MAR10-2009-006922

Abstract for an Invited Paper
for the MAR10 Meeting of
the American Physical Society

Unconditional security from noisy quantum storage[1]

STEPHANIE WEHNER, Caltech

We consider the implementation of two-party cryptographic primitives based on the sole *physical* assumption that no large-scale reliable quantum storage is available to the cheating party. An important example of such a task is secure identification. Here, Alice wants to identify herself to Bob (possibly an ATM machine) without revealing her password. More generally, Alice and Bob wish to solve problems where Alice holds an input x (e.g. her password), and Bob holds an input y (e.g. the password an honest Alice should possess), and they want to obtain the value of some function $f(x, y)$ (e.g. the equality function). Security means that the legitimate users should not learn anything beyond this specification. That is, Alice should not learn anything about y and Bob should not learn anything about x, other than what they may be able to infer from the value of $f(x, y)$. We show that any such problem can be solved securely in the noisy-storage model by constructing protocols for bit commitment and oblivious transfer, where we prove security against the most general attack. Our protocols can be implemented with present-day hardware used for quantum key distribution. In particular, no quantum storage is required for the honest parties. Our work raises a large number of immediate theoretical as well as experimental questions related to many aspects of quantum information science, such as for example understanding the information carrying properties of quantum channels and memories, randomness extraction, min-entropy sampling, as well as constructing small handheld devices which are suitable for the task of secure identification.

Full version available at arXiv:0906.1030 (theoretical) and arXiv:0911.2302 (practically oriented).

[1]NSF grant PHY-0803371