Tao Chen

📱 +086 157 5563 8830 | @ vageous@std.uestc.edu.cn | GitHub | 🌐 Portfolio | 📍 Chengdu, Sichuan, China

Education

Xi’an University of Posts & Telecommunications — Xian, China
B.Sc. in Information Security; ***GPA: 3.58/4.00*** — *Sep 2017 – Jul 2021*

University of Electronic Science and Technology of China — Chengdu, China
M.Sc. in Cryptography; ***GPA: 3.45/4*** — *Sep 2021 – Present*

Research Experience

Ciphertext Deduplication for Secure Cloud Storage — XUPT, Xian, Shanxi
Undergraduate Student — *Feb 2020 – Jul 2021*

- worked in the laboratory of Prof. Meixia Miao with her master students on a project about ciphertext deduplication for cloud storage.
- completed my dissertation ”A Lightweight Ciphertext Deduplication Technology with Public Data Auditing” supervised by Prof. Meixia Miao and Dr. Guohua Tian who studied at Xidian University.

Applied Cryptography & Federated Learning — UESTC, Chengdu, China
Master Student — *Sep 2021 – present*

- worked with Prof. Xiaofen Wang on the project ”Privacy-preserving and Verfiable Decentralized Federated Learning”.
- studied homomorphic encryption consisting of single-key homomorphic encryption and multi-key homomorphic encryption and designed a new notion of homomorphic encryption called multi-key homomorphic encryption with single-key decryption.
- studied identity-based broadcast encryption and designed a new identity-based broadcast encryption algorithm used to provide privacy protection and dropout tolerance for federated learning.
- studied functional encryption consisting of multi-input functional encryption, multi-client functional encryption, and decentralized functional encryption.

Publications

Papers

First Author (Accept) — IEEE International Conference on Communications

- Communication-Efficient Privacy-Preserving and Verifiable Federated Learning

First Author (Accept) — IEEE Global Communications Conference

- DTPP-DFL: A Dropout-Tolerated Privacy-Preserving Decentralized Federated Learning Framework

First Author (Accept) — IEEE Internet of Things Journal

- A Dropout-Tolerated Privacy-Preserving Method for Decentralized Crowdsourced Federated Learning

First Author (Manuscript in preparation) — IEEE Transactions on Information Forensics and Security

- An Efficient Privacy-Preserving and Verifiable Federated Learning Framework based on Multi-Key Homomorphic Encryption

First Author (Manuscript in preparation) — CT-RSA

- Decentralized Mulit-client Functional Encryption without private channels

Sixth Author (Under Review) — Peer-to-Peer Networking and Applications (PPNA)

- An Efficient Blockchain-Based Self-Tallying Voting Protocol with Full-Anonymity

Third Author (Accept) — The Sixth International Conference on Frontiers in Cyber Security

- ASEV: Anonymous and Scored-Based E-Voting Protocol on Blockchain

Patents

- A Verifiable Privacy-Preserving Federated Learning Method and System.
- A Certificateless Anonymous Cross-Domain Authentication Method for IoT devices based on Blockchain.
- An Efficient Fully Anonymous Self-Counting Voting Method Based on Blockchain.

Projects

Programming Projects

Multi-receiver anonymous signcryption for crowdsourced IoMT | *GitHub* Finished

- A python project which implements a multi-receiver anonymous signcryption algorithm used for trusted health data collection in Internet-of-Medical-Things and reproduces an existing multi-receiver signcrption scheme.
- The multi-receiver anonymous signcrytion integrates the attribute-based credential (ABC) and the identity-based multi-receiver encryption technologies, which can achieve fine-grained, privacy-preserving authentication and satisfy the necessary properties of traceability and non-repudiation.

A privacy-preserving and verifiable federated learning | *GitHub* Finished

- A python project which implements a privacy-preserving and verifiable federated learning framework, this project consists the following aspects: 1) a novel multi-key homomorphic encryption called multi-key homomorphic encryption with single-key decryption used for providing privacy protection for federated learning; 2) a vector homomorphic hash function used for federated learning, which can ensure the integrity of the local model and global model; 3) A reproduction of two existing traditional multi-key homomorphic encryption schemes used for federated learning and a comparison of overhead between these two schemes and the novel multi-key homomorphic encryption scheme.

A reproduction of poisoning attacks and defence in federated learning | *GitHub* Finished

- A python project which implements some poisoning attacks, such as label-flipping attacks and model replacing attacks and the corresponding defense strategies, such as Krum, Multi-Krum, and Bulyan.

A novel ID-based homomorphic broadcast encryption & Federated learning | *GitHub* Finished

- This project consists of a novel identity-based homomorphic broadcast encryption algorithm with aggregation decryption used for federated learning, which can provide privacy protection. Besides, the new identity-based broadcast encryption can support dropout tolerance, which means that no matter how many clients drop out from the federated learning system, it can still correctly provide privacy protection.

Writing Projects

A fund declaration about a decentralized secure federated learning framework. Finished

- This project is a declaration of the National Natural Science Foundation project, which has already been granted, and the main content is about a blockchain-based privacy-preserving and verifiable decentralized federated learning framework for medical treatment. The serial number is 62372092.

A brochure of a Go homomorphic encryption library Lattigo.| *GitHub* Ongoing

- In this project, I'm writing a brochure for a homomorphic encryption library called Lattigo, which includes explanations about how to use these functions and the rationales for some functions in Lattigo. The brochure is in Chinese now but I will translate it to English in the future.

Skills

Programming: C, C++, Python, MATLAB, Go

Cryptographic Libraries:(Python) Crypto, Pyseal, Pypbc, Gmpy2; (C& C++): SEAL, Relic, GMP, NTL, CiFEr, Miracle; (Go) Lattigo

Languages: Chinese (Native), English (IELTS 6.0)

Relevant Coursework

Major coursework: Modern Cryptography, Machine Learning, Number Theory, Abstract Algebra, Computer Network, Data Structures and Algorithms, Graph Theory

Minor coursework: Theory of Combinatorial Design and Optimization, Internet Security, Cloud Computing, The general theory of information security