In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG

Department of Information Engineering

Seminar

Evasive LWE Assumptions: Definitions, Classes, and Counterexamples

By

Ms. Ivy K. Y. Woo

Aalto University, Finland

Date : 10 December 2024 (Tuesday)

Time : 3:30pm – 4:00pm

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

Abstract

The Learning with Errors (LWE) problem w.r.t. a matrix B asks to distinguish c = sB+e mod q from uniformly random, where s is a uniform secret and e some short error. In Eurocrypt'22, Wee proposed the evasive LWE assumption, which postulates that "For any matrix P, if LWE w.r.t. the joint matrix (B,P) is hard, then LWE w.r.t. B is also hard even when given short preimages U satisfying BU=P mod q". A handful of evasive LWE variants have emerged since then, which have been shown to imply various advanced cryptographic primitives, ranging from attribute-based encryption for unbounded-depth circuits, witness encryption, to obfuscation for null-circuits.

In this talk we overview the evasive LWE assumption, including why it appears useful to cryptographic proofs of advanced primitives and the different types of its variants. Based on the standard LWE assumption, we construct simple counterexamples against three private-coin evasive LWE variants appeared in prior works. Then, based on existing variants and our counterexamples, we propose and define three classes of plausible evasive LWE assumptions, suitably capturing existing variants for which we are not aware of non-obfuscation-based counterexamples. We also reason why security proofs in relevant works may be repaired under our assumption formulations.

Joint work with Chris Brzuska and Akin Ünal.

Biography

Ivy Woo is a doctoral researcher at the cryptography group of Aalto University, Finland. She is mainly interested in the construction of cryptographic objects over lattices, and has been recently working on advanced encryption schemes and threshold primitives, among others. Ivy completed her Master's and Bachelor's studies at Ulm University in Germany and the University of Hong Kong, respectively.

**** 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)