3rd International Conference on

Quantum Optics and Quantum Computing

September 10-11, 2018 | London, UK

An information-theoretic perspective on the quantum bit commitment impossibility theorem

Naya Nagy[1] and **Marius Nagy**[2]
[1]Imam Abdulrahman Bin Faisal University, KSA
[2]Prince Mohammad Bin Fahd University, KSA

This is a proposal of 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 of Mayers' no-go theorem is 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.

Biography

Naya Nagy has completed her PhD in 2010 from Queen's University. She is currently an Assistant Professor at Imam Abdulrahman Bin Faisal University, Saudi Arabia, in the Computer Science Department. She has done research in quantum cryptography and multidisciplinary fields connected to Computer Science.

nmnagy@iau.edu.sa

Notes:

Journal of Lasers, Optics & Photonics
ISSN: 2469-410X

Quantum Optics 2018
September 10-11, 2018

Volume 5

Page 47