Scopus

Documents

Tatar, A.E., Nagy, M., Nagy, N.

The cost of breaking a quantum bit commitment protocol on equivalence classes
(2016) *ICETE 2016 - Proceedings of the 13th International Joint Conference on e-Business and Telecommunications*, 4, pp. 419-423.

Abstract
The importance of designing a secure quantum bit commitment (QBC) can be seen from its potential applications: remote coin tossing, zero-knowledge proofs, and secure two-party computation. Unconditionally secure QBC has been shown to be impossible (Mayers, 1996). This means that for any QBC protocol to date, there exist cheating that reveal more information than simple guessing. Nevertheless, the effort to break a QBC protocol may be impractical. The present paper explores the cheating strategy for a QBC designed within two equivalence classes and evaluates the complexity of a cheating attack and its practicality. Copyright © 2016 by SCITEPRESS - Science and Technology Publications, Lda. All rights reserved.

2-s2.0-85004007258
Document Type: Conference Paper
Publication Stage: Final
Source: Scopus