Quantum Computing and Cryptography - 20: The First Quantum Key Distribution Protocol

Length	Micromodule
Collection	NSA NCCP
Updated	March 14, 2019
Contributors	Abhishek Parakh
Academic Levels	Undergraduate, Graduate
Topics	Cryptography, Quantum Computing
Link	https://clark.center/details/aparakh/379fad93-7e27-416f-894c-0901cbb17483

Description

In this lesson, students will bring together all the knowledge they've gained so far to develop and understand BB84, the first quantum key distribution (QKD) protocol. Students will apply the principle of superposition and no-cloning theorem to construct BB84. They will apply quantum operations and measurement principles to quantum key distribution and understand the importance of non-orthogonal states in QKD protocols. Students will also analyze the QKD protocol for detecting eavesdropping.

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 principle of superposition and no-cloning theorem to construct a quantum key distribution protocol.
- Apply quantum operations and measurement principles to quantum key distribution.
- Analyze the QKD protocol for detecting eavesdropping.

- Recognize the importance of using non-orthogonal states in QKD.

Links

External links that are associated with this learning object

- User guide