Yu Xia

ORCID: 0009-0009-3130-5046 Email: xy19951128@gmail.com
Google scholar Personal website

EDUCATION

The University of Edinburgh, UK **Sep 2021 - Now**
Ph.D. in Computer Science

Monash University, Australia **Jul 2019 - Feb 2021**
Master of Network and Security

Australian National University, Australia **Jul 2016 – Jun 2018**
Bachelor of Software Engineering (Honours)

Beijing Institute of Technology, China **Sep 2014 – Jun 2016**
Bachelor of Software Engineering

CONFERENCE PUBLICATIONS

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

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 Yakoubov

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 Yakoubov

OTHER RELEVANT EXPERIENCES

Teaching

Teaching Assistant for Introduction to Modern Cryptography **Jan 2025 - May 2025**
The University of Edinburgh, UK

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

ArtChain Global **Aug 2018 - May 2019**

Part-time, Melbourne, Australia

DiGiCOR **May 2020 - Aug 2020**
Intern, Melbourne, Australia

Others
External Conference Reviews: *Eurocrypt 2022, Asiacrypt 2023, Crypto 2024, CSCML 2024, TCC 2024, FC 2025, Eurocrypt 2025, DLT 2025, Asiacrypt 2025, TCC 2025*
Journal Reviews: *IEEE Security & Privacy, Theoretical Computer Science, Frontiers in Big Data*

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.