Scopus

Documents

Nagy, M., Nagy, N.

An information-theoretic perspective on the quantum bit commitment impossibility theorem
(2018) *Entropy*, 20 (3), art. no. 193, . Cited 2 times.

Abstract
This paper proposes a different approach to pinpoint the causes for which an unconditionally secure quantum bit commitment protocol cannot be realized, beyond the technical details on which the proof ofMayers' no-go theoremis constructed.We have adopted the tools of quantum entropy analysis to investigate the conditions under which the security properties of quantum bit commitment can be circumvented. Our study has revealed that cheating the binding property requires the quantum system acting as the safe to harbor the same amount of uncertainty with respect to both observers (Alice and Bob) as well as the use of entanglement. Our analysis also suggests that the ability to cheat one of the two fundamental properties of bit commitment by any of the two participants depends on how much information is leaked from one side of the system to the other and how much remains hidden from the other participant. © 2018 by the authors.

2-s2.0-85044189341
Document Type: Article
Publication Stage: Final
Source: Scopus
Access Type: Open Access