Joint CQSE and CASTS Seminar

2020
November 6, Friday

TIME Nov. 6, 2020, 2:30~3:30pm
TITLE Post Quantum Cryptography (PQC) and the NIST PQC Standardization Competition
SPEAKER Prof. Bo-Yin Yang
Institue of Information Science, Academia Sinica
PLACE Rm104, Chin-Pao Yang Lecture Hall,
CCMS & New Physics Building, NTU

Abstract:

Post Quantum Cryptography (PQC) is the study of cryptography that is secure when the attackers have access to expensive quantum computing equipment. It is distinct from Quantum Cryptography in which the users have access to expensive quantum equipment. We tell the story of PQC and narrate the ongoing saga of the recent NIST PQC Standardization Competition.

Biography Brief:

Bo-Yin Yang received a Ph.D. in mathematics from MIT in 1991. From 1992 he taught at Tamkang University as an associate professor until 2006, when he transferred to Academia Sinica in Taipei. He works there today as a Research Fellow. His main research interests are cryptographic implementations and post-quantum cryptography, which he has studied since 2002. He has served the cryptographic community on many program committees and organized several conferences including CHES 2017. He is also the co-inventor of the Ed25519 digital signature scheme (2011, soon to be U.S. standard FIPS 186-5).

- N O T I C E -

▲Please swipe NTU card / ID card when entering CCMS-Phys. Building. ▲Please wearing a mask whenever social distancing (1.5m indoors) is impractical. ▲We provide alcohol sanitizer to keep your hands clean.

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