Quantum Key Distribution: A Deep Insight into the BB84 Protocol

Iñigo Perez Gamiz
Boston University

(Dated: December 12, 2023)

This paper provides a comprehensive analysis of the BB84 Quantum Key Distribution (QKD) protocol, a method for secure key generation based on Quantum Mechanics principles. The examination covers various aspects of the protocol, including its performance, imperfections, security vulnerabilities, and solutions to address these issues.

I. INTRODUCTION

The emergence of Quantum Computation has completely changed the computational landscape, specially in terms of cybersecurity. There are quantum algorithms that are supposed to efficiently solve the mathematical foundations of current encryption systems, meaning that they are a serious threat to them. This is the case of asymmetric encryption methods like the famous RSA, which are mainly threatened by Shor's quantum algorithm [1]. RSA is based on factorizing prime numbers, operation that Shor's algorithm can perform in polynomial instead of exponential time. In a similar fashion but to a lesser extent, Grover's algorithm [2] affects symmetric encryption methods (for instance, AES). Grover proved that the number of brute force attempts needed to break a symmetric encryption key can be reduced to the square root using a quantum computer.

In this context, cybersecurity professionals are now working to build safe encryption systems. They are mainly focusing on two technologies: Post-quantum cryptography and Quantum Key Distribution (QKD). Post-quantum cryptoghraphy aims to develop classical encryption algorithms for which quantum algorithms do not show a relevant speedup. On the other hand, Quantum Key Distribution protocols are intended for the secure generation of private keys exploiting the laws of Quantum Mechanics.

At this point, this paper aims to study one particular Quantum Key Distribution (QKD) protocol in depth, the BB84. The analysis will cover its mechanism of action, security, and imperfections derived from quantum noise and attacks.

II. SOME BACKGROUND: POLARIZED PHOTONS

Photons are particles that can be polarized with an apparatus specifically intended for that. Their polarization axis is determined by the orientation of the polarizing apparatus. The same way they can be polarized, they can also be detected using a filter with a certain orientation. The photons behave deterministically (probability 1) only when their axes are parallel (transmission) or perpendicular (absorbtion) to the axis of the filter. For the rest of the cases (the axes are neither parallel nor perpendicular), there is a probability $\cos^2(\alpha)$ that the photon is transmitted, being α the angle between the axes of the photon and filter, and a probability $\sin^2(\alpha)$ that the photon is absorbed. This means that the photons behave probabilistically [3].

III. QUANTUM KEY DISTRIBUTION PROTOCOLS

Quantum Key Distribution (QKD) is a communication protocol that allows the safe generation of a shared private key between a sender (Alice) and a receiver (Bob). It gains strength from its quantum nature, relying on two main principles: measurement disturbance and the no-cloning theorem. If a third party (Eve) tries to intercept the key while it is being generated, by the no-cloning theorem, she will not be able to copy the state of the key. The only way she has to get information about the key is measuring and, consequently, disturbing it. As a result, Alice and Bob will be able to detect the attack. This is a common characteristic for all Quantum Key Distribution protocols. However, they differ in the way the key is generated. Figure 1 shows an scheme of QKD, where Alice and Bob use a quantum channel and a public classical channel to communicate.

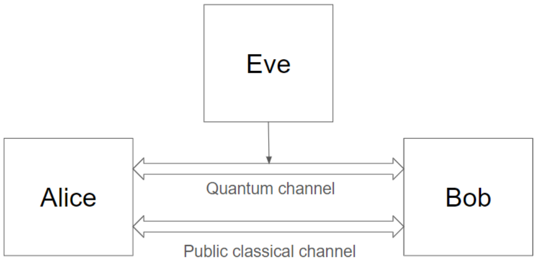

FIG. 1. QKD scheme.

IV. BB84

A. Description

The BB84 protocol was introduced by Charles H. Bennett and Gilles Brassard in 1984 [3]. It was the first QKD protocol developed and it inspired many of the protocols that were later proposed. It belongs to the so-called prepare-and-measure protocols.

In this protocol, Alice and Bob use a quantum channel and a classical public channel to communicate. Initially, Alice generates two random strings of n-bits (a and b). The first string contains the bits a_i for the key generation. These bits are encoded on the Z-basis or X-basis depending on the value of the corresponding bit b_i from the second string (0 for Z-basis and 1 for X-basis). The four possible states $|\phi_{a_i,b_i}\rangle$ for each encoded bit are the following:

$$|\phi_{00}\rangle = |0\rangle \qquad |\phi_{10}\rangle = |1\rangle$$

$$|\phi_{01}\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |+\rangle \qquad |\phi_{11}\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle$$

where, for instance, $|\phi_{01}\rangle$ represents the state of a bit 0 encoded in the X-basis. Physically, these states can be implemented using polarized photons. Considering that the state $|\phi_{00}\rangle$ corresponds to 0^{o} of polarization, the states $|\phi_{10}\rangle$, $|\phi_{01}\rangle$ and $|\phi_{11}\rangle$ correspond to 90^{o}, 45^{o} and -45^{o} polarizations respectively.

Computationally, the encoding process is obtained applying a controlled-Hadamard gate to each key generation qubit $|a_i\rangle$ (Figure 2), being this qubit the target and the qubit that determines the encoding basis $|b_i\rangle$ the control.

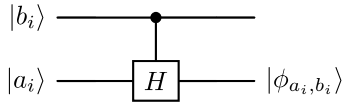

FIG. 2. Circuit to encode qubits.

Once all the bits a_i are encoded, that is, all the states $|\phi_{a_i,b_i}\rangle$ are prepared, they are sent to Bob through the quantum channel. Now Bob generates a random string c of n-bits to decode the received key string. Each bit c_i indicates in which basis is he going to measure the corresponding received state $|\phi_{a_i,b_i}\rangle$ (the same as for Alice, 0 for Z-basis and 1 for X-basis). If the chosen basis is the same as Alice's, then he will get the right bit. Otherwise, the result of the measure will be random. Physically, this consists on trying to detect the polarized photons placing a filter either horizontal/vertical (Z-basis) or diagonal (X-basis). The circuit that Bob will need to decode each bit is the inverse to the one that Alice used, that is, a controlled-Hadamard gate where $|c_i\rangle$ is the control qubit and $|\phi_{a_i,b_i}\rangle$ is the target (Figure 3). The measured bit will be $\overline{a_i}$.

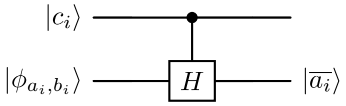

FIG. 3. Circuit to decode qubits.

After decoding the bits, Alice and Bob share through the classical channel which basis did they use for each bit of the key, and discard the bits for which they did not agree. This is known as key sifting. The length of the remaining string of key bits is expected to be half the initial one. Considering an ideal noise-free and eavesdropping-free quantum channel, this sequence of bits would constitute the intended mutually shared secret key.

Table I shows an example of a key generation between Alice and Bob.

a_i	0	1	0	1	1	0	1
b_i	0 (Z)	0 (Z)	1(X)	1(X)	1(X)	0(Z)	0(Z)
$\lvert\phi_{a_i,b_i}\rangle$	$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert +\rangle$	$\lvert -\rangle$	$\lvert -\rangle$	$\lvert 0\rangle$	$\lvert 1\rangle$
c_i	0 (Z)	1 (X)	0 (Z)	1 (X)	0 (Z)	0 (Z)	0 (Z)
Sifted key	0	–	–	1	–	0	1

TABLE I. Example of key generation in BB84.

B. Quantum noise

The above explained protocol assumes the absence of noise in transmissions and problems related to eavesdropping. However, in real life this situation is unfeasible. There is always going to be, at least, some noise. This noise can be reflected in, for instance, bit-flips or phase flips. To have an intuition of how they affect, consider the following simple model for a phase-flip derived from noise: Alice sends the state of one qubit, generally represented as $a|0\rangle + b|1\rangle$, and Bob receives $a|0\rangle \pm b|1\rangle$ with equal probability. In this model, when Alice sends the state $|\psi_{00}\rangle$, Bob receives it without error. On the contrary, if Alice sends, for instance, $|\psi_{01}\rangle$, then Bob will receive either $|\psi_{01}\rangle$ or $|\psi_{11}\rangle$, both with probability 1/2. The results in his measures will be modified, which means that some errors are introduced.

Another common form of quantum noise is the depolarizing channel. Given the state of a qubit $|\phi_{a_i,b_i}\rangle$, that has density matrix ρ_{a_i,b_i} (consider ρ for simplicity), the effect of depolarization can be described as [4]

$$\varepsilon(\rho) = p\frac{I}{2} + (1-p)\rho \tag{1}$$

where p is the probability that the state gets depolarized and $(1-p)$ is the probability that it remains unaltered. Using the property

$$\frac{I}{2} = \frac{1}{4}\left(\rho + X\rho X + Y\rho Y + Z\rho Z\right) \tag{2}$$

where X, Y, Z are the Pauli matrices, expression (1) becomes

$$\varepsilon(\rho) = \left(1 - \frac{3p}{4}\right)\rho + \frac{p}{4}\left(X\rho X + Y\rho Y + Z\rho Z\right) \tag{3}$$

Now taking into account that the density matrices for the four possible states of a qubit are

$$\rho_{00} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad \rho_{10} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \tag{4}$$

$$\rho_{01} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \qquad \rho_{11} = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \tag{5}$$

with the effect of the depolarizing channel they turn into $(\rho' = \varepsilon(\rho))$

$$\rho'_{00} = \frac{1}{2}\begin{pmatrix} 1+q & 0 \\ 0 & 1-q \end{pmatrix} \qquad \rho'_{10} = \frac{1}{2}\begin{pmatrix} 1-q & 0 \\ 0 & 1+q \end{pmatrix} \tag{6}$$

$$\rho'_{01} = \frac{1}{2}\begin{pmatrix} 1 & q \\ q & 1 \end{pmatrix} \qquad \rho'_{11} = \frac{1}{2}\begin{pmatrix} 1 & -q \\ -q & 1 \end{pmatrix} \tag{7}$$

being $q = 1 - p$. Regarding this expression, when the state is not depolarized $(p = 0)$, then $q = 1$ and the density matrices remain unaltered. Otherwise, if $p \neq 0$, they change gradually until they reach the totally mixed state $\rho'_{a_i,b_i} = \frac{I}{2}$ when $p = 1$.

Let us calculate now the quantum bit error rate caused by the depolarizing channel. This rate reflects the ratio between the number of incorrect bits in the sifted key and the total number of sifted keys. Consider the case of the bit 0 encoded in the Z-basis. In this case,

$$\rho_{00} = |0\rangle\langle 0|, \qquad \rho'_{00} = \frac{1+q}{2}|0\rangle\langle 0| + \frac{1-q}{2}|1\rangle\langle 1| \tag{8}$$

This means that probability that Bob measures the wrong bit as a result of depolarization is $p_w = \frac{1-q}{2}$. For the case of the bit 0 encoded in X-basis,

$$\rho_{01} = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|0\rangle\langle 1| + \frac{1}{2}|1\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = |+\rangle\langle +| \tag{9}$$

$$\begin{aligned} \rho'_{01} =& \frac{1}{2}|0\rangle\langle 0| + \frac{q}{2}|0\rangle\langle 1| + \frac{q}{2}|1\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| \\ =& \frac{1+q}{2}|+\rangle\langle +| + \frac{1-q}{2}|-\rangle\langle -| \end{aligned} \tag{10}$$

That is, we get the same probability of getting a wrong result. Applying the same procedure to the remaining two cases, we get that in general, the probability of measuring a wrong bit is $p_w = \frac{1-q}{2}$. With this result, we can calculate the quantum bit error rate [5]:

$$QBER = \frac{p_w}{p_c + p_w} = \frac{p}{2} \tag{11}$$

This is only the QBER caused by the depolarizing channel. To obtain the total rate, other sources of noise need to be considered.

C. Information reconciliation

Information reconciliation is known as the process in which Alice and Bob try to estimate a bit error rate to fix their sifted keys. As it has been explained, quantum channels generate noise that disturbs the state of the qubits, so they introduce error rates like the previously derived. At the same time, there might also be some attempts of eavesdropping that could contribute to increase the total error rate even more.

The process of information reconciliation works as follows. After forming the sifted key, Bob randomly chooses certain bits of his key and reveals them to Alice through the public channel. From this sample, they infer the bit error rate, and later discard the used bits. Assuming that this error rate is the same for the rest of the bits, they correct them. There are different approaches to correct the bits. One of the most common ones is the cascade protocol [6], that operates in several iterations. In each round, both Alice's and Bob's sifted keys are divided into blocks and the corresponding blocks' parity is compared. If for two blocks the parity is not the same, then a binary search is carried on to fix the errors. After comparing all the blocks, Alice and Bob randomly reorder the bits (both in the same way) and continue iterating. The process is repeated a number of times big enough so that Alice and Bob have the same key with high probability.

D. Privacy amplification

Privacy amplification is a technique that aims to mitigate the amount of information that an eavesdropper can have about the key. This information could have been obtained during the generation of the key or the information reconciliation process. The method consists on reducing the length of the key to even a shorter string of bits about which the eavesdropper has practically no information. This is normally done using hash functions [7]. The function receives the key and outputs a shorter one. The length of the final key is established by Alice and Bob and is estimated based on the bit error rate obtained during the information reconciliation process.

E. Security analysis

Let us analyze now the security of the protocol. Thanks to the principles of Quantum Mechanics, attempts of eavesdropping are detectable. When Alice and Bob estimate the bit error rate during the information reconciliation, obtaining a high rate suggests that somebody tried to intercept the key. This would lead them to interrupt the key generation process and restart again from scratch.

There are different strategies for Eve to try to get information about the key. The most trivial one is the intercept-resend attack: Eve intercepts every qubit, measures them in a certain basis to get information, and later sends the collapsed qubits to Bob. An intelligent election for the basis is the Breidbart basis [8]:

$$\begin{aligned} |e_0\rangle &= \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle \\ |e_1\rangle &= -\sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle \end{aligned} \tag{12}$$

The angle formed by $|e_0\rangle$ with the states $|0\rangle$ and $|+\rangle$ used to encode the bit 0 is $\frac{\pi}{8}$, so the probability to measure it is $\cos^2\left(\frac{\pi}{8}\right)$. Similarly, the angle between $|e_1\rangle$ and $|1\rangle$ is $\frac{\pi}{8}$, and the angle between $|e_1\rangle$ and $|-\rangle$ is $\frac{7\pi}{8}$, so the probability to measure bit 1 is $\cos^2\left(\frac{\pi}{8}\right) = \cos^2\left(\frac{7\pi}{8}\right)$. As a result, using the Breidbart basis, Eve will always be able to get information about a qubit with $\cos^2\left(\frac{\pi}{8}\right) \approx 0.85$ probability of success.

Let us calculate now the bit error rate that Alice and Bob will get after Eve intercepts and measures the key using the Breidbart basis. Consider an ideal absence of noise. For each of the four possible states of the qubit, all of them with equal probability $\frac{1}{4}$, we calculate the probability that the key bit x sent by Alice to Bob, is different from the key bit y sent by Eve to Bob. We start with, for instance, the probability that Bob gets bit 0 when Alice sent qubit $|1\rangle$.

$$\begin{aligned} &P(x \neq y) = P(\text{B gets 0}|\text{A sent }|1\rangle) \\ &= P(\text{E sends }|e_1\rangle|\text{A sent }|1\rangle) \cdot P(\text{B gets 0}|\text{B got }|e_1\rangle) \\ &+ P(\text{E sends }|e_0\rangle|\text{A sent }|1\rangle) \cdot P(\text{B gets 0}|\text{B got }|e_0\rangle) \\ &\qquad = |\langle e_1|1\rangle|^2|\langle 0|e_1\rangle|^2 + |\langle e_0|1\rangle|^2|\langle 0|e_0\rangle|^2 \\ &\qquad = \cos^2\frac{\pi}{8}\sin^2\frac{\pi}{8} + \sin^2\frac{\pi}{8}\cos^2\frac{\pi}{8} = \frac{1}{4} \end{aligned} \tag{13}$$

Applying the same procedure to the rest of the cases, we get also $\frac{1}{4}$, This means that the bit error rate is a 25%. This is the smallest error rate that can be achieved for an election of measuring basis by Eve, so any error rate above this value is a sign of potential eavesdropping. This number is a good approximation for Alice and Bob to know when to discard the key generation, although they would also have to take into account the effects of quantum noise.

When Alice and Bob carry on the information reconciliation, Eve might get some extra information about the key. However, with the subsequent privacy amplification, she will lose practically all knowledge of the key with high probability.

F. Photon Number Splitting Attack (PNS)

The Photon Number Splitting Attack (PNS) is a particular type of attack that takes advantage of the imperfections derived from the implementation of the BB84. It is really difficult to generate discrete individual photons as BB84 theoretically requires. That is why many times weak laser pulses are used to encode the bits. These pulses contain a large number of photons. In this context, Eve's strategy consists on intercepting a small number of photons from the pulse that represents a qubit, and let the remaining photons pass to Bob. Later, she waits for Alice to reveal the basis she used to encode the qubit and she measures the intercepted qubit to get information about it. The advantage of this attack is that Eve can intercept the qubits without being detected, since she does not manipulate the photons that Bob receives [9].

G. SARG04

The SARG04 is a variation of the BB84 protocol that was developed in 2004 to protect against the PNS attack. The initial phase of the key generation is exactly the same as the BB84. However, in SARG04, after Bob measures his qubits, Alice does not announce publicly the basis she used to encode the bits. Instead, she prepares a pair of non-orthogonal states for every qubit, where one of the states is the initial correct one, and announces them. The four possible pairs are $p_1 = (|0\rangle, |+\rangle)$, $p_2 = (|0\rangle, |-\rangle)$, $p_3 = (|1\rangle, |+\rangle)$ and $p_4 = (|1\rangle, |+\rangle)$. At this point, Bob knows that one of the two states that Alice announced is the correct one. He can now check if his previous measurement is consistent with either of the two states. If it is compatible with both states, he cannot infer which is the right one, so he announces that the bit is not valid. Otherwise, if only one of the states is consistent with his measurement, Bob can determine the right bit, announcing that it is valid [10].

Let us consider a practical example to visualize how the protocol works. Alice prepares the initial state $|1\rangle$ and sends it to Bob. If Bob measures it in the Z-basis, the only possible result is $|1\rangle$. However, if he measures it in the X-basis, he can get either $|+\rangle$ or $|-\rangle$ with equal probability $\frac{1}{2}$. Now consider that Alice sends the pair p_3. If Bob's measurement was in the Z-basis, both states of the pair ($|1\rangle$ and $|+\rangle$) could have given the result $|1\rangle$, so the bit is invalid. On the contrary, the result $|1\rangle$ is not compatible with a measurement of the state $|+\rangle$ in the X-basis, so the only possible state of the pair is $|1\rangle$. As a result, a measurement in the X-basis by Bob would give a valid bit 1.

With respect to Eve, even though she can intercept the photons with the PNS attack and know the pair sent by Alice, she cannot determine all the bits since she has no information about which basis used Bob to measure each qubit.

V. CONCLUSION

Our in-depth analysis of the BB84 Quantum Key Distribution (QKD) protocol reveals a robust method for secure key exchange, taking advantage of the principles of quantum mechanics. However, our examination also highlighted inherent imperfections, like the presence of quantum noise, and potential security vulnerabilities within the protocol. Against this situation, we introduced the information reconciliation and privacy amplification techniques to reduce noise and eavesdropping effects, and we presented the SARG04 protocol as an alternative to prevent Photon Number Splitting Attacks. Although there are other more sophisticated protocols, it is important to understand the BB84 protocol in depth since it establishes the fundamental concepts in Quantum Key Distribution.

[1] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, October 1997.

[2] Lov K. Grover. A fast quantum mechanical algorithm for database search, 1996.

[3] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, December 2014.

[4] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.

[5] Y. C. Jeong, Y. S. Kim, and Y. H. Kim. Effects of depolarizing quantum channels on bb84 and sarg04 quantum cryptography protocols. *Laser Physics*, 21(8):1438–1442, July 2011.

[6] Jesus Martinez-Mateo, Christoph Pacher, Momtchil Peev, Alex Ciurana, and Vicente Martin. Demystifying the information reconciliation protocol cascade, 2014.

[7] YG Yang, P Xu, R Yang, et al. Quantum hash function and its application to privacy amplification in quantum key distribution, pseudo-random number generation and image encryption. *Scientific Reports*, 6:19788, 2016.

[8] Nilanjana Datta. Quantum cryptography: Bb84 quantum key distribution. *DAMTP Cambridge*, 2019-2020.

[9] Maria Sabani, Ilias Savvas, Dimitrios Poulakis, and Georgios Makris. Quantum key distribution: Basic protocols and threats. In *Proceedings of the 26th Pan-Hellenic Conference on Informatics*, PCI '22, page 383–388, New York, NY, USA, 2023. Association for Computing Machinery.

[10] Valerio Scarani, Antonio Acín, Grégoire Ribordy, and Nicolas Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical Review Letters*, 92(5), February 2004.