Quantum key distribution security

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 key distribution, one aspect of 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. Unlike classical cryptography whose security is based on the difficulty of the mathematical and computational algorithm to provide security, the security of quantum cryptography is solely based on the laws of quantum mechanics. Therefore, 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 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 quantum key distribution is secure almost always.

1. Introduction

Quantum key distribution (QKD) enables secure distribution of 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]. A quantum channel allows quantum states to be transmitted. The security of QKD protocols 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. This implies that 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 acquire the quantum system, make a copy of the system and send the copy to Bob without being detected. Therefore, quantum mechanics guarantees that the two parties can exchange a secret key securely because the key remains always undisturbed.

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 invented 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

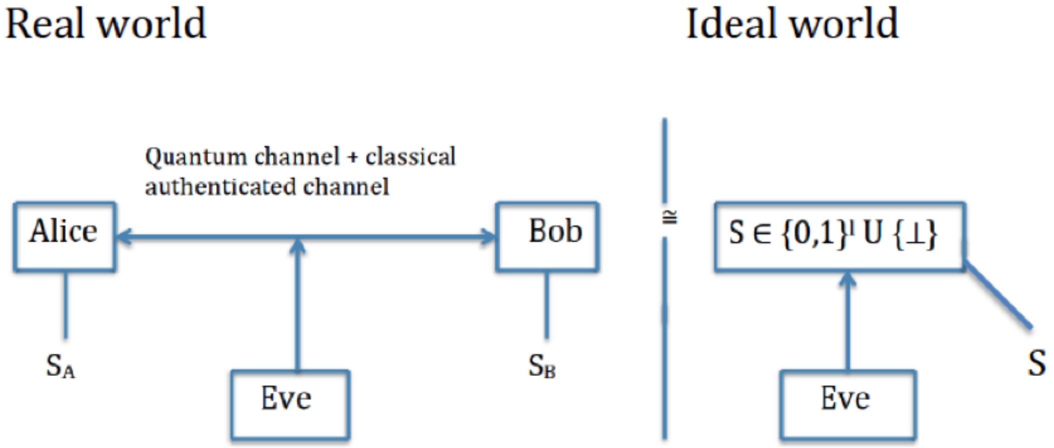

Figure 1. Comparison between what happens in a real and ideal quantum cryptographic world. Alice and Bob use the quantum and classical authenticated channel in the presence of Eve. At the end of the communication, in the real world Alice and Bob share two correlated secret keys S_A and S_B, respectively.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

exists another family of protocols called continuous-variable protocols and Distributed-Phase-Reference (DPR) protocols [10].

The aim of this work is to present the principle and a security framework for QKD protocols and also explain how the laws of quantum mechanics affords security. We show which properties of the laws of quantum mechanics are important in providing security for QKD protocols. This article is organized as follows. In section II we provide a brief description of the quantum communication procedure. In section III, we briefly outline the background of QKD security. In section IV, we give a description of the operation principle for the proposed entanglement-based version protocol, which we are going to study. In this section we also briefly 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 result in Eve gaining less than half of the information being transmitted i.e., $H(p)$=Pr$[G = A/B]\leq 1/2$, where $H(p)$ is the classical Shannon information and G is the guess for Alice's output A or Bob's output B. 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

In the ideal world, the Eve's access of the communication channel is prevented by the laws of physics and this results in no errors in the communication channel. Therefore, Alice and Bob output identical or a perfect secret key S which is of length l. However, 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. This is shown in Figure 1. The perfect secret key is then used for sending private messages by means of the one-time pad. The communication procedure is as follows; 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 authenticated so that Eve cannot learn the information that is being transmitted.

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 2001 [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 their practical implementation. For example, the unconditional security proofs for the BB84 based protocols have long since been realized [12]. This is because they share a common property of being symmetrical. However, the security proofs for the class of DPR protocols still remain unrealized [10], mainly because their construction and encoding deviates from the usual symmetry that exist in BB84-type based protocols. Moreover, the previous security proofs could only provide bounds in the asymptotic limit of infinitely long keys, which was not realistic. But recently, the study of security proof of QKD protocols in the asymptotic key length has been made in several papers [13, 14, 15, 16, 17, 18, 19, 20]. The bits that are processed in QKD are indeed of finite length. The tools to study security for QKD protocols in the finite-size limit were worked by Scarani and Renner in Ref [13]. However, one of the greatest challenges is that there still remains a mismatch between the theoretical security proof to real devices. The assumptions that are made in the analysis of security for QKD protocols are the following; devices do what they are suppose 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. Some of the QKD security requirements made in security proofs are [21];

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 the protocol aborts even though the eavesdropper is inactive.

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 $\varepsilon_{\text{cor}} + \varepsilon_{\text{sec}} \leq \varepsilon$.

However, one of the greatest challenges that still remain is a mismatch between the theoretical security proofs and real devices.

4. Operation of our QKD protocol

a) 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.

b) Alice and Bob then perform measurements in two mutually unbiased bases on their system respectively.

c) In the absence of an eavesdropper, if they measure in the same basis they obtain perfectly correlated outcomes which are completely random.

d) If the eavesdropper is present, then the three parties will share a quantum state $|\psi_{ABE}\rangle$. An example of this protocol is the E91 protocol [4].

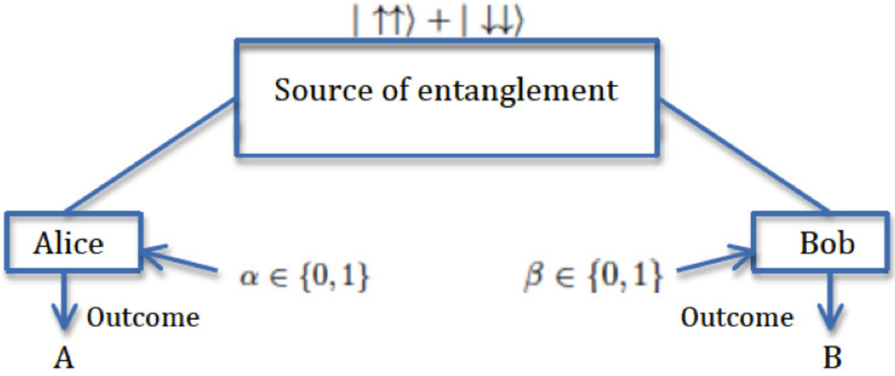

Figure 2. Principle of operation of a QKD protocol. An entanglement source emits pairs of entangled signals, which are then measured in certain bases chosen by Alice and Bob separately. Alice and Bob generate outcomes A and B respectively.

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

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.

If the authorized parties notice some errors in Bob's measurements, this implies that Eve has measured some of the quantum states. Therefore, QKD is secure because either of the following happens; if the error rate observed by Alice and Bob is lower than a critical 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; or the error rate is larger than QBER, in which case 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 following steps:

a) Alice chooses to measure photons in a certain basis and choose an angle e.g., Alice chooses α and Bob chooses β.

b) The experiment is repeated many times and check whether the statistics are compatible with the law of physics $p = \cos^2(\frac{\alpha-\beta}{2})$ [22].

c) If its compatible, then they may choose a particular basis $\alpha = \beta = 0$ and take $S_A = A$ and $S_B = B$, if not then $S_A = S_B = \perp$.

Theorem: Let G: guess for output A (on input $\alpha = 0$). We will prove that $H(p)$=Pr[G=A]$\leq \frac{1}{2}$ for any G by an eavesdropper.

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]=$\cos^2(\frac{\alpha-\beta}{2})$. This means that Pr[A≠ B| $\alpha = 0, \beta = \delta] = \delta^2$. In Table 1, if α and β=0, then Pr[A=G]=Pr[B=G]=p. However, if $\alpha = \beta = \delta$, 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 $\alpha = 2\delta$ and $\alpha = 3\delta$. The amount of Shannon information gained by Alice or Bob at the end of the protocol is equal to $H(p) = 1 + p \log p + (1 - p) \log(1 - p)$.

For example, in Table 1, in each of the cases the probability of success is always $1-p \geq p-\delta^2$. This will result in classical Shannon information between Alice and Bob being always greeter than a half, $H(p) \geq 0.5$. This implies that the amount information learned by Eve is always less than half. Therefore, the guessing probability of Alice or Bob's output always results in Eve gaining less than than half of the information.Thus, there is no measurement that Eve can perform and get a correct result with probability greater than half. A similar result has also been demonstrated in Ref [23]. 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 2001 *J. ACM* **48** 351–406 ISSN 0004-5411

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

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

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

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

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

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

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

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

[20] 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

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

[22] 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

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