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

MONASH University

CityU Architecture Lab for Arithmetic and Security (CALAS) Seminar Series

Lattice-based Optimisation Techniques, Algorithms, and Evaluations

Dr. Amin Sakzad, Associate Professor
Director of Research in the Department of Software Systems and Cybersecurity, Monash University, Australia

Brief Abstract:

I will be talking about my various contributions to the secure and efficient implementation techniques and optimisations of lattice-based cryptographic primitives and protocols across multiple programming languages, CPUs, GPUs, and constrained IoT devices and Networks.

Biography:

Dr. Amin Sakzad is an Associate Professor and Director of Research in the Department of Software Systems and Cybersecurity at Monash University. With a career spanning cutting-edge post-quantum cryptography, lattice coding, and secure wireless communications, Amin has become a global leader in shaping the cryptographic foundations that will safeguard the digital world against quantum threats. His research on Euclidean lattices and post-quantum cryptography (PQC) has not only advanced theory but also translated into real-world adoption. Notably, his work on the FACCT sampler was adopted in Falcon, a NIST PQC standard. Beyond academia, his open-source cryptographic implementations have reached extraordinary global impact, with over 30 million downloads via the Legion of the Bouncy Castle platform. Amin has attracted over $8M in competitive industry and government funding, including a landmark USD $1M project with the U.S. Department of State to advance PQC adoption across 11 Indo-Pacific nations. As a mentor, Amin has guided PhD students who have gone on to careers at CSIRO, Amazon, ANU, and ONI, ensuring his impact extends across academia, government, and industry. Amin is also a decorated educator, having received multiple awards including the Monash Vice-Chancellor’s Teaching Excellence Award and recognition as a Senior Fellow of the Higher Education Academy (SFHEA).

16 March 2026 (Monday); 2pm – 4pm; Yeung G5-315; Zoom link (https://cityu.zoom.us/j/96742093029)