Joint CQSE & NCTS Seminar

2023
Sep. 22, Friday

TIME Sep. 22, 2023, 2:30~3:30pm
TITLE Migration to Post-Quantum Cryptography
SPEAKER Assistant prof. Jimmy Chen (Dept. of Mathematics, National Taiwan University)
PLACE Rm104, Chin-Pao Yang Lecture Hall, CCMS & New Physics Building, NTU
ONLINE https://nationaltaiwanuniversity-zbn.my.webex.com/

Abstract:

In a rapidly advancing digital landscape, the advent of quantum computing presents both unprecedented opportunities and significant threats to our current cryptographic systems. The key challenges posed by quantum computers to current cryptosystems will be examined. The goal of PQC, Post-Quantum Cryptography, is to provide cryptographic solutions that are secure not only against current classical computing techniques but also against the potential threat posed by large-scale quantum computers in the future. We will delve into the principles, mathematical foundations, and standardization efforts surrounding PQC. From the lattice problems and hash-based cryptography, we will elucidate the mathematical underpinnings that provide the robustness required to withstand quantum threats. As the cryptographic community unites to develop standardized PQC algorithms, we will discuss the criteria for evaluating candidate algorithms and the steps taken toward establishing a secure and future-proof cryptographic landscape.

Biography Brief:

Dr. Jimmy Chen received B.S. and M.S. degrees in Mathematics at NTU. After completing his doctorate at Purdue University, he returned to NTU as an adjunct faculty member. Also, he possesses an entrepreneurial spirit that led him to co-found several companies. Among these are InfoKeyVault, WiSECURE, and QSancus, each specializing in cutting-edge technology and security solutions.

Center for Quantum Science and Engineering (CQSE) 國立臺灣大學 量子科學與工程研究中心 National Taiwan University