Quantum Computing and Cryptography - 22: The Three-Stage Quantum Key Distribution Protocol

Length	Micromodule
Collection	NSA NCCP
Updated	March 14, 2019
Contributors	Abhishek Parakh
Academic Levels	Undergraduate, Graduate
Topics	Quantum Computing
Link	https://clark.center/details/aparakh/94dba9b8-c66d-48e4-b903-8029e5cc0f29

Description

This lesson introduces a multi-qubit resistant quantum key distribution protocol based on double lock cryptography. At the end of the lesson students will understand the working of the three-stage quantum key distribution protocol. Students will analyze the security of the QKD scheme and understand the concept of indistinguishability of non-orthogonal states.

The files are named nanomodules but it will take between 1 to 4 hours to complete all the exercises.

Email Dr. Abhishek Parakh at aparakh@unomaha.edu for solutions to the problems.

Note: To get started with Jupyter notebooks please follow the userguide available at: https://sites.google.com/unomaha.edu/userguideqcl/

Outcomes

- Apply the concepts of orthogonality of basis, measurement and indistinguishability of non-orthogonal states.
- Explain the concept of double lock cryptography.
- Restate the working of three-stage quantum key distribution protocol.

Links

External links that are associated with this learning object

- User guide