Contribution ID: **38** Type: **not specified**

Quantum cryptography with classical communication - Parallel remote state preparation for copy-protection, verification, and more

Tuesday, July 11, 2023 4:20 PM (20 minutes)

Alexandru Gheorghiu, Tony Metger and Alexander Poremba

Abstract: Quantum mechanical effects have enabled the construction of cryptographic primitives that are impossible classically. For example, quantum copy-protection allows for a program to be encoded in a quantum state in such a way that the program can be evaluated, but not copied. Many of these cryptographic primitives are two-party protocols, where one party, Bob, has full quantum computational capabilities, and the other party, Alice, is only required to send random BB84 states to Bob. In this work, we show how such protocols can generically be converted to ones where Alice is fully classical, assuming that Bob cannot efficiently solve the LWE problem. In particular, this means that all communication between (classical) Alice and (quantum) Bob is classical, yet they can still make use of cryptographic primitives that would be impossible if both parties were classical. We apply this conversion procedure to obtain quantum cryptographic protocols with classical communication for unclonable encryption, copy-protection, computing on encrypted data, and verifiable blind delegated computation. The key technical ingredient for our result is a protocol for classically-instructed parallel remote state preparation of BB84 states. This is a multi-round protocol between (classical) Alice and (quantum polynomial-time) Bob that allows Alice to certify that Bob must have prepared n uniformly random BB84 states (up to a change of basis on his space). Furthermore, Alice knows which specific BB84 states Bob has prepared, while Bob himself does not. Hence, the situation at the end of this protocol is (almost) equivalent to one where Alice sent n random BB84 states to Bob. This allows us to replace the step of preparing and sending BB84 states in existing protocols by our remote-state preparation protocol in a generic and modular way.

Presenter: GHEORGHIU, Alexandru

Session Classification: Track A-2