Scopus

Documents

Nagy, N., Nagy, M.

Unconditionally secure quantum bit commitment protocol based on incomplete information

(2014) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8890, pp. 134-143.

Abstract
This paper is reversing the current belief on Quantum Bit Commitment. Several papers have claimed and given a formal proof that quantum bit commitment is impossible. Nevertheless, the hypotheses of the formal mathematical model are too restrictive and do not exhaustively reflect the original definition of the problem. They share the same unnecessary restriction that the responsibility of hiding information and committing to a bit value is attributed to the same communicating partner. The protocol described here fully abides to the original description of the bit commitment problem.The two communicating partners share responsibilities, one partner is mostly responsible for hiding information and the other one for committing to the bit value. The security of the protocol derives from quantum properties such as the unclonability of unknown states, the indistinguishability of non-orthogonal states and also from randomly discarding and permuting qubits. The protocol is safe from classical attacks and quantum attacks using entanglement. The level of security can be made arbitrarily large by using more qubits. This result opens the door for a whole set of cryptographic applications using bit commitment as a building block: remote coin tossing, zero-knowledge proofs and secure two-party computation. © Springer International Publishing Switzerland 2014.

2-s2.0-84917708539
Document Type: Conference Paper
Publication Stage: Final
Source: Scopus