



THE CHINESE UNIVERSITY OF HONG KONG
Department of Information Engineering
Seminar

Post-quantum Cryptography, A New Era.

By

Prof. Jintai Ding
Tsinghua University and BIMSA, China

Date : 25 March 2024 (Monday)

Time : 11:00am – 12:00pm

Venue : Room 405, William M.W. Mong Engineering Building, CUHK

Abstract

Public key cryptosystems (PKC) are the security foundation of modern communication systems, in particular, the Internet. However Shor's algorithm shows that the existing PKC like Diffie-Hellmann key exchange, RSA and ECC can be broken by a quantum computer. To prepare for the coming age of quantum computing, we need to build new public key cryptosystems that could resist quantum computer attacks. In this lecture, we will give an introduction to post-quantum cryptography and its recent developments, in particular, the NIST standardization process and its impact. Then we will present the multivariate public key signature schemes, in particular, the UOV and TUOV signature schemes that were submitted to NIST for the new PQC signature round.

Biography

Jintai Ding is a professor at Tsinghua University and a Charles Phelps Taft Distinguished Professor Emeritus at the University of Cincinnati. He received his Ph.D. from Yale University in 1995. His research was in quantum affine algebras, where he was credited for the invention of the Ding-Iohara-Miki algebra. His current interest is in post-quantum cryptography. He and his colleagues developed Rainbow signature and LWE-based key exchange schemes.

Rainbow was a third round candidate for the NIST post-quantum standardization process. He and his colleagues completely broke a NIST second round post-quantum signature candidate LUOV and a third round candidate GeMSS (HFEv-), for which they won the best paper honorable mention award for Crypto 2021. He is one of the designers of Kyber KEM scheme which was selected as a key establishment standard by the US National Institute of Standards and Technology (NIST), to which his patent is currently licensed.

**** ALL ARE WELCOME ****