In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG

Department of Information Engineering

Seminar

On the Expanding Zoo of Lattice Assumptions

By

Dr. Russell W. F. Lai

Aalto University, Finland

Date : 10 December 2024 (Tuesday)

Time : 2:30pm – 3:30pm

Venue : Rm 801, Ho Sin Hang Engineering Building, CUHK

Abstract

Cryptography is built upon computational assumptions, i.e. that certain computational problems are hard for any efficient algorithms. It is therefore of fundamental importance to understand the actual hardness of these problems. We focus particularly on computational problems over Euclidean lattices which serve as foundations of diverse cryptographic schemes with conjectured post-quantum security.

In this talk, we will overview the current landscape of computational problems considered in lattice-based cryptography, including established ones such as the shortest independent vector problem (SIVP), short integer solution (SIS) and learning with errors (LWE), as well as recently proposed hinted and structured variants which enabled constructions of advanced primtitives. We will also highlight gaps in our understanding of these problems and identify potential avenues for advancements.

Biography

Russell W. F. Lai is an assistant professor at Aalto University, Finland co-leading the cryptography group. His recent research focuses on the construction of advanced cryptographic primitives, such as succinct arguments and functional commitments, based on structured and hinted lattice assumptions and the analysis of these assumptions. Previously, Russell obtained his PhD degree at Friedrich-Alexander University Erlangen Nuremberg, Germany and his MPhil, BSc, BEng degrees in the Chinese University of Hong Kong.

**** ALL ARE WELCOME ****

Host: Prof. Sherman S. M. Chow (Tel: 3943-8376, Email: sherman@ie.cuhk.edu.hk)

Enquiries: Information Engineering Dept., CUHK (Tel.: 3943-8385)