Quantum Cryptography Protocols
PHY372H: Midterm Report

QiLin Xue

Contents

1 Decoy State Protocol

1.1 Photon Number Splitting Attacks

Realistically, single photon pulses are very difficult to achieve and almost impossible to guarantee. If multiple photons are sent, an evesdropper Eve could detect it and perform a photon number splitting (PNS) attack.

In a beam splitting attack, Eve employs a beam splitter to tap the optical channel. The core idea of the PNS attack lies in the eavesdropper (usually named Eve) tapping into the quantum channel and intercepting the photon pulses. Eve then leverages a photon-number-resolving (PNR) detector to measure the number of photons in the pulse rather than the quantum state[5]. If the pulse is composed of one photon, Eve sends it forward without disturbing it. However, in the event that the pulse contains multiple photons, Eve holds back one photon, allowing the rest to progress along the channel. Thus, while the key exchange participants' measure and generate their keys, Eve can also work on the withheld photon to decode the key, thereby undercutting the security of the quantum cryptography protocol by breaching the understated assumptions[8].

The PNS attack's strength lies in its stealthy nature, as it can be performed without noticeably influencing error rates, thus remaining undetectable if following the conventional protocol. It is difficult for Alice and Bob to determine if any losses in photons are due to an Evesdropper or due to channel loss.

1.2 Coherent States

Coherent state can be written in terms of the Fock basis [8],

$$|\alpha\rangle = e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle \tag{1.1}$$

where α is some complex number, and the probability of a pulse having n photons is given by,

$$P_\mu(n) = \frac{e^{-\mu}\mu^n}{n!}. \tag{1.2}$$

If $\mu = 1$, then the probability of emitting a single-photon source is only $P_1(1) = \frac{1}{e} \sim 37\%$. Thus, we typically will work with weak coherent states, where the average number of photons per pulse μ is smaller than one. But there will always be a nonzero probability more than one photon will be in each pulse, making it subject to PNS attacks.

An intuitive solution might be to reduce the pulse intensity as much as possible, ensuring that the probability of more than one photon per pulse is negligibly small to make it almost impossible for Eve, an eavesdropper, to extract any useful information.

However, this approach comes with a significant pitfall. The key generation rate R is proportionate to the square of the channel transmittance, i.e., $R = O(\eta^2)$. Now, η itself is a function of channel length and transmission loss parameter, and is given by

$$\eta \sim e^{-kL}, \tag{1.3}$$

where L is the channel length and k is the loss parameter. This implies that as the length of the channel increases or the transmission becomes less ideal, η decreases exponentially, which means the key generation rate drops off rapidly as well.

1.3 Simulation Project

The goal of the simulation project is to produce figure 2 in [4] and to numerically determine μ_{optimal}, similar to how it was derived mathematically via equation 12.

From the GLLP security analysis[8], the key rate satisfies

$$R \geq -Q_\mu H(E_\mu) + Q_1(1 - H(e_1)) \tag{1.4}$$

where

- Q_μ is the gain of signal states (probably of detection)
- E_μ is the overall QBER
- Q_i is the gain of the i-photon state
- e_i is the error rate of the i-photon state
- $H(x) = -x\log(x) - (1-x)\log(1-x)$ is the binary entropy function.

Note that the gain Q_μ and QBER E_μ are known quantities that can be experimentally determined. Therefore, only Y_1, e_1 need to be bounded. For realistic situations, the transmission distance is large $\eta \ll 1$ and working under this assumption we can assume that $E_i \approx e_i$[4]. The gain of the i-photon state can be written as

$$Q_i = Y_i P_\mu(i) = Y_i \frac{e^{-\mu}\mu^i}{i!} \tag{1.5}$$

where Y_i is the yield, defined as the probability of detecting exactly i photons. Therefore, the overall gain Q_μ is a sum of the individual gains

$$Q_\mu = \sum_{i=0}^{\infty} Y_i \frac{\mu^i}{i!} e^{-\mu}. \tag{1.6}$$

The overall QBER is therefore the sum of each individual gain, scaled by their respective error rate,

$$E_\mu = \sum_{i=0}^{\infty} e_i Y_i \frac{\mu^i}{i!} e^{-\mu}. \tag{1.7}$$

Note that Q_μ, E_μ can also experimentally be measured as[4]

$$Q_\mu = Y_0 + 1 - e^{-\eta\mu} \tag{1.8}$$
$$E_\mu = e_0 Y_0 + e_{\text{detector}}(1 - e^{-\eta\mu}) \tag{1.9}$$

where in the GYS experiment[2], they were able to measure

- $Y_0 \approx 1.7 \times 10^{-6}$ is the yield of the vacuum state.
- $\alpha = 0.21$ dB/km
- $e_0 = 0.5$ is the background error rate, and takes on this value based on the assumption the background is random.
- $e_{\text{detector}} = 3.3\%$ is a constant (independent of distance), which is the probability a photon hits the erroneous detector.

If two decoy states of intensities ν_1, ν_2 are used, they satisfy the exact same relationships, except with μ replaced with ν_1 or ν_2. This means that the key rate increases as Y_1 increases and decreases as e_1 increases.

The fundamental idea of using decoy states is that Y_i, e_i do not change,

$$Y_i(decoy) = Y_i(signal) \tag{1.10}$$
$$e_i(decoy) = e_i(signal). \tag{1.11}$$

That is, a decoy state should be indistinguishable from a signal state. Since Y_i, e_i are parameters that a hypothetical evesdropper Eve could control, we make the assumption that Eve has complete control over this. For a fixed μ, ν_1, ν_2, we assume she picks $\{Y_i, e_i\}$ to lower the rate as much as possible, so we need to lower bound Y_1 and upper bound e_1. Note that e_1 is small and for small values, H is a monotonically increasing function.

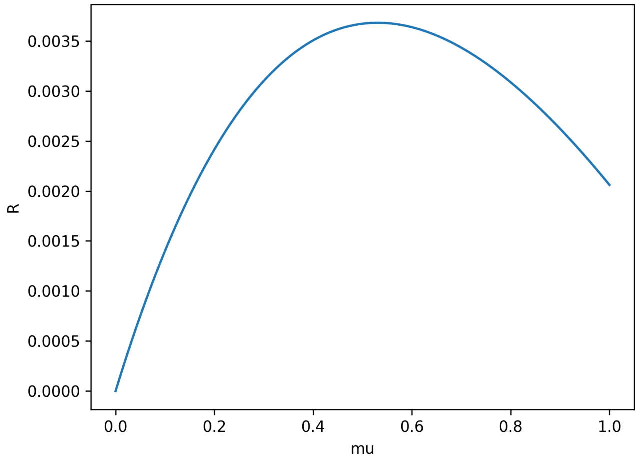
Our role then, is to pick the optimal combination of (μ, ν_1, ν_2) such that the worst-case scenario key-rate is as high as possible. This can be achieved using linear programming. Specifically, an iterative process was done. First, my variables were $Y_1, \ldots, Y_N$ (where $N = 10$) and my objective function was $-Y_i$ (because of lower bound), subject to the constraints

$$\begin{aligned}
Y_0 + 1 - e^{-\eta\mu} &= Y_0 e^{-\mu} + \sum_{i=1}^{N} Y_i \frac{\mu^i}{i!} e^{-\mu} \\
Y_0 + 1 - e^{-\eta\nu_1} &= Y_0 e^{-\nu_1} + \sum_{i=1}^{N} Y_i \frac{\nu_1^i}{i!} e^{-\nu_1} \\
Y_0 + 1 - e^{-\eta\nu_2} &= Y_0 e^{-\nu_2} + \sum_{i=1}^{N} Y_i \frac{\nu_2^i}{i!} e^{-\nu_2} \\
0 \le Y_i &\le 1.
\end{aligned}$$

Then the (optimized) versions of Y_i were now fixed and $\{e_i\}$ became the variables with the objective function of e_1. The constraints become

$$\begin{aligned}
e_0 Y_0 + e_{\text{detector}}(1 - e^{-\eta\mu}) &= e_0 Y_0 e^{-\mu} + \sum_{i=1}^{N} e_i Y_i \frac{\mu^i}{i!} e^{-\mu} \\
e_0 Y_0 + e_{\text{detector}}(1 - e^{-\eta\nu_1}) &= e_0 Y_0 e^{-\nu_1} + \sum_{i=1}^{N} e_i Y_i \frac{\nu_1^i}{i!} e^{-\nu_1} \\
e_0 Y_0 + e_{\text{detector}}(1 - e^{-\eta\nu_2}) &= e_0 Y_0 e^{-\nu_2} + \sum_{i=1}^{N} e_i Y_i \frac{\nu_2^i}{i!} e^{-\nu_2} \\
0 \le e_i &\le 1.
\end{aligned}$$

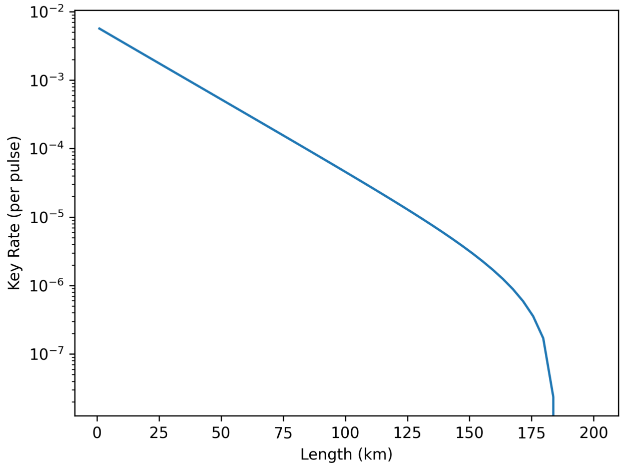
Solving this linear program for $\nu_1 = 0.05, \nu_2 = 0$ and varying μ gives the following graph (where $L = 10$ km is set as an example)



which takes on an optimal value of 0.54, which is slightly off from the value of $\mu_{\text{opt}} = 0.48$ computed in [4]. The efficiency as a function of distance can be written as

$$\eta = \eta_{\text{Bob}} 10^{-\alpha L/10} \tag{1.12}$$

where $\eta_{\text{Bob}} = 0.045$ is a fixed transmittance that describes losses that occur during detection, as measured in [2]. Therefore, if we plot out the key rate as a function of distance, we get



Note that after a certain point (around 180km) a secure key cannot be communicated anymore. In [4], this maximum distance was computed mathematically to be around 140km. The discrepancy could be caused by the iterative process not generating the most ideal set of $\{Y_i, e_i\}$ so the true minimum secure key rate could be lower than expected. Nonetheless, this preliminary idea that I have tried still captures the key features, and future work may involve nonlinear optimization techniques.

When linear programming is applied to solve similar decoy state problems, such as in [7], the constraints were put as an inequality, by putting a lower bound and upper bound on Q_μ, E_μ when the infinite sum gets cut off. As N increases, the constraints become tighter. However, I noticed that increasing N beyond 10 does not change the optimal μ, up to machine precision. This is a result of $\frac{1}{10!}$ being a very big number. This makes sense because in practice, there will be no photon pulses with more than 10 photons. Therefore, this simplified approach will not introduce any noticeable errors.

2 QKD Protocols

I have also looked at other QKD protocols as well as quantum repeaters, and have provided brief descriptions below.

2.1 EPR Pair BB-84

In the EPR Pair BB84 variant, entangled EPR pairs are measured by Alice and Bob in two potential bases. Any eavesdropping would change the state of the system and be detectable by Alice and Bob[8].

2.2 MDI-QKD

Measurement-device independent QKD offers a solution for potential detector attacks. Alice and Bob each prepare and send BB84 states to a third party, Charlie, who performs a Bell state measurement and broadcasts the result. This reveals only the correlation of Alice and Bob's qubits and no other information[8].

2.3 Twin Field QKD

Twin Field QKD uses single photon interference to enable measurement device independence and an improved key rate. This is caused by the fact that only a single photon needs to arrive at the center for it to be successful [8].

2.4 GMCS QKD

Gaussian-modulated coherent-states QKD encodes information in the amplitudes of weak coherent pulses allowing integration with existing telecom infrastructure. Alice and Bob compare their results publicly after enough measurements to extract a shared secret key from the continuous data[3].

3 Quantum Repeaters

Quantum repeaters use quantum teleportation to construct EPR pairs across several stations. There are key conditions for this to work - having established entanglement, having quantum memory to store qubits until entanglement is generated across all nodes, and being able to perform entanglement swapping operations[6].

There are a couple of noteworthy protocols for quantum repeaters:

3.1 DLCZ Protocol

The DLCZ protocol uses atomic ensembles as quantum memory sources but has the disadvantage of needing a long quantum memory since establishing EPR pairs and performing successful Bell State Measurements (BSMs) might require several attempts[6].

3.2 All Photonics Quantum Repeater

An All Photonics Quantum Repeater eliminates the need for quantum memory by using only photonics. Alice and Bob each send half of an EPR pair to an adjacent receiving node, which performs a BSM. Working in parallel increases the chances of success and eventually result in maximally entangled EPR pairs between Alice and Bob, and prevents the need for quantum memory.[1].

References

[1] Koji Azuma, Kiyoshi Tamaki, and Hoi-Kwong Lo. “All-photonic quantum repeaters”. In: *Nature Communications* 6.1 (Apr. 2015). DOI: 10.1038/ncomms7787. URL: https://doi.org/10.1038/ncomms7787.

[2] C. Gobby, Z. L. Yuan, and A. J. Shields. “Quantum key distribution over 122 km of standard telecom fiber”. In: *Applied Physics Letters* 84.19 (May 2004), pp. 3762–3764. DOI: 10.1063/1.1738173. URL: https://doi.org/10.1063/1.1738173.

[3] Hoi-Kwong Lo and Yi Zhao. *Quantum Cryptography*. 2008. arXiv: 0803.2507 [quant-ph].

[4] Xiongfeng Ma et al. “Practical decoy state for quantum key distribution”. In: *Physical Review A* 72.1 (July 2005). DOI: 10.1103/physreva.72.012326. URL: https://doi.org/10.1103/physreva.72.012326.

[5] Tobias Moroder, Marcos Curty, and Norbert Lütkenhaus. “Detector decoy quantum key distribution”. In: (2008). DOI: 10.1088/1367-2630/11/4/045008. eprint: arXiv:0811.0027.

[6] Nicolas Sangouard et al. “Quantum repeaters based on atomic ensembles and linear optics”. In: *Reviews of Modern Physics* 83.1 (Mar. 2011), pp. 33–80. DOI: 10.1103/revmodphys.83.33. URL: https://doi.org/10.1103/revmodphys.83.33.

[7] Wenyuan Wang and Hoi-Kwong Lo. “Simple method for asymmetric twin-field quantum key distribution”. In: *New Journal of Physics* 22.1 (Jan. 2020), p. 013020. DOI: 10.1088/1367-2630/ab623a. URL: https://doi.org/10.1088/1367-2630/ab623a.

[8] Feihu Xu et al. “Secure quantum key distribution with realistic devices”. In: *Reviews of Modern Physics* 92.2 (May 2020). DOI: 10.1103/revmodphys.92.025002. URL: https://doi.org/10.1103/revmodphys.92.025002.