Department of
Electrical Engineering
香港城市大學
City University of Hong Kong

Cryptographic Security Summit 2025

Date: 16 June 2025 (Mon)

Time: 12:00 - 15:00 HKT

Venue: P4302, 4/F

Yeung Kin Man Academic Building,

City University of Hong Kong

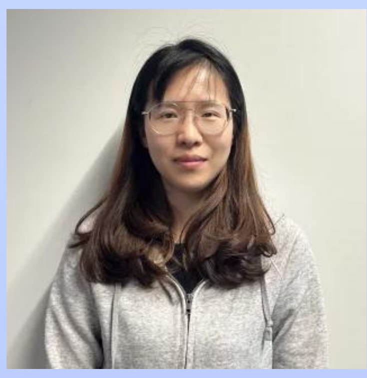
Zoom Link: (https://cityu.zoom.us/j/96742093029)

Prof. Ron Steinfeld
Monash University

Prof. Joseph Liu
Monash University

Prof. John Yuen
Monash University

Prof. Amin Sakzad
Monash University


Dr. Shujie Cui
Monash University

Dr. Muhammed Esgin
Monash University

Xinyu Zhang
Monash University

Dr. Shiyu Shen
City University of Hong Kong

Dr. Hao Yang
City University of Hong Kong

Organized by Prof. Chak Chung Ray Cheung
Associate Provost (DL), Office of the Provost and Deputy President
Professor, Department of Electrical Engineering
Professor, Affiliate, Department of Computer Science
Email: racheung@cityu.edu.hk

Department of
Electrical Engineering
香港城市大學
City University of Hong Kong

Prof. Ron Steinfeld
Associate Professor, Department of Software Systems & Cybersecurity, Monash University

Biography

Ron's research introduced structured lattice problems, in particular, the Polynomial-LWE problem (a common variant of Ring-LWE) and established their quantum security foundations and cryptographic applications. He also established the first quantum security foundations for NTRU-based encryption and signature algorithms. Variants of these structured lattice problems and algorithms are now routinely used in practical lattice-based cryptography, including the NIST Post Quantum Cryptography (PQC) standard algorithms Kyber, Dilithium, and Falcon. He was awarded the ASIACRYPT 2015 best paper award for Rényi divergence based analysis techniques bridging a gap between theory and practice in lattice-based cryptography, which form the basis for practical implementations of lattice-based cryptography. He has over 20 years of research experience in cryptography and information security. He has published more than 80 research papers in international refereed conferences and journals, more than 10 of which have each been cited over 100 times. He received more than AUD$4M in research and consulting funding,from organisations including Australian Research Council, Data61/CSIRO, and the cybersecurity industry. He has served as Technical Program committee member in numerous top-tier international research conferences worldwide (EUROCRYPT, CRYPTO, ASIACRYPT), has been an editorial board member of journal Designs Codes and Cryptography (2017-present), and consulted in cryptography design for the software industry.

Research interests

Ron's main research interests are in the design and analysis of cryptographic algorithms and protocols, and the formulation and proof of their security properties. He is especially interested in the area of quantum-safe cryptography and its applications.

Title: Post-Quantum Homomorphic Encryption and Verifiable Private Computation

Department of Electrical Engineering
香港城市大學
City University of Hong Kong

Prof. John Yuen
Associate Professor, Department of Software Systems & Cybersecurity, Monash University

Biography

Dr John Tsz Hon Yuen is an associate professor and the Director of Research in the Department of Software Systems & Cybersecurity at Monash University. His expertise is in the area of cryptography, security, privacy, blockchain and FinTech. He is a member of the Central Bank Digital Currency (CBDC) Expert Group of the Hong Kong Monetary Authority. Before joining Monash, Dr Yuen was an assistant professor in the Department of Computer Science at the University of Hong Kong. He had 4 years of industrial expereince at Huawei Singapore Research Centre and was a member of the Cryptography Expert Group in Huawei. He invented 10+ patents. He received his Ph.D. degree from the University of Wollongong in 2010.

Research interests

Dr Yuen published 80+ research papers including top tier conferences and journals in the area of cryptography and cybersecurity (CRYPTO, EUROCRYPT, CCS, SP, USENIX). Dr Yuen is interested to supervise students in the area of cryptograhpy, cybersecurity and privacy.

Title: Remote attestation/PSI/CBDC Wallet

Department of
Electrical Engineering
香港城市大學
City University of Hong Kong

Prof. Amin Sakzad
Associate Professor, Department of Software Systems & Cybersecurity, Monash University

Biography

Dr. Amin Sakzad has got a Ph.D. degree in Applied Mathematics from Amirkabir University of Technology (AUT), Tehran, Iran, 2011. He was a research visitor and a lecturer at Carleton University, Ottawa, Canada, in 2010. He was a research lecturer at AUT in 2011. Starting from Jan. 2012, he was a research fellow at Software Defined Telecommunications (SDT) Laboratory in the Department of Electrical and Computer Systems Engineering at Monash University under supervision of Prof. Emanuele Viterbo. From Feb. 2015 to April 2017, he was a research fellow at Clayton School of Information Technology at Monash University under supervision of Dr. Ron Steinfeld. As of May 2017, he is a Lecturer (Assistant Professor) at Faculty of Information Technology at Monash University. As of July 2021, Amin is a Senior Lecturer (Associate Professor) at FIT.

Research interests

Dr. Amin Sakzad is mainly interested in applications of lattices in cryptography and wireless communications. This includes applications of Algebraic Number Theory, Diophantine Approximation and Finite Fields in physical layer network coding and security, multiple-input multiple-output (MIMO) channels, lattice-based cryptography, and searchable encryption.

Title: Efficient and Secure Post-Quantum Cryptography Implementation

Department of
Electrical Engineering
香港城市大學
City University of Hong Kong

Dr. Muhammed Esgin
Lecturer, Department of Software Systems & Cybersecurity, Monash University

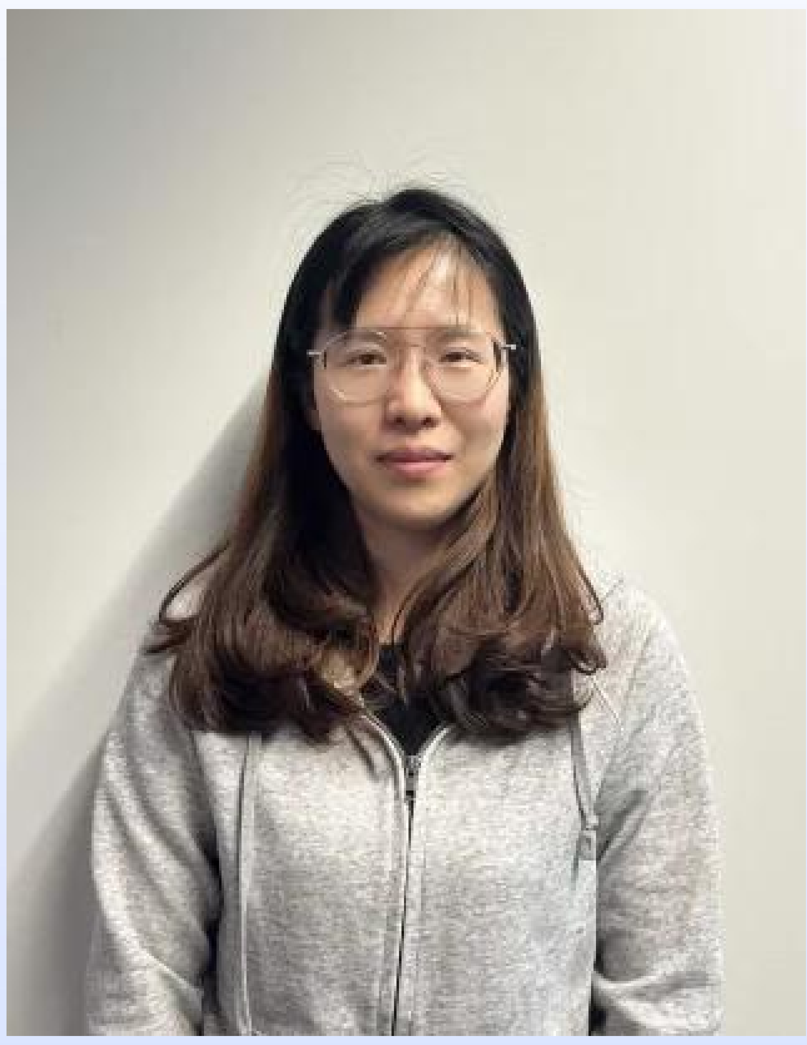
Biography

Muhammed is currently a lecturer at Faculty of Information Technology (FIT). Prior to this position, he was a post-doctoral researcher at Monash University and CSIRO's Data61 jointly. Before that, he did a research internship at IBM Research - Zurich, hosted by Vadim Lyubashevsky. He completed his PhD degree at Monash University in May 2020.

Research interests

Muhammed's research is focused around cybersecurity and lies at the intersection of Mathematics and Computer Science. In particular, he is interested in various aspects of cryptography such as quantum-resistant cryptography, privacy-enhancing technologies (e.g. zero-knowledge proofs) and blockchain protocols.

Title: Post-Quantum Privacy-Enhancing Protocol design



Dr. Shujie Cui
Lecturer, Department of Software Systems &
Cybersecurity, Monash University

Biography

I am a Lecturer in the Department of Software Systems and Cybersecurity at the Faculty of Information Technology. I obtained my PhD degree from the University of Auckland in 2019. Before joining Monash University, I was a Post-Doc researcher in the Large-Scale Data & Systems (LSDS) group in the Department of Computing at Imperial College London, UK.

Research interests

My main research interests include applied cryptography, information security in cloud computing and distributed systems, trusted execution environments, and privacy-preserving machine learning.

Title: Searchable Encryption and Trusted Execution
Environments / Side-Channel

Department of
Electrical Engineering
香港城市大學
City University of Hong Kong

Xinyu Zhang
Research Fellow, Department of Software Systems & Cybersecurity, Monash University

Biography

Xinyu Zhang is currently a PhD student at Monash University.

Research interests

My research area is symmetric key primitives based post-quantum cryptographic protocol design.

Title: Post-Quantum Cryptography from Legendre and Power Residue PRFs

Department of
Electrical Engineering
香港城市大學
City University of Hong Kong

Dr. Shiyu Shen
Postdoc, Department of Electrical Engineering, City University of Hong Kong

Biography

Dr. Shiyu SHEN(Sherie) received her Ph.D. degree in 2024 in the School of Computer Science, Fudan University.

Interests

- Fully Homomorphic Encryption
- Post-Quantum Cryptography
- High-Performance Computing
- Hardware Design

Title: Cryptographic Engineering in Post-Quantum World

Abstract:

As quantum computing rapidly approaches practical reality, ensuring cryptographic security in a post-quantum world has become critically important. This talk addresses key challenges and cutting-edge solutions in cryptographic engineering tailored for post-quantum cryptography. Specifically, we explore the advantages and nuances of architecture-aware arithmetic optimization techniques designed to maximize efficiency across diverse computational platforms. Further, we delve into RISC-V cryptographic extensions, highlighting their potential to enhance cryptographic operations by seamlessly integrating specialized instructions at the processor level. The discussion extends to sophisticated hardware designs, emphasizing their essential role in boosting security and performance, and also high-throughput GPU solutions that effectively handle demanding cryptographic workloads. Join us to discover how innovative approaches in cryptographic engineering are shaping secure, quantum-resistant infrastructures for the next generation.