Security of quantum key distribution

Mhlambululi Mafu

Department of Physics and Astronomy, Botswana International University of Science and Technology, P/Bag 16, Palapye, Botswana

E-mail: mafum@biust.ac.bw

Abstract. Quantum cryptography forms one of the most mature fields of information theory. The goal of quantum cryptography is to create a secret key between authorized parties. In this work, we explain the role played by quantum mechanics in cryptographic tasks and also investigate how secure is quantum cryptography. More importantly, we show by a simple security proof that for any state sent by the sender, the eavesdropper can only guess the output state with a probability that will allow her not to learn more than half of the classical Shannon information shared between the legitimate parties. This implies that with high probability, the shared key is secure.

1. Introduction

Quantum key distribution (QKD), one aspect of quantum cryptography, provides a secure method for distributing cryptographic keys between two parties conventionally known as Alice (sender) and Bob (receiver), who are connected by a quantum channel and an authenticated classical channel in the presence of an extremely competent malicious party, an eavesdropper, Eve [1]. The security of a QKD protocol is mainly based on the laws of quantum mechanics, which state that (i) one cannot make a measurement without perturbing the system unless the quantum state is compatible with the measurement. If there is no disturbance in the system, then no measurement was made, which implies that there was no eavesdropping. Therefore, Eve cannot intercept the information being transmitted in the communication channel without introducing disturbances that would reveal her presence; this is also known as quantum indeterminacy, (ii) it is impossible to duplicate an unknown quantum state with perfect fidelity. This means that Eve cannot intercept the channel and get hold of the quantum system, make a copy of the system and the copy to Bob without being detected. Therefore, quantum mechanics guarantees that the two parties can exchange a secret key securely because the key always remains uncompromised.

Based on Wiesner's idea of conjugate coding [2], Bennett and Brassard in 1984 proposed a first established and operable QKD protocol now commonly known as the BB84 protocol [3]. In 1991, Ekert [4] extended the idea by introducing quantum entanglement and the violation of Bell's theorem [5]. Since then, several protocols have been proposed by both theorists and experimentalists. These include: Bennett 1992 (B92) [6], six state [7]; Phoenix, Barnett and Chefles 2000 (PBC00) [8], the Scarani, Acín, Ribordy, Gisin 2004 (SARG04) protocol [9]. These protocols belong to a family called Discrete-Variable (DV) protocols. However, there exists another family of protocols called continuous-variable protocols and Distributed-Phase-Reference (DPR) protocols [10].

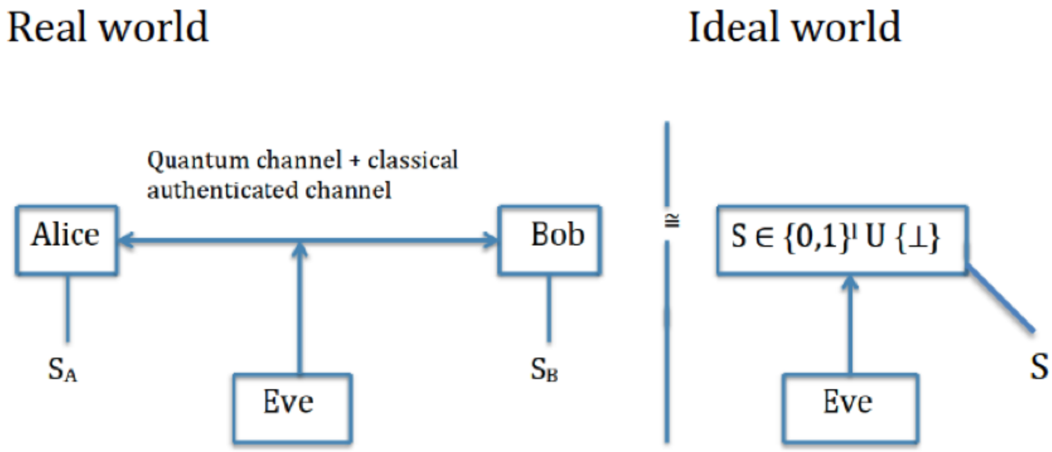

Figure 1. Comparison between what happens in a real and ideal quantum cryptographic world. Alice and Bob use the quantum and classical authenticated channel in the presence of Eve. At the end of the communication, in the real world Alice and Bob share two correlated secret keys S_A and S_B, respectively. In an ideal world, the access of Eve is broken; therefore Alice and Bob share a perfect secret key S.

The aim of this work is to present a simple security proof for a quantum protocol based on measurements on a maximally entangled state. In particular, we demonstrate how the laws of quantum mechanics afford security especially which properties are important in providing security for QKD protocols. This article is organized as follows. In section II we briefly describe the quantum communication procedure. In section III, we provide a short review of QKD security. In section IV, we give a description of the operation principle for our proposed entanglement-based protocol, which we are going to study. In this section we also outline the security requirements for QKD. Our main result is that the success guessing probability, p for the eavesdropper to guess the state sent by Alice or received by Bob will always result in Eve gaining less than half of the information being transmitted i.e., $H(p) = Pr[G = A|E] \leq 1/2$, where $H(p) = -p\log_2 p - (1-p)\log_2(1-p)$ is the classical Shannon information and G is the guess for output A (Alice) when given E (Eve). This means that the eavesdropper can only learn less of the transmitted information and this forbids her from trying to reconstruct the original message shared by the legitimate parties with high accuracy. This implies that the exchanged secret key is always secure. Lastly, section V is the conclusion.

2. Quantum communication procedure

Alice and Bob first use the quantum channel to distribute quantum states and then apply a quantum key distillation scheme to generate a common string of secret correlated data which are later transformed into a secret key. The eavesdropper can freely interact with the transmitted states while the two parties communicate and try to extract information. However, Eve can only perform the most general attack allowed by the laws of quantum mechanics. The quantum channel is used to transmit quantum signals while the classical channel is used to transmit classical information. The classical channel is authenticated so that Eve cannot learn the information that is being transmitted.

In a real world, at the end of the protocol, Alice outputs the key S_A while Bob outputs the key S_B. The output keys must be identical, but because of the presence of an eavesdropper and errors in the channel, the keys are almost identical. However, in the ideal world, Eve's access of the key is detected and also there are no errors in the communication channel, therefore Alice and Bob generate a perfect secret key S which is of length l. This is shown in Figure 1. This perfect secret key is then used for sending private messages by means of the one-time pad.

3. Review of QKD security

In the last two decades, a lot of progress has been realized in the study of QKD security. Today, the unconditional security i.e., security guaranteed in an information-theoretical sense has been established for many protocols. The first unconditional security proof of QKD was proposed by Mayers in 1996 [11]. Since then, various techniques for proving the security of QKD protocols have been developed [10]. The security proofs generally depend on the construction of the protocol and also on its practical implementation. For example, the unconditional security proofs for the BB84 based protocols have long since been realized [12]. This is mainly because they share a common property of being symmetrical. On the side, the security proofs for the class of DPR protocols still remain unrealized [10, 13], mainly because their construction and encoding deviates from the usual symmetry that exist in BB84-type based protocols. Moreover, the previous security proofs could provide bounds only in the asymptotic limit of infinitely long keys, which is not realistic. But recently, the tools for studying QKD security in the finite-size limit have now become available [14]. This has been followed by various studies on security in the finite-size limit [14, 15, 16, 17, 18, 19, 20, 21]. In these papers, it was shown that the bits which are processed in QKD are indeed of finite length.

However, one of the greatest challenges that still remain in QKD implementations is a mismatch between the theoretical security proofs to real devices. This is because several assumptions are usually made when proving the security of QKD protocols. These assumptions are; devices do what they are supposed to do (according to a specified model) and not more, there should be access to perfect or almost perfect randomness (locally), there should be no side-channels and quantum theory is correct.

In order for a QKD protocol to be secure, it has to satisfy a number of security requirements. These requirements are [22];

a) correctness - a QKD protocol is called ε_{cor}-correct if, for any strategy by the eavesdropper $Pr[S_A \neq S_B] \leq \varepsilon_{\text{cor}}$, where S_A and S_B are Alice's and Bob's output classical keys, respectively.

b) secrecy - if $S \neq \perp$, then S is uniform $\{0,1\}^l$ and independent of Eve.

c) Robustness - a QKD protocol is said to be "robust" if it's guaranteed that it does not abort as long as the eavesdropper is inactive. When an eavesdropper is inactive, the protocol would continue to generate a secret key, otherwise if an adversary tampers with the quantum channel, the protocol recognises the attack and aborts the computation of the key.

d) Finally, a QKD is secure if it is correct and secret, that a protocol is ε-secure, if it is ε_{cor}-correct and ε_{sec} with $\varepsilon_{\text{cor}} + \varepsilon_{\text{sec}} \leq \varepsilon$.

4. Operation of our proposed QKD protocol

A source prepares and distributes a maximally entangled quantum state where one system is sent to Alice and another to Bob. This is shown in Figure 2. Alice and Bob then perform measurements in two mutually unbiased bases on their system respectively. In the absence of an eavesdropper, if they measure in the same basis they obtain perfectly correlated outcomes, which are completely random. The three parties will then share a quantum state $|\psi\rangle_{ABE}$. An example of this protocol is the E91 protocol [4].

If the authorized parties notice some errors in Bob's measurements, this implies that Eve has measured some of the photon polarizations. Therefore, QKD is secure because either of the following happens; if the error rate observed by Alice and Bob is lower than a critical

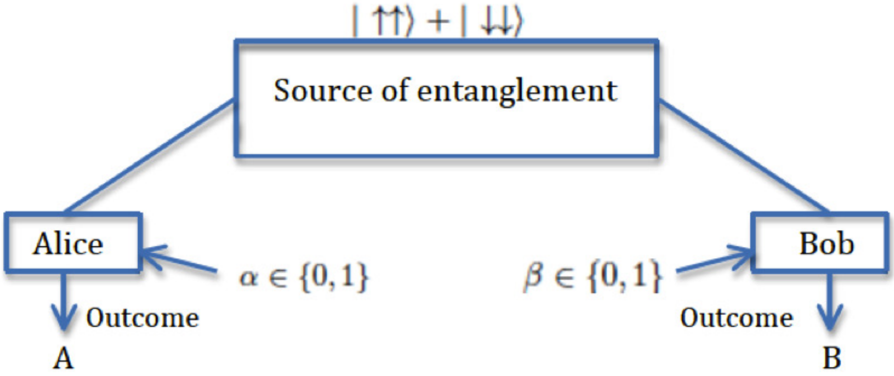

Figure 2. The operation principle of the proposed QKD protocol. An entanglement source produces a pair of entangled signals, which are randomly measured in certain bases chosen by Alice and Bob separately. Alice and Bob generate outcomes A and B respectively.

	Pr[A=G]	Pr[B=G]	
$\phi_\alpha = 0$	p	p	$\beta = 0$
$\phi_\alpha = \delta$		$\geq p - \delta^2$	$\beta = \delta$
$\phi_\alpha = 2\delta$	$\geq p - 2\delta^2$		
$\phi_\alpha = 3\delta$		$\geq p - 3\delta^2$	
$\phi_\alpha = \frac{1}{2}$		$\geq p - \frac{1}{2}\frac{\delta^2}{\delta}$	$\delta{=}\frac{1}{2}$

Table 1. Example of transmission of qubits between Alice and Bob showing some various possibilities and the result of the inferred bits. The probability that the eavesdropper makes a correct guess on the output held by Alice and Bob is written as p=[A=G] and p=[B=G], respectively, and δ is any value between 0 to 1.

value usually referred to as quantum-bit-error rate (QBER), in which case a secret key can be extracted by using techniques of classical information theory. However, if the error rate is larger than QBER, Alice and Bob throw their data away and never use them to encode any message. Therefore, the eavesdropper is prevented from learning any messages being communicated from Alice to Bob.

Our proposed protocol is executed by the following steps:

a) Alice chooses to measure photons in a certain basis and also the measurement direction of the polarisation e.g., Alice chooses ϕ_α and Bob chooses ϕ_β.
b) Repeat this experiment many times and check whether the statistics are compatible with the law of physics $p = \cos^2(\frac{\phi_\alpha - \phi_\beta}{2})$, where the angle ϕ_α and ϕ_β denotes the measurement direction of the polarisation [23].
c) If the statistics are compatible, then they may choose a particular basis $\phi_\alpha = \phi_\beta = 0$ and take $S_A = A$ and $S_B = B$, if not then $S_A = S_B = \perp$ i.e., they abort the protocol.

Theorem : Let G: guess for output A or B (on input $\phi_\alpha = 0$). We prove that for the classical random variable α, β and ϵ corresponding respectively to Alice, Bob and Eve's measurement outcomes, the joint entropy between Alice and Eve is always less than half, i.e., $I(\alpha, \epsilon) \leq 1/2$.

Proof: In the protocol, Alice and Bob test the presence of an eavesdropper by publicly comparing polarizations of a random subset of the photons on which they think they should agree. The probability that a photon sent by Alice is detected by Bob is p= Pr[A≠ B]=cos$^2(\frac{\phi_\alpha - \phi_\beta}{2})$. This means that Pr[A≠ B| $\phi_\alpha = 0, \phi_\beta = \delta$] $= \delta^2$. In Table 1, if ϕ_α and ϕ_β=0, then Pr[A=G]=Pr[B=G]=p. However, if $\phi_\alpha = \phi_\beta = \delta$, then the probability of choosing Pr[B=G] is $\geq p - \delta^2$ while the Pr[A=G] becomes $1 - p$. This can be generalized for $\phi_\alpha = 2\delta$ and $\phi_\alpha = 3\delta$.

As mentioned above, let α, β and ϵ be the classical random variables obtained by Alice, Bob and Eve, respectively, when they perform measurements on their quantum systems. The joint probability of the distribution for all the parties is expressed as $P(\alpha, \beta, \epsilon)$. By using only error correction and privacy amplification, Alice and Bob can extract a sent key from $P(\alpha, \beta, \epsilon)$ if and only if

$$I(\alpha) \geq (\alpha, \epsilon) \tag{1}$$

or

$$I(\alpha, \beta) \geq I(\beta, \epsilon), \tag{2}$$

where $I(\alpha, \beta)$=$H(\alpha) - H(\alpha|\beta)$ is the mutual information between Alice and Bob and $H(\cdot)$ is the Shannon entropy. Physically, this means that Bob must possess more information about Alice's bits than Eve does.

For such a source, the preparation quality [18] is given by

$$q = \max_{\epsilon,\beta}\{|\langle\epsilon|\beta\rangle|\}, \tag{3}$$

where $|\epsilon\rangle$ and $|\beta\rangle$ are the eigenvalues corresponding to α and β then,

$$I(\alpha, \epsilon) + I(\alpha, \beta) \leq 2\log_2(Nq), \tag{4}$$

where $I(\alpha, \epsilon) = H(\alpha) - H(\alpha|\epsilon)$ and $I(\alpha, \beta) = H(\alpha) - H(\alpha|\beta)$ are the entropies that correspond to the probability of the eigenvalues α priori to and deduced from any measurement by Eve and Bob, respectively, N is the dimension of the Hilbert space and in this case, $N = 2^n$. So, it follows that

$$I(\alpha, \epsilon) + I(\alpha, \beta) \leq \log_2(2^n 2^{-n/2}) = n. \tag{5}$$

Therefore, one can deduce that the secret key rate is obtained when $I(\alpha, \beta) \geq n/2$. Since, $I(\alpha, \beta) = H(\alpha) - H(\alpha|\beta)$, then

$$I(\alpha, \beta) = n[1 - p\log_2 p - (1-p)\log_2(1-p)]. \tag{6}$$

which gives us the sufficient condition

$$p\log_2 p + (1-p)\log_2(1-p) \leq 1/2, \tag{7}$$

on the error rate p. Because a key can only be extracted if $I(\alpha, \beta) \geq I(\beta, \epsilon)$, it follows that $I(\beta, \epsilon) \leq 1/2$ and this together with Equation (7) satisfies our theorem. Thus, the amount of information that Eve can gain about Bob's or Alice's bit is always less than half. A similar result has also been demonstrated in Ref [24]. This demonstrates that always, the eavesdropper has some limited knowledge of knowing the output from Alice or from Bob. Therefore, QKD provides a kind of security that is very secure.

5. Conclusion

We have demonstrated the principle of operation of QKD. We have shown how one can use the properties of the laws of quantum mechanics to allow the legitimate parties to share a secret key. In particular, we have shown that the eavesdropper cannot guess the output or outcome from Alice and gain more than half of the information being transmitted. This means that the key generated by quantum cryptography is always secure, thus showing the power of quantum mechanics in securing information.

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145–195

[2] Wiesner S 1983 *ACM Sigact News* **15** 78–88

[3] Bennett C, Brassard G *et al.* 1984 *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* vol 175 (Bangalore, India)

[4] Ekert A 1991 *Physical Review Letters* **67** 661–663

[5] Bell J 1964 *Physics* **1** 195–200

[6] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121–3124

[7] Bruß D 1998 *Phys. Rev. Lett.* **81** 3018–3021

[8] Phoenix S J, Barnett S M and Chefles A 2000 *Journal of Modern Optics* **47** 507–516

[9] Scarani V, Acín A, Ribordy G and Gisin N 2004 *Phys. Rev. Lett.* **92** 057901

[10] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301–1350

[11] Mayers D 1996 *J. ACM* **48** 351–406 ISSN 0004-5411

[12] Shor P and Preskill J 2000 *Physical Review Letters* **85** 441–444

[13] Mafu M, Marais A and Petruccione F 2014 *Appl. Math* **8** 2769–2773

[14] Scarani V and Renner R 2008 *Phys. Rev. Lett.* **100**(20) 200501

[15] Cai R and Scarani V 2009 *New Journal of Physics* **11** 045024

[16] Sheridan L, Le T P and Scarani V 2010 *New Journal of Physics* **12** 123019

[17] Abruzzo S, Kampermann H, Mertz M and Bruß D 2011 *Physical Review A* **84** 032321

[18] Tomamichel M, Lim C C W, Gisin N and Renner R 2012 *Nature communications* **3** 634

[19] Mafu M, Garapo K and Petruccione F 2013 *Physical Review A* **88** 062306

[20] Mafu M, Garapo K and Petruccione F 2014 *Phys. Rev. A* **90**(3) 032308

[21] Zhou C, Bao W S, Zhang H l, Li H W, Wang Y, Li Y and Wang X 2015 *Phys. Rev. A* **91**(2) 022313

[22] Renner R 2008 *International Journal of Quantum Information* **6** 1–127

[23] Hughes R J, Buttler W T, Kwiat P G, Luther G G, Morgan G L, Nordholt J E, Peterson C G and Simmons C M 1997 *AeroSense'97* (International Society for Optics and Photonics) pp 2–11

[24] Bennett C, Bessette F, Brassard G, Salvail L and Smolin J 1992 *Journal of Cryptology* **5** 3–28