# XINSHU MA

+44 (0)7512-184-378 • maxinshusu@gmail.com • Homepage: sus0pid.github.io/

## EDUCATION

**Phd, Network Security** 2021 - present
University of Edinburgh, Edinburgh, UK
School of Informatics
Supervisor: Michio Honda

**Master, Cyberspace Security** 2017 - 2020
Nanjing University of Aeronautics and Astronautics, Nanjing, China Outstanding dissertation
College of Computer Science and Technology
Supervisor: Zhe Liu

**Bachelor, Computer Science** 2013 - 2017
Nanjing University of Aeronautics and Astronautics, Nanjing, China GPA 91/100, Ranking 1/281
College of Computer Science and Technology

## INTERNSHIP

**Singapore University of Technology and Design (SUTD), Singapore: Research Intern** Feb 2019 – May 2019

- Supervisor: Dr. Pawel Szalachowski
- Topic: **Security Analysis of PoW Consensus algorithm**
- Applied Markov Decision Process (MDP) to model the adversary's behaviour in order to find the optimal Selfish Mining Attack Strategy on the StrongChian (Usenix'19) PoW consesnsus algorithm and the maximum profit that the adversary can get.
- Authored a technical report for the complete security analysis of StrongChain.

## SELECTED ACADEMIC PROJECTS

**Homals: A Secure Datacenter Transport Protocol with low latency** Sept 2023 - now
Enabling datacenter connections with confidentiality and authentication.

- Dive deep into TLS1.3 and QUIC design and implementation.
- Design the handshake protocol that fits datacenter scenario.

**In Mixnet We Trust? REMOTE: A Reliable Mixnet (Re)Configuration** July 2022 – July 2023
Removed the reliance on single trusted third party in constructing a decentralized network with outsourced resources.

- Design goals: unbiased mixnet construction, eclipse attack resistance, guarantee of nodes participation fairness.
- Transparency Logs, Applied cryptographic primitives: verifiable random function, merkle tree, threshold signature.

**Defending against Malicious Mixes with Topological Engineering** Mar 2021 - April 2022
Suggested re-engineering mixnet construction and using guard layer idea to lower the risk of users being de-anonymized.

- Pointed conflicting observation: almost 100% users will fall into a fully malicious path within one week.
- Published a paper at ACSAC'2022 and release source code (Python & Rust).

## ADDITIONAL EXPERIENCE

**Sandia National Laboratories, Austin, US: TracerFIRE (Forensic and Incident Response Exercise)** Dec 2022

- Performed forensic analysis on infected machines and memory images; traffic analysis via Wireshark; reverse engineering of malicious binaries with Ghidra.

**Udemy, Online: Build an custom HTTP server from scratch with Rust** Oct 2021 - Dec 2021

- Understood Rust such as ownership, references & borrowing, and memory model.

## PUBLICATIONS

1. Xinshu Ma, Florentin Rochet, Tariq Elahi: Stopping Silent Sneaks: Defending against Malicious Mixes with Topological Engineering. In Proceedings of the 38th Annual Computer Security Applications Conference, pp. 132-145. **ACSAC** 2022.

2. Chunpeng Ge, Xinshu Ma, Zhe Liu: A Semi-autonomous Distributed Blockchain-based Framework for UAVs Communication Systems. Journal of Systems Architecture. **JSA** 2020, 107: 101728.

3. Xinshu Ma, Chunpeng Ge, Zhe Liu: Blockchain-Enabled Privacy-Preserving Internet of Vehicles: Decentralized and Reputation-Based Network Architecture[C]. In International Conference on Network and System Security. Springer, Cham, 2019: 336-351. **NSS** 2019. Best Paper Award

4. Xinshu Ma, Xiaojun Zhu*, Bing Chen: Exact algorithms for maximizing lifetime of WSNs using integer linear programming. In 2017 IEEE Wireless Communications and Networking Conference (pp.1-6). IEEE. **WCNC** 2017.

5. Xinshu Ma, Youwen Zhu*, Xingxin Li: An efficient and secure ridge regression outsourcing scheme in wearable devices[J]. Computers & Electrical Engineering, 63: 246-256. Elsevier **CEE** 2017.

* PRC Patent Application No.: 201610659332.X, Publication No.: CN106131878A, A kind of data collection method for energy heterogeneous wireless sensor network, Xiaojun Zhu, Xinshu Ma and Jing Zhang, 2016.

## POSTER & TALKS

1. AUTONOMY: Auto-adaptive Well-behaved Anonymous Communication Systems
   **PoPETS'22 Workshop** on Interdependent and Multi-party Privacy (IDP),
   Sydney, Australia, July 2022.

2. Defending against Malicious Mixes with Topological Engineering
   **SICSA'22 PhD Conference**,
   Glasgow, UK, June 2022.

3. **Defending against Malicious Mixes with Topological Engineering**
   Laboratory for Foundations of Computer Science (LFCS) Lab Talk,
   Edinburgh, UK, May 2022.

4. Bow-Tie: Towards Secure Mix Network Topological Construction Algorithm
   **REPHRAIN All-Hands Meeting** Poster Session, Best Poster Award
   Bristol, UK, March 2022.

## SELECTED AWARDS AND HONOURS

| | |
|---|---|
| JUNE. 2023 | PoPETS Stipend (USD 1,610) |
| JUNE. 2023 | SICSA Research Scholarship (GBP 500) |
| MAR. 2022 | SICSA Research Travel Funding (GBP 500) |
| AUG. 2020 | First Prize of Jiangsu Province 'Internet Plus' Innovation and Entrepreneurship Competition |
| DEC. 2017 | Second Prize of Information Security and Countermeasures Contest |
| OCT. 2017 | **First Class Graduate Freshmen Scholarship** (CNY 20,000, 1/190) |
| 2017-2019 | First Class Graduates Scholarship (CNY 10,000/year) |
| 2017-2019 | Graduate Student Research Scholarship (CNY 6,000/year) |
| MAR. 2017 | **Third Prize of the Ministry of Industry and Information Technology Innovation Scholarship** (CNY 10,000) |
| NOV. 2016 | National Encouragement Scholarship (CNY 5000) |
| NOV. 2015 | **National Scholarship** (CNY 8000, 3/310) |
| 2015-2017 | First Class Undergraduates Scholarship (CNY 3500) |
| NOV. 2014 | Third Class Undergraduates Scholarship (CNY 1500) |

## TECHNICAL SKILLS

**Programming:** Python, C, Rust **Modeling Tools:** MATLAB, R **Language:** IELTS 7.0