Derivation of the quantum bit-error-rate for BB84 protocol based on the phase-covariant cloning machine

Mhlambululi Mafu[1], **Francesco Petruccione**[1,2]

[1] Centre for Quantum Technology, School of Chemistry and Physics, University of KwaZulu-Natal, P/Bag X54001 Durban, South Africa

[2] National Institute for Theoretical Physics (NITheP), KwaZulu-Natal, South Africa

E-mail: mafum@ukzn.ac.za, petruccione@ukzn.ac.za

Abstract. Based on the laws of physics, in particular the no-cloning theorem, quantum key distribution makes possible the distribution of a secret key between two legitimate parties commonly known as Alice and Bob. The third party known as an eavesdropper, Eve, can not clone the quantum states sent by Alice and then re-send a perfect copy to Bob without being detected. However, the phase-covariant cloning machine seems to be the best cloning machine for the BB84 quantum states but there is a trade-off between the quality of the clone and the amount of information that Eve can gain while the protocol remaining secure. By using the phase-covariant cloning machine to illustrate strategies performed by the eavesdropper, we arrive at the quantum bit-error-rate of 0.1464, which agrees with previous results.

1. Introduction

Quantum cryptography or more exactly quantum key distribution (QKD) provides the only physically secure and proven method for the transmission of a secret key between two distant parties, Alice and Bob, who are connected by an authenticated classical channel and an insecure quantum channel [1]. The security of QKD is based on the laws of physics rather than on the complicated mathematical algorithms to afford security [2, 3]. Specifically, QKD is based on the no-cloning theorem [4] which prohibits perfect cloning of an unknown quantum state with perfect fidelity and also on the Heisenberg uncertainty principle [5].

Wootters and Zurek showed that it is impossible to construct a device that will produce an exact copy of an arbitrary quantum state [4]. If perfect cloning was allowed then Eve would duplicate exact copies of the signal states being transmitted between legitimate parties. However imperfect cloning is possible, but it comes at a cost of being detected. For example, Eve can make a poor clone for herself and then send a perfect clone to Bob without being detected, but does not obtain much information about the key. On the contrary, she can make a perfect clone for herself and then send a poor copy to Bob. However, this affords her to obtain enough information but would reveal her presence to the legitimate parties.

In a QKD protocol, the quantum-bit-error-rate (QBER) refers to the fraction of positions where Alice's and Bob's bit strings differ. QBER is generally a direct measure for the secrecy of Alice and Bob's strings since any eavesdropping strategy would perturb the correlations between

them. For example, if the QBER is very high, the two parties abort the protocol or else they use the classical post-processing procedure to distill a secret key.

The security proof of the BB84 protocol [6] against arbitrary eavesdropping strategies was first shown in a complicated proof by Mayers [7]. Later, a simpler proof was shown by Lo and Chau [8]. However, their proof needs a quantum computer to implement it. A number of years later, Shor and Preskill generalized the ideas of Lo and Chau's security proof [8] and proposed a simpler proof for the BB84 protocol [9]. Many versions of security analysis have been derived for this protocol [10, 11, 12]. This protocol was first proven to be unconditionally secure by Inamori [13]. We highlight that this unconditional security proof also takes into account the finite-size key effects and this is immediate to practical implementations of the protocol.

There is a trade-off between the quality of the clone and the amount of information that Eve can gain about the key. Hence in this paper, our goal is to calculate an upper bound on the achievable information that Eve can gain but still the protocol remaining secure. In our derivation, we normalize clearly the states to be cloned in order to explicitly arrive at a QBER of 0.14644, which has been proven in various papers [14, 9].

2. BB84 Protocol

The BB84 protocol utilizes two communication channels between Alice and Bob. It consist first of a public classical channel where each party including the eavesdropper can listen to conversations but cannot change the contents of the message and, second of a quantum communication channel used for the transmission of quantum signals. However, the quantum communication channel is assumed to be insecure. This means that the eavesdropper has got all the resources needed to manipulate the signals. The protocol uses four quantum states $\{|0\rangle, |1\rangle, |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$. These basis states can be represented by any two-level quantum system, for example, by photon polarization and spin 1/2 systems. For linearly polarized photons, the first two states correspond to vertically ($\uparrow$) and horizontally polarized ($\rightarrow$) photons. For circularly polarized photons, the last two states correspond to polarization angles $45°$($\nearrow$) and $-45°$($\nwarrow$) with respect to the vertical axis. The states $|0\rangle$ and $|+\rangle$ represent bit value 0 while the states $|1\rangle$ and $|-\rangle$ represent bit value 1. The pairs $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ form two non-orthonormal and conjugate bases. The BB84 protocol consists of the following steps:

a) **Quantum Transmission Phase**

Alice randomly generates a bit string that she wants to send. For each bit, she randomly and independently chooses her encoding basis and prepares the states. She sends these prepared states via the insecure quantum channel. Upon receiving these states, Bob independently of Alice randomly chooses his measurements basis for each qubit he receives. Bob records his measurements bases and also the result of the measurements.

b) **Bases Announcement**

Alice and Bob communicate over the unjammable classical channel to compare the bit value of each basis, discarding those instances in which they used different bases. This step is called sifting. Statistically, this happens in half of the cases. The remaining sequence of bits forms the sifted key.

c) **Error estimation**

Ideally, in the absence of errors, the raw key should be identical between Alice and Bob meaning that Eve has no information and therefore the raw key becomes the secret key. Alice and Bob can check whether an eavesdropper was present or not by checking the difference between their keys (i.e., error rate) by comparing some randomly chosen bits. Let us assume that the error rate for measurements in both bases are the same

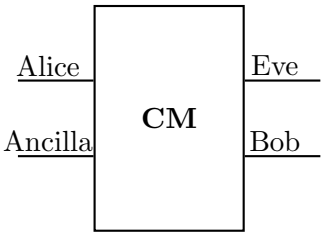

Figure 1. Eavesdropping by using a phase-covariant cloning machine. **CM** represents the cloning machine.

and equal to ε. If the calculated error rate is higher than some prescribed threshold they abort the protocol. Otherwise they have to perform classical post-processing and this is performed on the classical channel. At the end of this processing Alice and Bob share a truly secret key or nothing at all since they abort the protocol.

3. Description of the phase-covariant cloning machine

Regardless of the no-cloning theorem, the best eavesdropping strategy for the BB84 quantum states can be achieved by using the phase-covariant cloning machine [15]. This cloning machine consists of two inputs states labelled as Alice, $|0\rangle_a$ and ancilla $|Q_0\rangle_x$. These are states to be cloned. The cloning machine gives out a state which is sent to Bob, $|0\rangle_b$ and another to Eve, $|\bar{Q}_0\rangle_x$ which she keeps. This is shown in Figure 1.

We describe the behavior of an ideal quantum copying machine as

$$|s\rangle_a|Q\rangle_x \rightarrow |s\rangle_a|s\rangle_b|\bar{Q}\rangle_x, \tag{1}$$

where $|s\rangle_a$ represents the *in* state of the original mode to be copied, $|Q\rangle_x$ represents the *in* state of the copying machine, $|s\rangle_b$ represents the *out* state of the copy mode and $|\bar{Q}\rangle_x$ represents the final state of the copying machine.

The cloning machine can be described by the following transformation rules on the *in* states $|0\rangle_a$ and $|1\rangle_a$ as

$$|0\rangle_a|Q\rangle_x \rightarrow |0\rangle_a|0\rangle_b|Q_0\rangle_x, \tag{2}$$

and

$$|1\rangle_a|Q\rangle_x \rightarrow |1\rangle_a|1\rangle_b|Q_1\rangle_x. \tag{3}$$

We note that the basis vectors $|0\rangle_a$ and $|1\rangle_a$ can be perfectly cloned but others cannot be. Instead of using these quantum states $|0\rangle_a$ and $|1\rangle_a$ which can be copied ideally, we use the Pauli matrix **Y** to demonstrate what happens in a real scenario as

$$|0\rangle_a = \tfrac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \tag{4}$$

and

$$|1\rangle_a = \tfrac{1}{\sqrt{2}}(|0\rangle - i|1\rangle). \tag{5}$$

The action of the phase covariant cloning machine can now be described as follows

$$|0\rangle_a|Q_0\rangle_x \rightarrow |0\rangle_b|\bar{Q}_0\rangle_x, \tag{6}$$

$$|1\rangle_a|Q_0\rangle_x \rightarrow \cos\gamma|1\rangle_b|\bar{Q}_1\rangle_x + i\sin\gamma|0\rangle_b|\bar{Q}_0\rangle_x, \tag{7}$$

where $0 \leq \gamma \leq \pi/2$. We use the basis $\{|0\rangle, |1\rangle\}$ to explain how the cloning machine operates when various states are sent by the following operation

$$|a\rangle_\alpha|Q_0\rangle_x \rightarrow \sum_{b,c\in\{0,1\}} \zeta_{abc}|b\rangle_\beta|c\rangle_{\text{Eve}}, \tag{8}$$

with,

$$\zeta_{abc} = e^{i(a+b+c)\pi/2}((-1)^a + (-1)^b\cos\gamma + (-1)^c\sin\gamma), \tag{9}$$

where γ determines the quality of the two clones. If Bob measures a $|1\rangle$ when Alice has sent a $|0\rangle$ this results in an error in Alice's and Bob's key elements. We find that

$$\begin{aligned} |\zeta_{010}|^2 &= (1+\cos\gamma-\sin\gamma)^2 \\ &= 2+2\cos\gamma-2\sin\gamma-2\cos\gamma\sin\gamma, \end{aligned} \tag{10}$$

and

$$\begin{aligned} |\zeta_{011}|^2 &= (1-\cos\gamma-\sin\gamma)^2 \\ &= 2-2\cos\gamma-2\sin\gamma+2\cos\gamma\sin\gamma. \end{aligned} \tag{11}$$

Then, we can find the error probability by evaluating $|\zeta_{010}|^2 + |\zeta_{011}|^2$ as follows

$$\begin{aligned} |\zeta_{010}|^2 + |\zeta_{011}|^2 &= (1-\cos\gamma)^2(1-\cos\gamma)\sin\gamma + \sin^2\gamma \\ &\quad + (1-\cos\gamma)^2 - 2(1-\cos\gamma)\sin\gamma + \sin^2\gamma \\ &= 4(1-\cos\gamma). \end{aligned} \tag{12}$$

Now, our goal is to calculate the normalization constant where we use $|\psi\rangle = \sum_{b,c\in 0,1}\zeta_{abc}|b\rangle_\beta|c\rangle_{\text{Eve}}$, $a \in 0,1$ and the fact that $||\psi||^2 = \langle\psi|\psi\rangle$ and proceed as follows

$$\begin{aligned} |\psi\rangle &= \zeta_{a00}|0\rangle|0\rangle + \zeta_{a10}|1\rangle|0\rangle + \zeta_{a01}|0\rangle|1\rangle + \zeta_{a11}|1\rangle|1\rangle \\ \langle\psi| &= \zeta^*_{a00}\langle 0|\langle 0| + \zeta^*_{a10}\langle 1|\langle 0| + \zeta^*_{a01}\langle 0|\langle 1| + \zeta^*_{a11}\langle 1|\langle 1| \\ \langle\psi_{a=0}|\psi_{a=0}\rangle &= 2((1+\cos\gamma)^2+\sin^2\gamma) + 2((1-\cos\gamma)^2+\sin^2\gamma) \\ &= 8. \end{aligned} \tag{13}$$

The amount of error between Alice's and Bob's key elements can be obtained by evaluating the probability that Bob measures $|1\rangle$ although Alice sent the state $|0\rangle$. This is obtained by calculating the probability mass on the $|1\rangle_b$ state. This is the probability that Bob measures $|1\rangle$ exactly and we can calculate it as follows

$$\varepsilon = \sum_{c=0,1}|\zeta_{01c}|^2 = 4(1-\cos\gamma)/8 = (1-\cos\gamma)/2. \tag{14}$$

The degree of correlations between Alice and Bob can be quantified by the mutual information which is expressed as $I(A:B) = H(A) - H(A|B)$. The entropy of Alice's string A equals $H(A) = 1$ and the conditional entropy of A given B is given by $H(A|B) = h(\varepsilon)$. This can then be written as

$$\begin{aligned} I(A:B) &= H(A) - H(A|B) \\ &= 1 - h(\varepsilon) \\ &= 1 - h[(1-\cos\gamma)/2], \end{aligned} \tag{15}$$

where $h(\varepsilon) = -\varepsilon \log_2 \varepsilon - (1-\varepsilon)\log_2(1-\varepsilon)$ is the binary entropy function. The probability of Eve guessing a result can be found by calculating the probability on the $|1\rangle_{\text{Eve}}$ state which is

$$\varepsilon = \sum_{b=0,1} |\zeta_{0b1}|^2. \tag{16}$$

Also, by using $\zeta_{abc} = e^{i(a+b+c)\pi/2}((-1)^a + (-1)^b \cos\gamma + (-1)^c \sin\gamma)$ we find that,

$$\begin{aligned} |\zeta_{001}|^2 &= (1 + \cos\gamma - \sin\gamma)^2 \\ &= 2 + 2\cos\gamma - 2\sin\gamma - 2\cos\gamma\sin\gamma, \end{aligned} \tag{17}$$

$$\begin{aligned} |\zeta_{011}|^2 &= (1 - \cos\gamma - \sin\gamma)^2 \\ &= 2 - 2\cos\gamma - 2\sin\gamma + 2\cos\gamma\sin\gamma. \end{aligned} \tag{18}$$

We again find the error probability by evaluating $|\zeta_{010}|^2 + |\zeta_{011}|^2$ as follows

$$\begin{aligned} |\zeta_{001}|^2 + |\zeta_{011}|^2 &= 2 + 2\cos\gamma - 2\sin\gamma - 2\cos\gamma\sin\gamma \\ &\quad + 2 - 2\cos\gamma - 2\sin\gamma + 2\cos\gamma\sin\gamma \\ &= 4(1 - \sin\gamma). \end{aligned} \tag{19}$$

It can also be recognized that by using the same procedure as in Equation (13), the normalization is again calculated and found equal to $\langle\psi_{a=0}|\psi_{a=0}\rangle = 8$. Then, we can evaluate the error probability as

$$\varepsilon = \sum_{b=0,1} |\zeta_{0b1}|^2 = 4(1 - \sin\gamma)/8 = (1 - \sin\gamma)/2. \tag{20}$$

Again, the degree of correlations between Bob and Eve is quantified by the mutual information and is calculated as

$$\begin{aligned} I(B:E) &= H(B) - H(B|E) \\ &= 1 - h(\varepsilon) \\ &= 1 - h[(1 - \sin\gamma)/2]. \end{aligned} \tag{21}$$

In order to determine whether the channel is secure for communication, one must compare the mutual information between Alice and Bob, $I(A:B)$ and the minimum mutual information between each party and Eve. This gives us an expression for the secret fraction r and is expressed as

$$r = I(A:B) - \min(I_{AE}, I_{EB}), \tag{22}$$

The secret key fraction is expressed as $r = \ell/N$ where, ℓ is the length of the secret key to be extracted and N is the number of signals exchanged by Alice and Bob in a run of key exchange. In this scheme, the optimal mutual information between Alice and Bob is the same. We use the Csiszár-Körner bound [16] which is expressed as

$$\ell = I(A:B) - \max_{\text{Eve}} I(A:E). \tag{23}$$

In order to find the security bound for individual attacks we can express

$$I(A:E) = \max_{\text{Eve}} I(A:E), \tag{24}$$

and similarly $I(E:B)$ is defined in the same manner. The term $\max_{\text{Eve}}$ means that one must maximize the mutual information over Eve's strategies. Then the amount of information gained by the eavesdropper as a function of error rate can expressed as

$$\begin{aligned} I(A:E) &= 1 - h[(1-\sin\gamma)/2] \\ &= 1 - h[\tfrac{1}{2} - \sqrt{\varepsilon(1-\varepsilon)}], \end{aligned} \tag{25}$$

where $\varepsilon = (1-\cos\gamma)/2$ from Eq (14). In the case of $\gamma = \pi/4$, the two clones have the same quality. Therefore, if we take $\gamma = \pi/4$ (this is where we evaluate the minimum of $I(B:E) = I(A:E)$), this equation gives the upper bound on the bit-error-rate for the BB84 protocol by using one-way classical post-processing. The value of the QBER becomes $\varepsilon = 0.14644$ at which it is safe to extract a secret key. This is the limiting QBER at which the communication channel is considered to be secure for the generation of the security key. We note that this derived QBER value agrees with the previous results which appear in Refs. [14, 9].

4. Conclusion

Based on the above calculation, we recognize that the most dangerous eavesdropping attack can be realized with the aid of phase-covariant cloning machine, which was used to perfectly clone the quantum states of the BB84 protocol. This can also be interpreted via the complimentarity principle. If Bob receives the first clone and the second clone is the eavesdropper's copy then the more Eve knows Alice and Bob's signals, the less strongly their signals are correlated, thus leading to detection. This means the quantum bit-error-rate will be above 0.1464, so they abort the protocol because the channel is no longer secure for reliable communication.

Acknowledgments

This work is based on research supported by the South African Research Chair Initiative of the Department of Science and Technology and National Research Foundation.

References

[1] Scarani V, Bechmann-Pasquinucci H, Cerf N, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
[2] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145–195
[3] Ekert A K 1991 *Phys. Rev. Lett.* **67**(6) 661–663
[4] Wooters W and Zurek W 1982 *Nature* **299** 802
[5] Busch P, Heinonen T and Lahti P 2007 *Physics Reports* **452** 155–176
[6] Bennett C and Brassard G 1984 *in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing (IEEE, New York)* p 175
[7] Mayers D 2001 *J. Assoc. Comput. Mach.* **48** 351–406
[8] Lo H and Chau H 1999 *Science* **283** 2050–2056
[9] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441–444
[10] Xiangbin W 2005 *Phys. Rev. A* **71** 052328
[11] Gottesman D and Preskill J 2001 *Phys. Rev. A* **63** 022309
[12] Gottesman D and Lo H 2003 *IEEE Trans. Info. Theory* 457–475
[13] Inamori H, Lütkenhaus N and Mayers D 2007 *Eur. Phys. J. D* **41** 599–627
[14] Branciard C, Gisin N, Kraus B and Scarani V 2005 *Phys. Rev. A* **72** 32301
[15] Bruss D, Cinchetti M, Mauro G and Macchiavello C 2000 *Phys. Rev. A* **62** 12302
[16] Csiszár I and Korner J 1978 *IEEE Trans. Info. Theory* **24** 339–348