

Yansong Feng

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

Email: ysfeng2023@163.com
Mobile: +86-188-2203-2054

SUMMARY

Enrolled in the autumn of 2022, currently a second year master's 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
MSc in Applied Mathematics (Expected) GPA: 3.75/4
Courses: 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: Differential Geometry, Differential Manifold, Representation Theory of Finite Groups, Dynamical System, Associative Algebra

SKILLS SUMMARY

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

RESEARCH EXPERIENCE

- **Lattice-Based Cryptography Seminar** Beijing, China
Student Sept. 2022 - Current
 - **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.

PROJECTS

- **xxx:** xxxxxx
- **xxx:** xxxxxx

PUBLICATIONS

- **Generalized Implicit Factorization Problem:** Yansong Feng, Abderrahmane Nitaj, Yanbin Pan, accepted by Selected Areas in Cryptography - 30th International Conference, SAC 2023
- **On Rangasamy's outsourcing algorithm for solving quadratic congruence equations:** Xiulan Li, Yansong Feng, Yanbin Pan, CoRR abs/2203.10751 (2022)
- **Partial Prime Factor Exposure Attacks on Some RSA Variants:** Yansong Feng, Abderrahmane Nitaj, Yanbin Pan, under submission

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

VOLUNTEER EXPERIENCE

- **Volunteer at the Museum of Paleontology** Beijing, China
Assist staff and help visitors at the Museum of Paleontology. Mar. 2023
- **Volunteer of Yuyuantan Park** Beijing, China
Assist staff and help visitors at Yuyuantan Park. Mar. 2023