CP-10-03

Quantum cryptography without one-way functions

Tomoyuki Morimae

Kyoto University

Abstract

One-way functions are the most fundamental primitives in classical cryptography. In this talk, I show that in quantum cryptography, one-way functions are not necessarily the most fundamental ones. We construct commitments and digital signature from pseudo-random quantum states generators. Pseudo-random quantum states generators are shown to exist even if BQP=QMA, which means that pseudo-random quantum states generators exist even if all post-quantum classical cryptographic primitives (inluding post-quantum one-way functions) are broken. Our result therefore means that several quantum cryptographic primitives can be constructed without one-way functions. This is a joint work with Takashi Yamakawa (NTT). [Morimae and Yamakawa, CRYPTO2022]