Quantum Cryptography Protocols

QiLin Xue

Contents

1 Decoy State Protocol

1.1 Photon Beam 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. She can then measure the photon number in each pulse and keep the multi-photon pulses while discarding the single-photon ones. In theory, Eve can gather nontrivial information about what Alice and Bob are communicating, and they have no way to check.

1.2 Coherent States

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

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

where α is some complex number. A weak coherent state is when 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.

So why not just make the pulse weak enough such that the information Eve receives is insufficient? It turns out that the optimal intensity (quantified by μ) should be similar to the channel transmittance η where

$$\eta \sim e^{-kL} \tag{1.2}$$

where L is the length of the channel. They key rate depends quadratically $R = O(\eta^2)$ so this becomes very bad, fast.

1.3 Simulation Project

From GLLP security analysis, the key rate satisfies

$$R \geq -Q_\mu H(E_\mu) + Q_1(1 - H(e_1)) \tag{1.3}$$

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 $E_i \approx e_i$. The gain of the i-photon state can be written as

$$Q_i = Y_i \frac{e^{-\mu}\mu^n}{n!} \tag{1.4}$$

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

$$Q_\mu = \sum_{i=0}^{\infty} Y_i \frac{\mu^i}{i!} e^{-\mu}. \tag{1.5}$$

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

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

Note that Q_μ, E_μ can also experimentally be measured as

$$Q_\mu = Y_0 + 1 - e^{-\eta\mu} \tag{1.7}$$

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

- $Y_0 \approx 1.7 \times 10^{-6}$ is the yield of the vacuum state.
- $e_0 = 0.5$ is the background error rate, and takes on this value based on the assumption the background is random.
- e_{detector} 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 is related to the quantity

$$R \sim Y_1(1 - H(e_1)). \tag{1.9}$$

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

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

$$Y_0 + 1 - e^{-\eta\nu_1} = Y_0 e^{-\nu_1} + \sum_{i=1}^{N} Y_i \frac{\nu_1^i}{i!} e^{-\nu_1}$$

$$Y_0 + 1 - e^{-\eta\nu_2} = Y_0 e^{-\nu_2} + \sum_{i=1}^{N} Y_i \frac{\nu_2^i}{i!} e^{-\nu_2}$$

$$0 \le Y_i \le 1.$$

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

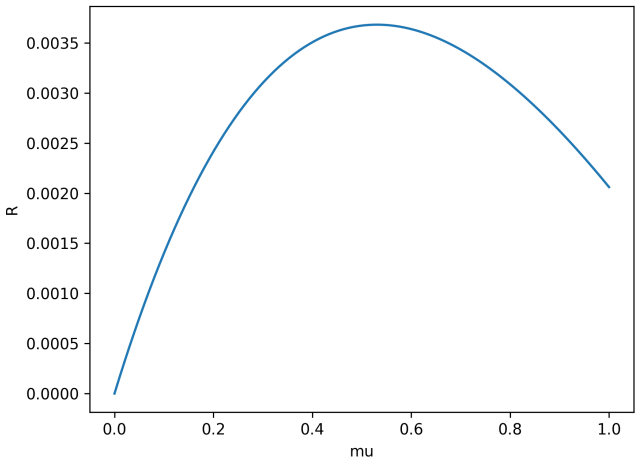
$$e_0 Y_0 + e_{\text{detector}}(1 - e^{-\eta\mu}) = e_0 Y_0 e^{-\mu} + \sum_{i=1}^{N} e_i Y_i \frac{\mu^i}{i!} e^{-\mu}$$

$$e_0 Y_0 + e_{\text{detector}}(1 - e^{-\eta\nu_1}) = e_0 Y_0 e^{-\nu_1} + \sum_{i=1}^{N} e_i Y_i \frac{\nu_1^i}{i!} e^{-\nu_1}$$

$$e_0 Y_0 + e_{\text{detector}}(1 - e^{-\eta\nu_2}) = e_0 Y_0 e^{-\nu_2} + \sum_{i=1}^{N} e_i Y_i \frac{\nu_2^i}{i!} e^{-\nu_2}$$

$$0 \leq e_i \leq 1.$$

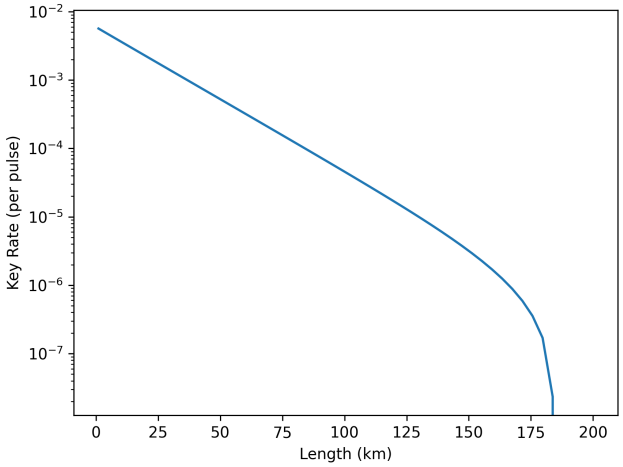
Solving this linear program for $\nu_1 = 0.05, \nu_2 = 0$ and varying μ gives the following graph



which takes on an optimal value of 0.54, which is slightly off from the value of $\mu_{\text{opt}} = 0.48$ computed in [3]. The efficiency as a function of distance can be written as

(1.12)

where $\eta_{\text{Bob}} = 0.045$ is a fixed transmittance that describes losses that occur during detection, and $\alpha = 0.21$ dB/km. 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 [3], 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.

2 QKD Protocols

2.1 EPR Pair BB-84

The BB84 Protocol is a prepare-and-measure protocol. However, the exact same idea can be used with entanglement. Suppose Alice and Bob are each holding a set of qubits, where each pair of qubits forms an EPR pair

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \tag{2.1}$$

This can be rewritten as

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|{+}{+}\rangle + |{-}{-}\rangle\right). \tag{2.2}$$

Therefore, if Alice and Bob choose to both measure in the $+/-$ basis or both choose to measure in the $0/1$ basis, their qubits will align. And similarly to the prepare-and-measure BB84 protocol, if they measure in different bases, then they cannot gain any information about the other person's qubit.

However, how does Alice and Bob trust that they are actually holding a pair from the state ψ? What Alice and Bob can do is take a subset of the EPR pairs and compare their results. When they have the same basis, they should expect to get the exact same result each time, with both results being equally likely. Only one state will give that intended behaviour, which is $|\psi\rangle$. If Eve spied on the qubits, she would need to make a measurement, which will cause the state to change, allowing Alice and Bob to detect the interference.[5]

2.2 MDI-QKD

Measurement-device independent QKD aims to solve the problem of detection attacks. This is important because we typically assume Eve has complete control over the channel and can send Alice and Bob anything, leading to potential attacks that are currently not modelled. To prevent the photon detectors from being attacked, the standard EPR pair protocol can be adapted to a time-reversed version.

Instead of having a centre station, which we'll call Charlie, distribute the EPR pairs to Alice and Bob, the reverse will happen. Each of Alice and Bob will prepare one of the four BB84 states, $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ and send them to Charlie, who performs a bell state measurement (BSM), using several beam splitters. The result is publicly transmitted.

Similar to the BB84 protocl in both the prepare-and-measure version and the EPR pair version, Alice and Bob can publicly announce their basis choices, and sift through the data in a similar way. Since the BSM result will only tell the parity between what Alice and Bob sent, no information is leaked to potential evesdroppers.

One disadvantage is that for a BSM to be performed, a qubit, typically in the form of a photon, must arrive from both Alice's source and Bob's source. Other modifications to MDI-QKD only requires one photon to arrive[5].

2.3 Twin Field QKD

Twin Field QKD is similar to MDI-QKD but is more sophisticated by utilizing single photon interference. This gives it several advantages and disadvantages[5].

Advantages

- Measurement device independent
- Key rate scales $\mathcal{O}(\sqrt{\eta})$ with transmittance η as opposed to linearly.

Disadvantages

- Single-photon interference requires subwavelength-order phase stability for optical channels. This becomes harder the longer the distance.
- For asymmetric losses, hard to get it to work over longer distances
- Single photon detectors are very expensive

2.4 GMCS QKD

Gaussian-modulated coherent-states QKD (GMCS QKD) is one of the continuous-variable quantum key distribution protocols, where the information is encoded in the quadrature amplitudes of a weak coherent pulse.

In GMCS QKD, Alice randomly generates two Gaussian random numbers to specify a complex number representing the amplitude and phase of her optical pulse. Alice then sends the pulse through a quantum channel to Bob. Bob makes measurements of the received pulse using homodyne or heterodyne detection methods to measure either one or both of the quadrature amplitudes, respectively. After performing sufficient measurements, Alice and Bob publicly compare their results and use error correction and privacy amplification methods to extract a shared secret key[2].

Advantages

- Every signal will lead to a bit in the key
- Doesn't require single photon detectors, cheaper
- Compatible with existing telecommunications equipment

Disadvantages

- Very sensitive to losses, bad for longer distances
- High speed implementations requires challenging pieces of technology
- The photon source (from Alice and Bob) need to be trusted. This is not actually too bad: just need to make sure they themselves are competent enough to not create a side channel to Eve.

3 Quantum Repeaters

Because the transmittance of a signal decreases exponentially with distance, it would be nice if there was a way to amplify the signal, such as how regular repeaters amplify electrical signals. The only issue is that the quantum no cloning theorem prohibits any duplication. After all, this is what allows QKD to be secure in the first place.

Quantum repeaters are able to circumvent this issue by constructing the EPR pair through quantum-teleportation like techniques across several stations between Alice and Bob. Suppose there are $2N$ nodes between Alice and Bob labelled $C_1, \ldots, C_{2N}$.

1. Entanglement (i.e. an EPR pair) is generated between C_1 and C_2. Similarly, EPR pairs are also generated between C_3 and C_4, as well as C_{2i-1}, C_{2i} for $i \geq 1$.
2. A BSM operation is performed between C_2 and C_3 which allows an entanglement swap. In other words, now C_1 and C_4 are entangled. The same is done with C_{2N-1} and C_{2N-2}.
3. The procedure is recursively performed inwards until the last entanglement swapping causes Alice (A) and Bob (B) to have generated an EPR pair[4].

3.1 Key Conditions

For most cases, these three conditions are necessary (maybe not sufficient)[4]:

- Need to establish entanglement and know when entanglement has been established.
- Needs quantum memory: needs to wait for entanglement to be established on neighbours as well
  - Memoryless repeaters are called quantum relays
- Need to perform entanglement swapping operations.

3.2 DLCZ Protocol

The DLCZ protocol uses atomic ensembles as sources for quantum memory. However, there are two main drawbacks. First, it requires a long quantum memory. This is because generating an EPr pair between neighbouring nodes may not always be successful as BSMs are not always successful. As a result, multiple attempts may be required, causing the other entangled qubits to need to be stored for longer, requiring a longer coherence time. Even after the EPR pairs are generated, the protocol is a heralding process as the entanglement swappings slowly move inwards. The outside swaps must happen before the inside swaps.

One way that addresses the first problem is by running it in parallel. At each node, instead of performing a single BSM, there could be several EPR pairs that are created, so problematically, it is almost guaranteed that at least one successful pair can be generated.

The second, and perhaps harder problem is that this protocl requires the switching between logical qubits (where we can manipulate them using quantum gates) and flying qubits (where we can send them from one physical location to another). This is DiVincenzo's extra criteria, which is extra hard. Therefore, it is very likely building a quantum repeater that relies on quantum memory may be even harder than building a quantum computer[1]!

3.3 All Photonics Quantum Repeater

One proposed method to eliminate the challenges described in the previous section is to use only photonics, eliminating the need for quantum memory. Similar to MDI-QKD, it is a time-reversed version of the traditional quantum repeater protocol. Between Alice and Bob lies several source nodes and several receiver nodes, placed between adjacent source nodes.

1. Alice and Bob each prepare m EPR pairs and sends one from each pair to the adjacent receiver node.
2. At the same time, all the other source nodes sends photons to their adjacent receiver nodes
3. At each receiver node, a BSM is performed. Since the idea of working in parallel from the previous section is still used here, it will almost always be a success.
4. Still at each receiver node, it performs other measurements and allow a maximally entangled EPR pair between Alice and Bob[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] Hoi-Kwong Lo and Yi Zhao. *Quantum Cryptography*. 2008. arXiv: 0803.2507 [quant-ph].
[3] 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.
[4] 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.
[5] 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.