XINSHU MA

+44 (0)7512-184-378 • x.ma@ed.ac.uk • Homepage: sus0pid.github.io/

EDUCATION

Ph.D. in Network Security 2021 - May 2026 (expected)
University of Edinburgh, Edinburgh, UK
School of Informatics
Supervisor: Michio Honda
Approved interruption: Aug 2023 – July 2024
Thesis: Towards Fast, Secure, and Privacy-preserving Networking

M.S. in Cyberspace Security 2017 - 2020
Nanjing University of Aeronautics and Astronautics, Nanjing, China Outstanding dissertation
College of Computer Science and Technology
Supervisor: Zhe Liu
Thesis: Towards Secure Data Sharing in Internet of Things Based on Blockchain

B.S. in Computer Science 2013 - 2017
Nanjing University of Aeronautics and Astronautics, Nanjing, China
College of Computer Science and Technology
Thesis: An Efficient and Secure Ridge Regression Outsourcing Scheme for Wearable Devices

SELECTED RESEARCH PROJECTS

Looma: A Low-Latency PQTLS Authentication Architecture for Cloud Applications NDSS'26
Looma re-architects PQTLS authentication to support fast mutual TLS handshake at datacenter scale. It achieves this by decoupling costly authentication operation from the latency-critical handshake path, enabling the handshake to use lightweight online signing/verification.

Designing Transport-Level Encryption for Datacenter Networks S&P'26
SMT integrates TLS-based encryption with message-oriented datacenter transports like NDP and Homa to provide secure, efficient RPC communication. It introduces per-message sequence spaces and unique message identities to prevent replay attacks while leveraging existing NIC TLS offloads.

Defending against Malicious Mixes with Topological Engineering ACSAC'22
This work enhances user anonymity in stratified Mixnets by addressing real-world vulnerabilities such as relay sampling, topology placement, and network churn that existing designs overlook. It introduces an engineered guard layer and client guard logic—adapting Tor's guard concept—to resist long-term deanonymization attacks.

RESEARCH EXPERIENCE

Research Intern, Singapore University of Technology and Design (SUTD), Singapore Feb 2019 – May 2019
Advisor: Dr. Pawel Szalachowski
Focus: Security Analysis of PoW Consensus algorithm by utilizing Markov Decision Process (MDP) to model the adversary's behaviour in order to find the optimal Selfish Mining Attack Strategy.

PUBLICATIONS

1. **Xinshu Ma**, Michio Honda: Looma: A Low-Latency PQTLS Authentication Architecture for Cloud Applications. In Network and Distributed Systems Security Symposium, NDSS 2026.
2. Tianyi Gao, **Xinshu Ma**, Suhas Narreddy, Eugenio Luo, Steven Chien and Michio Honda: Designing Transport-Level Encryption for Datacenter Networks. In 47th IEEE Symposium on Security and Privacy, S&P 2026.
3. **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, ACSAC 2022.
4. Chunpeng Ge, **Xinshu Ma**, Zhe Liu: A Semi-autonomous Distributed Blockchain-based Framework for UAVs Communication Systems. Journal of Systems Architecture. JSA 2020.

5. Shenqing Wang, Jianwang, Chunhua Su, **Xinshu Ma**: Intelligent Detection Algorithm Against UAVs' GPS Spoofing Attack. IEEE 26th International Conference on Parallel and Distributed Systems, ICPADS, 2020.
6. **Xinshu Ma**, Chunpeng Ge, Zhe Liu: Blockchain-Enabled Privacy-Preserving Internet of Vehicles: Decentralized and Reputation-Based Network Architecture. In International Conference on Network and System Security, NSS 2019. Best Paper Award
7. **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, WCNC 2017.
8. **Xinshu Ma**, Youwen Zhu*, Xingxin Li: An efficient and secure ridge regression outsourcing scheme in wearable devices. Computers & Electrical Engineering, Elsevier, 63: 246-256. CEE 2017.

POSTER & TALKS

1. Towards Fast Mutual PQTLS Handshake in Datacenters
   Coseners, UK Academic Meeting on Systems and Networks,
   Abingdon, UK July 2025.
2. AUTONOMY: Auto-adaptive Well-behaved Anonymous Communication Systems
   PoPETS'22 Workshop on Interdependent and Multi-party Privacy (IDP),
   Sydney, Australia, July 2022.
3. Defending against Malicious Mixes with Topological Engineering
   SICSA'22 PhD Conference,
   Glasgow, UK, June 2022.
4. Bow-Tie: Towards Secure Mix Network Topological Construction Algorithm
   REPHRAIN All-Hands Meeting Poster Session, Best Poster Award
   Bristol, UK, March 2022.

SERVICES

ACM SoCC 2026	Program Committee
IEEE TIFS 2023	Invited Reviewer

TEACHING

Computer Communications and Networks	Fall 2024
Computer Security	Fall 2021, Fall 2022

STUDENT SCHOLARSHIP

JUNE. 2026	IRTF Diversity Travel Grant, USD 2.5K
JUNE. 2023	PoPETS Stipend, USD 1.6K
MAR. 2022	SICSA Research Travel Funding, GBP 500
MAR. 2021	University of Edinburgh Doctoral College Scholarship, GBP 66K
OCT. 2017	First Class Graduate Freshmen Scholarship, CNY 20K

SELECTED AWARDS AND HONOURS

AUG. 2020	First Prize of Jiangsu Province 'Internet Plus' Innovation and Entrepreneurship Competition
DEC. 2017	Second Prize of Information Security and Countermeasures Contest

REFERENCES

Michio Honda	University of Edinburgh
Florentin Rochet	University of Namur
Pawel Szalachowski	Chainlink Labs
Zhe Liu	Zhejiang University