- Yansong Feng, Abderrahmane Nitaj, Yanbin Pan. Generalized Implicit Factorization Problem.** SAC'23. <https://eprint.iacr.org/2023/1562>

PROJECTS

- Useful-Links:** It's a webpage designed to provide many useful links related to cryptography. <https://link.ffmpegath.com>
- Identifying-Ideal-Lattice:** A toolkit for identifying whether the input lattice is an ideal lattice or not. <https://github.com/ffmpegath/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), L^AT_EX(Overleaf), Microsoft Office, Git (version control).
- Soft Skills Leadership, Event Management, Writing, Public Speaking, Time Management