Quantum Mechanics Report

Quantum Key Distribution Overview

Gabriel Wechta 250111

Wroclaw University of Science and Technology
Faculty of Algorithmic Informatics

December 29, 2022

Introduction

With the rise of the Internet, the importance of cryptography is growing every day. Each time we make an online the action we should be concerned with is secure communication. The security of conventional cryptography is typically based on computational assumptions. More precisely on some computational problem that is believed to be hard, for example, factorization problem or discrete logarithm problem. In contrast, Quantum Key Distribution (QKD), promises to achieve security not by computational hardness but by physical properties and laws of physics.

Contents

1. Standard Security Model

Normally when we analyze the security of a scheme, we argue about potential actions that an adversary can perform in order to gain some knowledge about ongoing communication. Typically by adding more and more power to the adversary, and simultaneously showing that the scheme is still secure we further develop the belief in the security of that particular scheme. Also, as mentioned before, security solely lies in the fact that some known problems do not have known optimal algorithms for finding solutions. Therefore finding a solution by the best-known algorithm is not much better than finding it by brute force. With such a setup, giving a problem in a space that is big enough basically guarantees that finding a solution is infeasible in a finite and reasonable time.

That's the overall argumentation, that we use today to postulate that the schemes that we use are secure and will be secure long enough.

But as mentioned in [2], there is always a possibility that some very persistent organization will use the overheard transcript, let's say today, wait many years for some great technological breakthrough or simply for hardware development and use it to break the security. For example, a potential target may be some government where secrets are kept for decades. It is also important to notice the latest discoveries of quantum code-breaking algorithms such as Shor's [4] efficient algorithm for factoring. Consequently, conventional cryptography is vulnerable to

- transcript aging,
- unanticipated advances in hardware and algorithms,
- quantum code-breaking.

Of course there exist countermeasures for conventional cryptography such as post-quantum cryptography, for example, Lattice-based primitives that are resistant to progress in quantum computing development.

2. Quantum Key Distribution

Suppose a sender, Alice, would like to send a secret message to a receiver, Bob, through an open (available to everyone, so also to eavesdroppers) communication channel. In order to keep the message content secret encryption is needed. If they share a common string of secret bits, called a secret key, Alice can use her secret key to transform a plaintext into a ciphertext using some symmetric encryption, which would be unintelligible to Eve. In contrast, Bob, with his key, can decrypt the ciphertext and recover the plaintext. In cryptography, the security of a crypto-system should rely solely on the secrecy of the key, not the obfuscation of the procedures (Kerckhoffs's principle). The question is: how to distribute a key securely without the need to make any pre-conversation between Alice and Bob? In conventional cryptography, it is done using asymmetric cryptography which utilizes some trapdoor problems. This motivates the development of quantum key distribution (QKD).

3. BB84

The best-known QKD protocol is the so-called BB84. So-called because authors – Bennett and Brassard never called it in their 1984 paper [1]. We will state the quantum properties that it utilizes and afterward shortly describe the key distribution protocol.

Essential Properties of Polarized Photons Although polarization is a continuous variable the uncertainty principle forbids measurements on any single photon for revealing more than one bit about its polarization. So let's say that a particle has polarization axis α and the filter gate is oriented at β, then individual photons are transmitted with probability $\cos^2(\alpha - \beta)$ and absorbed with complementary probability $\sin^2(\alpha - \beta)$. It's important to notice that based on that the photons behave deterministically only when two axes are parallel (certain transmission) or perpendicular (certain absorption), if none of this is true then the measurement is uncertain. Furthermore, during measurement, when photons pass through the β gate, they are left with polarization β, therefore it is infeasible to retrieve any more information from the system. More formally: let ψ be a vector of unit length in a linear space H over $\mathbb{C}$, let M_k represent the projection operator onto k-th subspace of measurement M, so that the identity operator on H can be represented as $I = M_1 + M_2 + \dots$. Then when a system is in a state ψ is subjected to measurement M, its behavior is in general probabilistic: outcome k occurs with a probability equal to $|M_k\psi|^2$. After the measurement, the system is left in a new state $M_k\psi/|M_k\psi|$, which is the normalized unit vector in the direction of the old state vector's projection into subspace M_k.The measurement thus has a deterministic outcome and leaves the state vector unmodified, only in the exceptional case that the initial state

vector happens to lie entirely in one of the orthogonal subspaces characterizing the measurement.

The Hilbert space considered in this study is 2 dimensional, therefore the state of a photon may be completely described as a linear combination of, for example, the two unit vectors $r_1 = (1, 0)$ and $r_2 = (0, 1)$ for rectilinear basis and two unit vectors $d_1 = (\sin(\frac{\pi}{4}), \cos(\frac{\pi}{4}))$ and $d_2 = (\sin(\frac{3}{4}\pi), \cos(\frac{3}{4}\pi))$ for diagonal basis. Two bases (e.g. rectilinear and diagonal) are said to be *conjugate* if each vector of one basis has equal-length projections onto all vectors of the other basis: this means that a system prepared in a specific state of one basis will behave entirely randomly, and lose all its stored information when subjected to a measurement corresponding to the other basis.

Key Distribution Protocol

- Alice sends Bob a sequence of photons prepared in different polarization states, which are chosen at random from two conjugate bases.
- For each photon, Bob selects randomly one of the two conjugate bases and performs a measurement.
- Bob records the outcome of his measurement and the chosen basis.
- Through an authenticated channel, Alice and Bob broadcast their measurement bases.
- They discard all polarization data sent and received in different bases and use the remaining data to generate a secret key.
- To test for tampering they compute the quantum bit error rate (QBER) of a randomly selected subset of data and verify that the QBER is below a certain threshold value.

After such key exchange, in the original paper, the authors proposed to use a one-time pad which is well known to have provable perfect security, but in practice, like in most of today's schemes, some kind of symmetric encryption is used, for example, AES block cipher.

4. QKD Practical Implementations

In the original theoretical proposal, Alice sends Bob single-photon states. However, as practical and efficient single-photon sources are yet to be realized, most implementations of the BB84 protocol are based on phase-randomized weak coherent state pulses (WCPs). These states can be easily prepared using standard semiconductor lasers and calibrated attenuators. The main drawback of these systems, however, arises from the fact that some signals may contain more than one photon prepared in the same quantum state.

Photon-Number-Splitting Attack In the above scenario, Adversary may dexterously perform a Photon-Number-Splitting (PNS) attack on the multi-photon pulses, thus gaining undetectable knowledge about parts of the shared key. Therefore only single-photon pulses may be considered secure holders of the key information. But the Adversary can intercept multi-photon pulses, split to single-photon and allow passage to Bob. It may look like this hardware disadvantage spoils the whole idea of QDK. Fortunately, there are countermeasures that do not require too much technological overhead.

Decoy-State Method In [3] Decoy-State method is introduced. The procedure is as follows. Instead of sending signals of equal intensity, Alice chooses first the intensity for each signal at random from a set of prescribed values. States sent in one particular intensity are called signal states, whereas the states sent with other intensities are called *decoy-states*. Once Bob has detected all the signals, Alice broadcasts the intensity used for each pulse. This way, even if Eve knows the total number of photons contained in a given pulse, her decision on whether or not to send that signal to Bob cannot depend on its intensity. That is, Eve's decision is based on what is known a priori. Consequently, the probability of having a detection event given that Alice sent a single-photon pulse is the same for the signal and decoy pulses. As a result, Alice and Bob can estimate the fraction of detected events that arise from single-photons more precisely.

References

[1] Charles Bennett and Gilles Brassard. "WITHDRAWN: Quantum cryptography: Public key distribution and coin tossing". In: vol. 560. Jan. 1984, pp. 175–179. DOI: 10.1016/j.tcs.2011.08.039.

[2] Hoi-Kwong Lo, Marcos Curty, and Kiyoshi Tamaki. "Secure quantum key distribution". In: *Nature Photonics* 8.8 (July 2014), pp. 595–604. DOI: 10.1038/nphoton.2014.149. URL: https://doi.org/10.1038/nphoton.2014.149.

[3] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. "Decoy State Quantum Key Distribution". In: *Physical Review Letters* 94.23 (June 2005). DOI: 10.1103/physrevlett.94.230504. URL: https://doi.org/10.1103/physrevlett.94.230504.

[4] P.W. Shor. "Algorithms for quantum computation: discrete logarithms and factoring". In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.