Contribution ID : **8** Type : **not specified**

Tomoyuki Morimae: Quantum commitments and signatures without one-way functions

Thursday, 15 June 2023 11:00 (60)

In the classical world, the existence of commitments is equivalent to the existence of one-way functions. In the quantum setting, on the other hand, commitments are not known to imply one-way functions, but all known constructions of quantum commitments use at least one-way functions. Are one-way functions really necessary for commitments in the quantum world? In this work, we show that non-interactive quantum commitments (for classical messages) with computational hiding and statistical binding exist if pseudorandom quantum states exist. Pseudorandom quantum states are sets of quantum states that are efficiently generated but their polynomially many copies are computationally indistinguishable from the same number of copies of Haar random states [Ji, Liu, and Song, CRYPTO 2018]. It is known that pseudorandom quantum states exist even if BQP=QMA (relative to a quantum oracle) [Kretschmer, TQC 2021], which means that pseudorandom quantum states can exist even if no quantum-secure classical cryptographic primitive exists. Our result therefore shows that quantum commitments can exist even if no quantum-secure classical cryptographic primitive exists. In particular, quantum commitments can exist even if no quantum-secure one-way function exists. In this work, we also consider digital signatures, which are other fundamental primitives in cryptography. We show that one-time secure digital signatures with quantum public keys exist if pseudorandom quantum states exist. In the classical setting, the existence of digital signatures is equivalent to the existence of one-way functions. Our result, on the other hand, shows that quantum signatures can exist even if no quantum-secure classical cryptographic primitive (including quantum-secure one-way functions) exists.