Joint CQSE and CASTS Seminar

2020
November 27, Friday

TIME Nov. 27, 2020, 2:30~3:30pm
TITLE Post-quantum cryptography: the theoretical foundation to real-world constructions
SPEAKER Dr. Po-Chun Kuo
Institute of Information Science, Academia Sinica
PLACE Rm104, Chin-Pao Yang Lecture Hall,
CCMS & New Physics Building, NTU

Abstract:

Post-quantum cryptography is the cryptographic algorithms that are secure against the threats from quantum computers. In this talk, I will explain the theoretical foundation of post-quantum cryptography: why it can (potentially) against quantum attack.

I will also introduce state-of-the-art post-quantum cryptography.

Biography Brief:

Po-Chun Kuo received his B.S., M.S, and Ph.D. in electrical engineering from National Taiwan University in 2010, 2011 and 2020, respectively.

He was the co-founder and the COO in Byzantine Lab during 2019/6-2020/6 and was the Chief Scientist in DEXON/COBINHOOD during 2017/5-2018/5.

He is currently the visiting scholar at Institute of Information Science, Academia Sinica. His research interests include consensus algorithm, post-quantum cryptography, and graph theory.

- 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.