Quantum Cryptography: Decoy State Protocol

QiLin Xue
University of Toronto

October 11, 2024

Why go quantum?

- Classical key distribution assumes certain problems are hard.
  - Shor's Algorithm: can factor large numbers very quickly. Uses:

    $$a^{\varphi(n)} \equiv 1 \pmod{n} \tag{1}$$

    and the Quantum Fourier Transform.
- In Quantum key distribution (QKD), the laws of physics provides *unconditional security*

What is a Quantum State

- A quantum state is a vector inside a Hilbert space, given by

$$\alpha |0\rangle + \beta |1\rangle \tag{2}$$

0 with $\alpha, \beta \in \mathbb{C}$ and $|0\rangle, |1\rangle$ form an orthonormal basis.

- Measurements are done with respect to a basis. They result is one of the basis vectors:

$$P(|0\rangle) = |\alpha|^2, \qquad P(|1\rangle) = |\beta|^2 \tag{3}$$

- Another orthonormal base is $|+\rangle, |-\rangle$ given by

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{4}$$

What is a Quantum State

- Basic vectors
  - $|0\rangle$ corresponds to $\updownarrow$ (0 in rectangular basis)
  - $|1\rangle$ corresponds to $\leftrightarrow$ (1 in rectangular basis)
  - $|+\rangle$ corresponds to $\neswarrow$ (0 in diagonal basis)
  - $|-\rangle$ corresponds to $\nwsearrow$ (1 in diagonal basis)
- Basis choices
  - Rectangular basis: 
  - Diagonal basis: 

Theorem

No Cloning Theorem: It is impossible to create an identical copy of a quantum state.

BB84 Protocol: Motivation

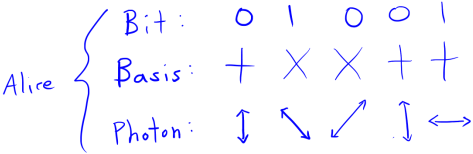
Goal: To share a *one-time pad*, that only Alice and Bob knows about. An n-bit key can encrypt and decrypt an n-bit message by applying XOR.

Example

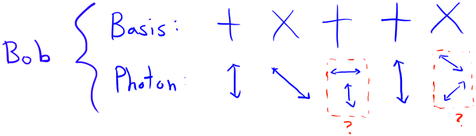
If the key is 01001 and the message is 11101 then the encrypted message is 10100. Applying XOR again gives the original message.

BB84 Protocol: Procedure

1. Alice sends a random key, (for example: 01001) with each bit encoded in a single photon selected from a random basis.



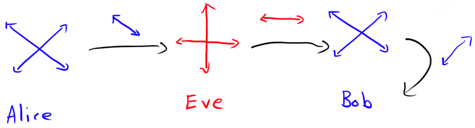
2. Bob measures each photon, also by randomly selected a basis each time.



3. After everything is done, they both communicate what basis they used over a *public channel* and only keep results where basis choice matches.

BB84 Protocol: Security

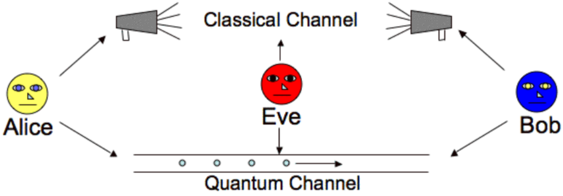
- To defend against eavesdroppers, Alice can reserve some bits for error-checking.



After all bits have been communicated, Alice tells Bob which bits are for error correcting and they compare inputs/outputs.
- If error rate above a certain percentage, terminate immediately.

BB84 Protocol: Assumptions

- True random number generators
  - Existing solutions using quantum RNG
- Authenticated public channels
- Single photon source
  - Difficult to achieve
  - Key vulnerability: **Photon Number Splitting** (PNS) attacks!



Practical Devices: Weak Coherent Lasers

- Each pulse consists of a certain number of photons
- If the average number of photons is μ, the probability of actually sending n photons follows a *Poisson distribution*,

$$P_\mu(n) = \frac{e^{-\mu}\mu^n}{n!} \tag{5}$$

  Even if $\mu = 1$, single photons only occur $e^{-1} \approx 37\%$ of the time!
- Only solution is to make μ smaller, but this causes optimal key rate to scale as $R \sim \eta^2$ where η is the transmittance.

Decoy State Protocol

- Idea: try to estimate the amount of interference by sending out decoy states
- Common method: Use 2 decoy states where the average photon numbers, ν_1, ν_2 are very low
- The yield Y_i is the probability of detecting exactly i photons. Assume Eve has *complete control* over this.
- The gain of the i-photon state is

$$Q_i = Y_i P_\mu(i) = Y_i \frac{e^{-\mu}\mu^n}{n!} \tag{6}$$

- The error rate (QBER) of the i-photon state is

$$e_i = \frac{\text{erroneous bits}}{\text{total bits}} \tag{7}$$

Alice also has control over this

Decoy State Protocol

- The overall gain is given by

$$Y_0 + 1 - e^{-\eta\mu} = \sum_{i=0}^{\infty} Y_i \frac{\mu^i}{i!} e^{-\mu} \tag{8}$$

- The overall QBER is given by

$$e_0 Y_0 + e_{\text{detector}}(1 - e^{-\eta\mu}) = \sum_{i=0}^{\infty} e_i Y_i \frac{\mu^i}{i!} e^{-\mu} \tag{9}$$

- The key rate is dependent on

$$R \sim Y_1(1 - H_2(e_1)) \tag{10}$$

  where H_2 is the binary entropy function.
- **Idea:** Bounding Y_1, e_1 given the equations allows us to lower bound R

Decoy State Protocol

Accounting for the decoy states, we have linear constraints

$$Y_0 + 1 - e^{-\eta\mu} = \sum_{i=0}^{\infty} Y_i \frac{\mu^i}{i!} e^{-\mu}$$

$$Y_0 + 1 - e^{-\eta\nu_k} = \sum_{i=0}^{\infty} Y_i \frac{{\nu_k}^i}{i!} e^{-\nu_k}$$

$$e_0 Y_0 + e_{\text{detector}}(1 - e^{-\eta\mu}) = \sum_{i=0}^{\infty} e_i Y_i \frac{\mu^i}{i!} e^{-\mu}$$

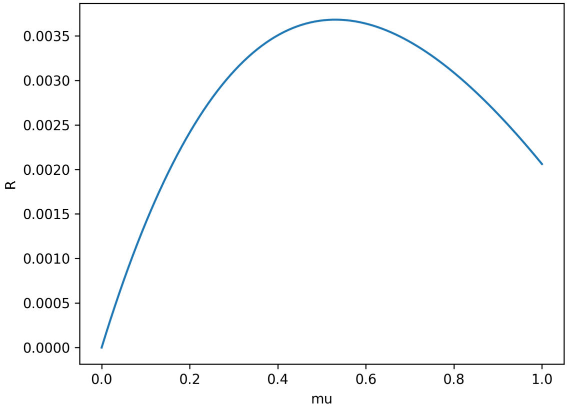
$$e_0 Y_0 + e_{\text{detector}}(1 - e^{-\eta\nu_k}) = \sum_{i=0}^{\infty} e_i Y_i \frac{\nu_k^i}{i!} e^{-\nu_k}$$

$$0 \leq e_i, Y_i \leq 1$$

to minimize Y_1 and maximize e_1.

Decoy State Protocol

Common to take $\nu_1 = 0$ and $\nu_2 = 0.05$. (vacuum + weak decoy).
Optimal intensity is around $\mu \sim 0.5$.



Decoy State Protocol

A secure key can be transmitted over 100 km.