

Yu Xia

ORCID: [0009-0009-3130-5046](https://orcid.org/0009-0009-3130-5046)
[Google scholar](#)

Email: xy19951128@gmail.com
[Personal website](#)

EDUCATION

The University of Edinburgh, UK
Ph.D. in Computer Science

Monash University, Australia
Master of Network and Security

Australian National University, Australia
Bachelor of Software Engineering (Honours)

CONFERENCE PUBLICATIONS

Delayed-Input Multi-Party Computation **ACNS 2025**
Michele Ciampi, Jure Sternad, Yu Xia

Broadcast-Optimal Four-Round MPC in the Plain Model **TCC 2023**
Michele Ciampi, Ivan Damgård, Divya Ravi, Luisa Siniscalchi, Yu Xia, Sophia Yakubov

Multi-Theorem Fiat-Shamir Transform from Correlation-Intractable Hash Functions **ACNS 2023**
Michele Ciampi, Yu Xia

WORKSHOP PUBLICATIONS

Robust Combiners for Non-Interactive Zero-Knowledge Proofs **ArcticCrypt 2025**
Michele Ciampi, Lorenzo Magliocco, Daniele Venturi, Yu Xia

Broadcast-Optimal Four-Round MPC in the Plain Model **TPMPC 2023**
Michele Ciampi, Ivan Damgård, Divya Ravi, Luisa Siniscalchi, Yu Xia, Sophia Yakubov

UNDER SUBMISSION

Broadcast-Optimal Secure Computation From Black-Box Oblivious Transfer **Eurocrypt 2025**
Michele Ciampi, Divya Ravi, Luisa Siniscalchi, Yu Xia

Robust Non-Interactive Zero-Knowledge Combiners **Eurocrypt 2025**
Michele Ciampi, Lorenzo Magliocco, Daniele Venturi, Yu Xia

OTHER RELEVANT EXPERIENCES

Teaching

Teaching Assistant for Introduction to Modern Cryptography **Jan 2024 - May 2024**
The University of Edinburgh, UK

Teaching Assistant for Introduction to Modern Cryptography **Jan 2023 - May 2023**
The University of Edinburgh, UK

Teaching Assistant for Introduction to Modern Cryptography **Jan 2022 - May 2022**
The University of Edinburgh, UK

Industry Work Experience

Others

External Conference Reviews: Eurocrypt 2022, Asiacrypt 2023, Crypto 2024, CSCML 2024, TCC 2024, FC 2025, Eurocrypt 2025

Journal Reviews: IEEE Security & Privacy, Theoretical Computer Science

TALKS

Broadcast-Optimal Four-Round MPC in the Plain Model **30 Nov 2023**
TCC 2023, Taipei

Multi-Theorem Fiat-Shamir Transform from Correlation-Intractable Hash Functions **22 Jun 2023**
ACNS 2023, Kyoto, Japan

Broadcast-Optimal Four-Round MPC in the Plain Model **09 Jun 2023**
TPMPC 2023, Aarhus, Denmark

Multiple talks in internal seminars at The University of Edinburgh

Awards

IACR / TCC stipend, for attending TCC 2023

TPMPC 2023 & ITC 2023 stipend, for attending ITC 2023 and TPMPC 2023

TPMPC 2022 student stipend, for attending TPMPC 2022

REFEREES

Available upon request.