Kaixing Wang

Home Page: https://wangkaixing.github.io
Github: https://github.com/Wangkaixing

Email : ucaswkx@gmail.com
Mobile : +86-151-6677-2838

Education

- **University of Chinese Academy of Sciences** — Beijing, China
  Masters of Electronic Information and Engineering; GPA: 3.86 — *Aug 2022 - Current*
  Courses: Cryptanalysis, Introduction to Data Science, The Security of Computer Network and Information System, Foundation of Computational Complexity Theory, Lattice Based Cryptography, Public Key Cryptography and Applied Cryptography

- **Xiamen University** — Xiamen, China
  Bachelor of Computer Science; GPA: 3.39 — *Sep 2018 - Jun 2022*
  Courses: Operating Systems, Analysis Of Algorithms, Pattern Recognition, Principle of Computer Composition, Probability and Statistics, Calculus, Discrete Mathematics and Finance.

Publications

- Binwu Xiang, Jiang Zhang, **Kaixing Wang**, Yi Deng, Dengguo Feng, "NTRU-based Bootstrapping for MK-FHEs without using Overstretched Parameters." **Asiacrypt 2024**
- **Kaixing Wang**, Binwu Xiang, Jiang Zhang, "Improved FHE Bootstrapping and Its Applications in Privacy Preserving Inference of Discretized Neural Networks." (to be submitted)

Software Projects

- OpenFHE (a leading library for homomorphic encryption), https://github.com/openfheorg/openfhe-development

Experience

- **State Key Laboratory of Cryptology** — Beijing, China
  Visiting Student — *Jul 2023 - Current*
  - **Research on homomorphic encryption theory and implementation**: Conducted research on homomorphic encryption algorithms and developed corresponding implementations using the OpenFHE open-source library.
    - Proposed a new bootstrapping algorithm based on a GSW-like encryption from the NTRU assumption. And utilized the blind rotation algorithm as a building block to present new bootstrapping algorithms for both LWE and RLWE ciphertexts. The scheme features smaller key sizes and faster bootstrapping speeds.
    - Optimized the first algorithm by introducing a new bootstrapping framework which reduces the size of the key-swithing key from $\tilde{O}(n^2)$ to $\tilde{O}(n)$. It requires less than 3MB bootstrapping key and completes in merely 9ms at 128-bit security, significantly outperforming the state-of-the-art method by Xiang et al. (CRYPTO 2023) a 30x reduction in key size and a 1.5x speedup.
    - Conducted experiments to validate its performance in privacy preserving inference of discretized neural networks.

- **SpAtial Sensing and Computing Lab** — Xiamen, China
  Intern Student — *Nov 2021 - Jun 2022*
  - **Research on Healthcare Demand Based on Urban Spatial Big Data**: Based on the data of nucleic acid testing sites in Xiamen, worked on building a system that can reasonably predict future medical needs of the testing site.
    - Summarized and analyzed different statistical models and deep learning models and combined the multi-step prediction strategy, the medical demand was predicted from both time and space dimensions.
    - Used the multi-step prediction method to continuously predict the crowding degree of nucleic acid test sites for several hours in the future.
    - Used Apache ECharts framework to visually display the basic information of each detection point, such as congestion, street pictures, geographic location, etc., through web pages.

Academic Projects

- **Nachos Concurrent Programming (Kernel Programming)**: Implemented synchronisation mechanisms on the Nachos virtual machine and used these to implement thread-safe table structures and several other tool classes. (Apr '21)
- **TCP Congestion Control Algorithm Simulation (Networking)**: Used the ns-3 Internet module to compare the impact of NewReno, High Speed, Veno, and Bic on transmission performance in different network environments to deepen the understanding of various congestion control algorithms. Utilized ns-3 simulation programming and Wireshark packet analysis. (Dec '20)

Honors and Awards

- Honorary Title of 'Triple-A' Student, University of Chinese Academy of Sciences 2022-2023.
- Third Prize of the Zhengyuan Cryptography Outstanding Student Award, University of Chinese Academy of Sciences 2023.
- Merit Student Scholarship, School of Informatics, Xiamen University 2020-2021.
- Merit Student Scholarship, School of Informatics, Xiamen University 2019-2020.
- First Prize in Shandong Provincial High School Mathematics Competition, 2017
- National First Prize in the National High School Students' English Proficiency Competition, 2017

Skills Summary

- Proficient in C/C++, Python, Linux scripting
- Proficient in Sage, Matlab, LaTeX