QKD Proposal Presentation

By: Bommasani Sunny, Arshad Sadaf, Yu Eric, Gurumurthy Greesan, Li Haoran, Yang Chufan, Pham David

PI: Professor Bishop

TD: Jennifer Cheung

Motivation

It is interesting to understand more about how quantum computers pose security threats to classical security protocols, and how mitigation of such threats is possible. Such research will eventually provide better security for processes involving symmetric key cryptography, including sender validation, payment verification, communication security, and random number generation. We plan to do the following things:

- Understand QKD and its fallacies
- Collect possible ways to circumvent QKD's fallacies by researching companies that are implementing QKD
- Compare PQC and QKD

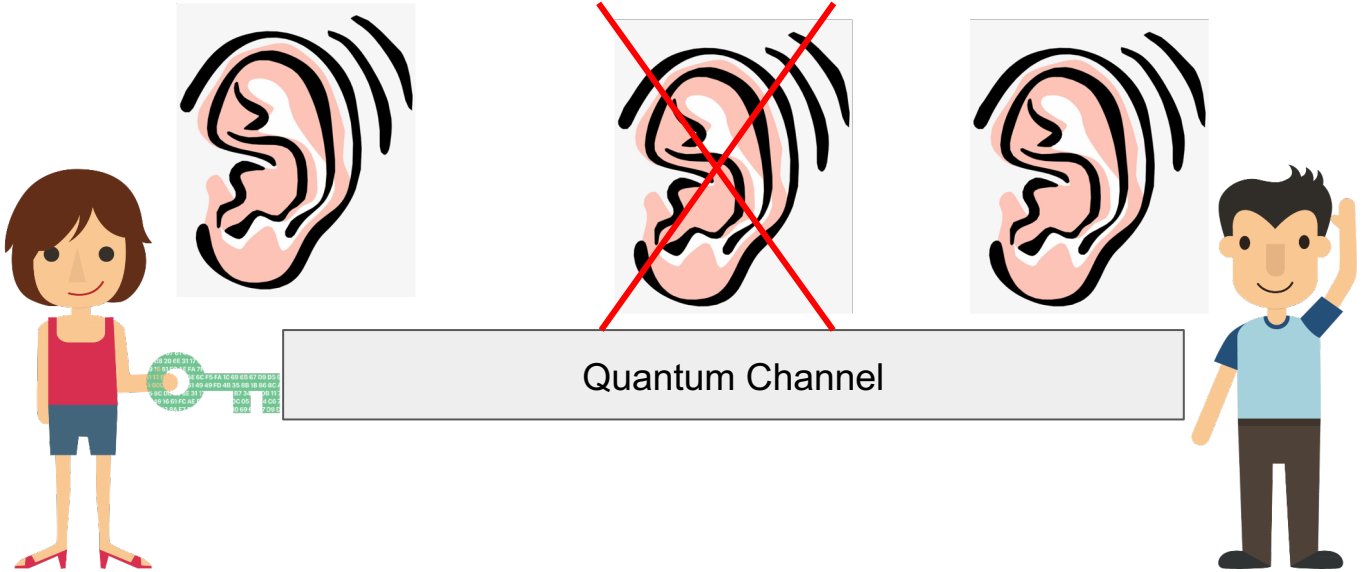
Lit Review done so far:

- Tech Report: Security considerations for quantum key distribution networks
  - High overview on QKD, issues, current implementations
- Black Paper of Quantum Cryptography: Real Implementation Problems
  - Focuses on more particular issues
- A Quantum Key Distribution Protocol for Rapid Denial of Service Detection
  - Focuses on the possibility of DOS attacks on QKD, and details a possible solution

Technical Report - Security considerations for quantum key distribution network

- Overview: paper introduces the security considerations for QKDN & gap analysis
  - Examples of QKD deployment around the world (China, Japan, South Korea and Switzerland)
- Quantum key distribution is a method for securely exchanging encryption keys, based on principles of quantum mechanics
- Combat Quantum Computing Attacks
  - Enhancement of current crypto system
  - Design of new public key system
  - Use of QKD to replace public key

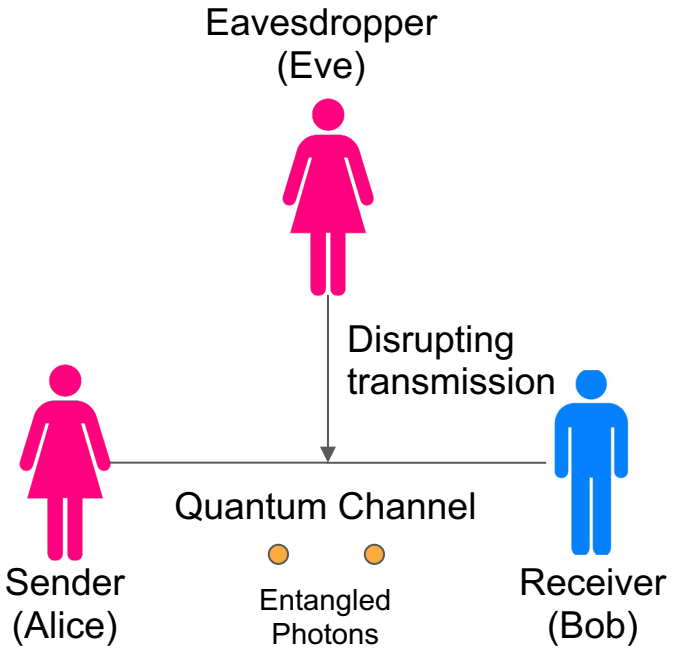
Black Paper of Quantum Cryptography: Real Implementation Problems

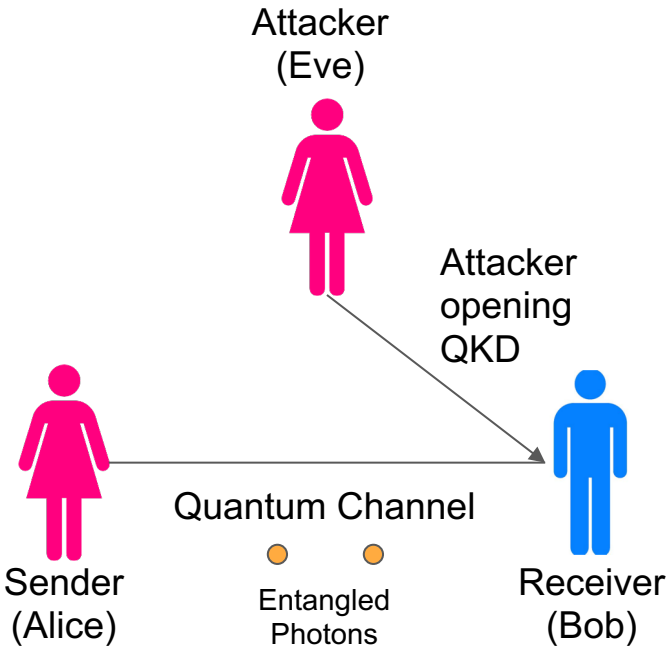


Black Paper of Quantum Cryptography: Real Implementation Problems

- Quantum Physics (if implemented properly) ensures:
  - That if the quantum courier (photon) is prepared properly, it will not be corrupted or leak info
- Issues exist when:
  - Quantum courier (photon) is improperly characterized
  - Eavesdropper affects preparation of qubits at sender side
  - Eavesdropper affects detection of qubits at receiver side
- Security proof assumptions
  - Can technical implementations stand up to these?

A quantum key distribution protocol for rapid denial of service detection





Data Management Plan

Deliverables:

- A list of our findings on research of QKD and PQC
- A list of solutions
- Documentation of our project for future reference

Where to access:

- Google Drive (Private)
- INSuRE repository (Public to INSuREHub members)

Final Culmination: Paper + Documentation

Issues

- Issue 1: understand QKD in a limited time period
- Solution 1: separate the learning work to each teammate so that everyone just needs to focus on a specific part.

- Issue 2: collect meaningful information from companies
- Solution 2: discuss what information we want to collect and then design a questionnaire to list out all our concerned points.

Milestones	Due date
Bids submission	Jan 18, 2022
Problem Assignment	Jan 20, 2022
Proposal	Jan 28, 2022
Literature Review	Feb 15, 2022
Literature Review Presentation	Feb 15, 2022
Discussion with Companies + Whitepaper Security Analysis	Feb 24, 2022
Dashboard	Feb 24, 2022
Progress Report	Mar 11, 2022
Midterm Progress report	March 17th, 2022
Midterm Progress presentation	March 18th, 2022
Final Presentation Submission	April 28th, 2022
Final Report & Presentation	April 29th, 2022

Lit Review Split-up

- Currently starting simple:
  - Understand QKD → focus on DOS prevention mechanisms
- 5 people working on QKD
  - What would a practical implementation look like?
  - Understanding BB84 and BB91 protocols
- 2 people working on PQC
  - NIST PQC Competition → how were implementations compared?

Possible practical implementations to evaluate

- Involves reading whitepapers and discussion with companies attempting to implement larger-scale QKD

Plans for this week

- BB84 Lit Review with basic qiskit implementation
  - Quantum Key Distribution (qiskit.org)
  - IRJET-V7I8438.pdf
- NIST PQC basic Lit Review
  - Post-Quantum Cryptography | CSRC (nist.gov)

The End

Any Questions?