Yansong Feng

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

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

Summary

Currently I'm a Phd student majoring in Cryptography, interested in lattice based Cryptography, complexity proof and provable security.

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

- **Lattice-Based Cryptography Seminar** — Beijing, China
  Student — *Sept. 2022 - Jun. 2023*
  - **Instructor**: Yanbin Pan.
  - **Status**: Completed the exercises in the notes of Oded Regev and accomplished one paper.
  - **Duties and Achievements**:
    * Read Regev's classical lecture notes.
    * Accomplished one paper. This paper is about the Implicit Factorization Problem. We find a result on the general case which is accepted by SAC 2023, Canada.

Publications

- **Embedding Integer Lattices as Ideals into Polynomial Rings**: Yihang Cheng, Yansong Feng, Yanbin Pan, under submission https://arxiv.org/abs/2307.12497
- **Provable Automated Coppersmith for Linear Equations and its Applications**: Yansong Feng, Abderrahmane Nitaj, Yanbin Pan, under submission
- **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
- **On Rangasamy's outsourcing algorithm for solving quadratic congruence equations** : Xiulan Li, Yansong Feng, Yanbin Pan https://arxiv.org/abs/2203.10751

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

- First Prize in North Zone of The 7th National College Cryptomath Challenge - Nov. 2022
- First Prize in Tianjin of Mathematical Competition for College Students - Sept. 2020
- First Prize in Hebei Province of Middle School Mathematics Competition - Aug. 2017

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