

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

College of Computer Science and Technology

Supervisor: Zhe Liu

Thesis: Towards Secure Data Sharing in Internet of Things Based on Blockchain

Outstanding dissertation

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

- Xinshu Ma**, Michio Honda: [Looma: A Low-Latency PQTLS Authentication Architecture for Cloud Applications](#). In Network and Distributed Systems Security Symposium, NDSS 2026.
- 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.
- 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.
- Chunpeng Ge, **Xinshu Ma**, Zhe Liu: A Semi-autonomous Distributed Blockchain-based Framework for UAVs Communication Systems. Journal of Systems Architecture. JSA 2020.

- ## POSTER & TALKS

- ## SERVICES

TEACHING

STUDENT SCHOLARSHIP

SELECTED AWARDS AND HONOURS

REFERENCES

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