Assoc Professor. Ron Steinfeld
Dept of Software Systems & Cybersecurity
Email: Ron.Steinfeld@monash.edu

Biography

BSc in Mathematics and Physics, Monash University, Australia, 1998.

BE (Hons., First Class) in Electrical and Computer Systems, Monash University, Australia, 2000

PhD, Computer Science, Monash University, Australia, 2003

Postdoc Research Fellow, Macquarie University, Australia, 2003-2006

Macquarie University Research Fellow, Macquarie University, Australia, 2007-2009

ARC Research Fellow, Macquarie University, Australia, 2009-2012

Lecturer / ARC Research Fellow, Monash University, Australia, 2012-2014

Senior Lecturer, Monash University, Australia, 2015-2019

Associate Professor, Monash University, Australia, since 2020

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.

Qualifications

Cryptography, Doctor of Philosophy, Monash University
Award Date: 9 Oct 2003

Electrical and Computer Systems, Bachelor of Engineering (Honours), Monash University
Award Date: 9 Oct 2000

Mathematics and Physics, Bachelor of Science, Monash University
Award Date: 9 Oct 1998

Activities

CSIRO - Commonwealth Scientific and Industrial Research Organisation (External organisation)
Muhammed Esgin (Member) & Ron Steinfeld (Member)

Deputy Course Director - Master of Networks and Security - Faculty of Information Technology, Monash University
Ron Steinfeld (Chair/ Co-Chair)
2016

IEEE Computer Society (CS) (United States) (External organisation)
Ron Steinfeld (Member)
2016

International Association for Cryptologic Research (External organisation)
Ron Steinfeld (Member)
2016