

# SHIYU LI

shaili0106@gmail.com <https://shiyuuli.github.io>

## EDUCATION

<b>University of Electronic Science and Technology of China</b> M.Eng. in Cybersecurity Advisor: Prof. Yuan Zhang	Sept. 2021 - Jun. 2024 (expected) GPA: 3.75/4.00
<b>University of Memphis</b> Visiting Student in Computer Science Advisor: Prof. Kan Yang	Jan. 2023 - Mar. 2023
<b>University of Electronic Science and Technology of China</b> B.Eng. in Information Security	Sept. 2017 - Jun. 2021 GPA: 3.87/4.00

## CORE COURSE

### Undergraduate

Calculus, Discrete Mathematics, Linear Algebra and Space Analytic Geometry, Mathematical Foundations of Information Security, Data Structure and Algorithm, Information Theory and Coding Theory, Cryptography, Computer Operating Systems, Computer Networks, Computer Architecture

### Graduated

Abstract Algebra, Number Theory, Modern Cryptography, Security Protocols and Standards

## PUBLICATION & MANUSCRIPT

- [1] **S. Li**, Y. Zhang, C. Xu, Y. Song, N. Cheng, Z. Liu, Y. Du, and X. Shen. “HealthFort: A Cloud-Based eHealth System with Conditional Forward Transparency and Secure Provenance via Blockchain”. *IEEE Transactions on Mobile Computing* (IF 7.9), vol. 22, no. 11, pp. 6508 – 6525, 2022. <https://doi.org/10.1109/TMC.2022.3199048>.
- [2] **S. Li**, Y. Zhang, N. Cheng, and Y. Song. “Badge: Blockchain-Assisted Secure Authenticated Data Transmission in Mobile Edge Computing”. *IEEE International Conference on Communications*, pp. 4757 - 4762, 2022. <https://doi.org/10.1109/ICC45855.2022.9838606>.
- [3] **S. Li**, Y. Zhang, C. Xu, N. Cheng, Z. Liu, and X. Shen. “BESURE: Blockchain-Based Cloud-Assisted eHealth System with Secure Data Provenance”. *IEEE/ACM International Symposium on Quality of Service*, pp. 1 - 6, 2021. <https://doi.org/10.1109/IWQOS52092.2021.9521289>.
- [4] Y. Song, C. Xu, Y. Zhang, and **S. Li**. “Hardening Password-Based Credential Databases”. *IEEE Transactions on Information Forensics and Security* (IF 6.8), to appear, 2023. <https://doi.org/10.1109/TIFS.2023.3324326>.
- [5] **S. Li**, Y. Zhang, Y. Song, K. Yang, F. Wu, F. Lyu, and Q. Tang. “EpiOracle: Privacy-Preserving Cross-Facility Early Warning for Unknown Epidemics”. (In Submission) <https://eprint.iacr.org/2023/1779.pdf>.
- [6] **S. Li**, Y. Zhang, Y. Song, H. Liu, N. Cheng, H. Li, and K. Yang. “Beyond Security: Achieving Fairness in Mailmen-Assisted Timed Data Delivery”. (In Submission) <https://eprint.iacr.org/2023/1775.pdf>.
- [7] Y. Song, Y. Zhang, **S. Li**, W. Li, Z. Lai, and Q. Tang. “There Is Always a Way Out! Destruction-Resistant Key Management: Formal Definition and Practical Instantiation”. (In Submission) <https://eprint.iacr.org/2023/1785.pdf>.

## RESEARCH EXPERIENCE

---

### Tradeoffs between Privacy and Utility in eHealth

Mar. 2021 - present

Mentor: Prof. Yuan Zhang, Prof. Kan Yang

- **Background.** The deployment of eHealth systems significantly enhances the utility of healthcare data. However, substantial privacy concerns arise when using this data due to its sensitive nature. Our goal is to maintain the utility of healthcare data while ensuring a reasonable level of privacy.
- **Action.** Developed an *eHealth system with conditional forward transparency to preserve individual privacy*, allowing a patient to efficiently authorize a doctor to access only necessary information. Proposed an *early epidemic warning scheme to preserve group privacy*, in which frequencies of symptoms among all patients are monitored while not leaked to any unrelated party. Completed papers [1], [5].
- **Result.** This project could encourage patients and healthcare facilities to contribute their healthcare data by providing privacy preservation. It is promising for a more diverse and comprehensive data pool available for research, facilitating the development of innovative techniques in healthcare.

### Trustworthy Electronic Voting

Mar. 2022 - Mar. 2023

Mentor: Prof. Yuan Zhang, Prof. Kan Yang

- **Background.** Electronic voting is widely deployed for elections. To protect voters from becoming a coercion target, each vote should be public only after a specified period. While some approaches leverage time-locked puzzles to send votes “into the future”, they suffer from a practical issue: fail to allow voters to precisely control the arrival time of votes. To overcome this limitation, other approaches employ a set of mailmen for vote delivery, where the security is based on the honesty of the mailmen.
- **Action.** Defined fairness in the context of mailmen-assisted timed-data delivery in electronic voting. Proposed a mailmen-assisted timed-data delivery with defined fairness, where mailmen are incentivized to faithfully adhere to the prescribed delivery mission. Completed paper [6].
- **Result.** The timed-data delivery with fairness in this project could contribute to trustworthy electronic voting by achieving secure delivery of votes and protecting voters from potential coercion, which could lead to increased voter turnout.

## AWARD & SCHOLARSHIP

---

### Third Prize in National Cryptographic Technology Competition

2023

Chinese Association for Cryptographic Research

### National Scholarship

2022

Ministry of Education of the People's Republic of China

### Honored Graduate

2021

University of Electronic Science and Technology of China

### First Prize in National College Student Information Security Contest

2020

Ministry of Education of the People's Republic of China