Scopus

Documents

Nagy, M., Nagy, N.

Quantum Oblivious Transfer: a secure practical implementation
(2016) *Quantum Information Processing*, 15 (12), pp. 5037-5050. Cited 2 times.

Abstract
Together with bit commitment, Oblivious Transfer is a very useful cryptographic primitive with important applications, most notably in secure multiparty computations. It has been long known that secure Quantum Oblivious Transfer can be achieved from a secure implementation of Quantum Bit Commitment. Unfortunately, it is also well known that unconditionally secure Quantum Bit Commitment is impossible, so building a secure Oblivious Transfer protocol on top of Quantum Bit Commitment is ruled out. In this paper, we propose a relatively simple quantum protocol for Oblivious Transfer which does not require qubit storage, does not rely on bit commitment as a primitive and is easily implementable with current technology, if the two actors are honest. The protocol is proven to be secure against any individual measurements and entanglement-based attacks. Any cheating attempt trying to speculate collective measurements would be considerably difficult to put in practice, even in the near future. Furthermore, the number of qubits used in our scheme (embodied as photons in a physical realization of the protocol) acts as a security parameter, making it increasingly hard to cheat. © 2016, Springer Science+Business Media New York.

2-s2.0-84988358009
Document Type: Article
Publication Stage: Final
Source: Scopus