Turkish Journal of Computer and Mathematics Education *Vol.14 No.02 (2023),119-124*

Research Article

Quantum key distribution from the origins to nowadays

M. S. MEGNOUNIF[a], A. GAFOUR[b]

[a]*EEDIS* Laboratory, computer science, *Djillali Liabes University*, Sidi Bel Abbes, Algeria.
[b]*EEDIS* Laboratory, computer science, *Djillali Liabes University*, Sidi Bel Abbes, Algeria.

Article History: *Received: 12 December 2022; Revised :15 January 2023; Accepted 10 February 202; Published online: 9 march 2023*

Abstract: This work traces the state of the art in quantum key distribution from the perspective of a computer scientist. A brief discussion of the relevant principles of quantum mechanics is given before reviewing the most important quantum key distribution protocols present in the literature. In particular, the BB84 protocol and its many variants will be described as well as Eckert's quantum entanglement approach. We will then see some of the problems that arise in practical implementations, including privacy amplification and the photon number splitting attack.

Keywords: quantum cryptography, quantum key distribution, QKD, BB84, Eckert, Bennet, Brassard, photon number division attack, PNS, privacy amplification.

1. Introduction

1. Introduction

Classical cryptography can be divided into two main branches: secret key or symmetric cryptography where both parties (Alice and Bob) must first exchange a secret key which is actually the weak point of this branch of cryptography, although some secret key schemes, such as one-time buffers, seem to be perfectly secure but are not always practical against an attacker with arbitrary computing power (Gisin. N et al 2002), and public-key cryptography, also known as asymmetric cryptography which has , In order to establish a secret key over an insecure channel, key distribution schemes based on public-key cryptography, such as Diffie-Hellman, are typically used. Unlike secret key cryptography, public key cryptography does not require the establishment of a shared secret key prior to communication. Instead, each party has a private key, which remains secret, and a public key, which it can distribute freely. If one party, say Alice, wants to send a message to another party, Bob, she must encrypt the message with Bob's public key, after which only Bob can decrypt the message using his private key. Indeed, algorithms have already been proposed to perform integer factorization and solve the discrete logarithm problem in polynomial time on a quantum computer (Shor.p 1997) (Bruss.D et al 2007).Note that the advent of a feasible quantum computer would render current public key cryptosystems obsolete and threaten key distribution protocols such as Diffie-Hellman, some of the principles that allow quantum computers to operate also offer an unconditionally secure solution to the key distribution problem. In addition, quantum mechanics also provides the ability to detect the presence of someone trying to learn the key, which is a novelty in the field of cryptography. Several research works are going in the direction of using quantum mechanics to allow a secure distribution of quantum keys (QKD). The objective of this paper is to review the most important quantum key distribution protocols and their security.

However, to understand these protocols, it is important to describe some principles of quantum mechanics. From these principles, protocols are divided into two categories: those based primarily on the Heisenberg uncertainty principle and those using quantum entanglement.

While most current research focuses on the development of practical quantum algorithms (Bruss.D et al 2007), a brief overview of the security of these protocols is explored in this paper. The work is structured as follows: in Section 2 we briefly discuss the fundamental principles of quantum mechanics. Section 3 describes protocols based on the Heisenberg uncertainty principle, in particular the BB84 protocol and its variants. Section 4 focuses on protocols using quantum entanglement, in particular the Eckert protocol. Section 5 deals with recent results in terms of maximum distance for quantum key exchange. In section 6 we discuss the theoretical capabilities of quantum cryptography and discuss security from a practical point of view. Finally, we end with a conclusion.

2. Fundamental Principles of Quantum Cryptography

The basic model of QKD protocols involves two parties, called Alice and Bob, exchanging a key and having access to a classical public communication channel and a quantum communication channel(see Figure1). A malicious intruder(Eve), is assumed to have access to both channels and no assumptions are made about the resources available to him. Once this basic model is established, we will describe in simple terms the quantum principles necessary to understand QKD protocols.

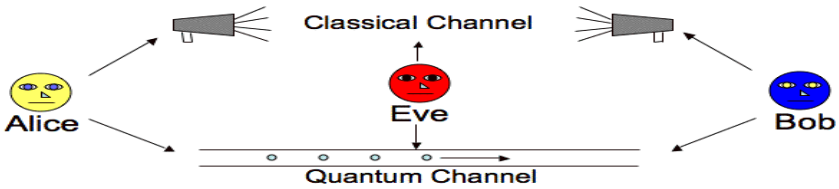

Fig 1: classical quantum key distribution (QKD) scheme

2.1 Heisenberg uncertainty principle

The security of quantum cryptography is based on several principles derived from quantum physics. The most important of these principles is the Heisenberg Uncertainty Principle (HUP), which states that in a quantum system, only one property of a pair of conjugate properties can be known with certainty. Heisenberg, who was working on the position and momentum of a particle, established that any conceivable measurement of the position of a particle would disturb its conjugate property, the momentum. It is therefore impossible to know both properties simultaneously with certainty. Quantum cryptography uses the polarization of photons on different bases as the conjugate property in question. This is because photons can be exchanged over fiber optic links and are perhaps the most practical quantum systems for transmission between two parties wishing to exchange keys. A famous theorem of quantum mechanics, the no-cloning theorem, follows intuitively from Heisenberg's uncertainty principle. The no-cloning theorem, published by Wooters, Zurek and Dieks in 1982 states that it is impossible to create identical copies of an arbitrary unknown quantum state (Bruss.D et al 2007). One could understand that without the no-cloning theorem, it would be possible to circumvent the Heisenberg uncertainty principle by creating multiple clones of a quantum state and measuring a different conjugate property on each copy. This would allow to know simultaneously and with certainty both conjugate properties of the original quantum particle, which is in contradiction with the Heisenberg uncertainty principle.

2.2 Quantum entanglement

The second important rule on which QKD can be based is the principle of quantum entanglement. Two particles can be entangled in such a way that when a particular property is measured on one particle, the opposite state will be immediately observed on the entangled particle. This is true regardless of the distance between the entangled particles. However, it is impossible to predict, before the measurement, the state that will be observed. It is therefore not possible to communicate via intricate particles without prior discussion of the observations on a classical channel. Communicating via entangled states, based on a classical information channel, is known as quantum teleportation and forms the basis of the Eckert protocol (Ekert.A.K 1991), which will be described in Section 4.

3. Protocols using the Heisenberg uncertainty principle

3.1 The BB84 protocol

The work of Charles Bennett and Gilles Brassard led, in 1984, to the publication of the first QKD protocol called BB84 (Bennett.C.H and Brassard.G 1984). Its basic principle is the Heisenberg uncertainty principle. It is currently one of the most important protocols and almost all other HUP-based protocols are derived from it. The basic idea of all these protocols is that Alice can transmit a random secret key to Bob by sending a string of photons where the bits of the secret key are encoded in the polarization of the photons. Heisenberg's uncertainty principle can be used to ensure that an eavesdropper cannot measure these photons and transmit them to Bob without changing the state of the photon, thus revealing its presence.

3.2 The SSP protocol

Another protocol inspired by BB84 is the six-state protocol (SSP) proposed by Pasquinucci and Gisin in 1999 (Bechmann-Pasquinucci.H, Gisin.N 1999). SSP is very similar to BB84, except that, as the name implies, instead of using two or four states, SSP uses six states on three orthogonal bases to encode the bits sent. This stipulates that an eavesdropper must choose the correct base from three possibilities. This causes the eavesdropper to produce a higher error rate and thus becomes easily detectable. Brus and Micchiavello proved in 2002 that such high-dimensional systems offer better security (Bruss.D,Macchiavello.C 2002). Although there are many variants of BB84, one of the most recent is SARG (Scarani.A et al 2004).

3.3 The SARG04 protocol

This protocol proposed in 2004 by Scarani, Acin, Ribordy and Gisin has the same first step as BB84. In the second step, when Alice and Bob determine for which bits their bases correspond, Alice does not directly reveal her bases. Instead, she announces a pair of non-orthogonal states, one of which is used to encode her bit. If Bob used the correct base, he will measure the correct state. If he made the wrong choice, he will not measure any of Alice's states and will not be able to determine the bit. The advantage of this protocol is when it is used in practical equipment, as we will see in section 6. So let's recap, BB84 was the first proposed QKD protocol and it was based on Heisenberg's uncertainty principle and many have built on the ideas of this protocol. Examples are B92, SSP and Sarg04. The following section describes the second family of protocols based on the quantum entanglement principle.

4. Protocols using quantum entanglement

In 1991 Artur Eckert, inspired by quantum entanglement, proposed a new approach to quantum key distribution. (Ekert.A.K 1991). In what follows, we will describe his protocol and its application to the HUP-based protocols described in the previous section.

4.1 The Eckert protocol

The Eckert protocol involves a channel where a single source emits pairs of entangled particles (polarized photons as an example) (Ekert.A.K 1991). Alice and Bob each receive a particle from each pair, then they each choose a random basis for measuring the received particles and then discuss in the open which basis they use for their measurements (As in BB84). Starting from the principle of quantum entanglement for each measurement where Alice and Bob use the same bases, they will have opposite results and each will obtain a string of bits which is the binary complement of the other. Either Alice(or Bob) could invert his key and will thus have the same secret key as Bob (or Alice). The presence of a spy can be revealed by examining the photons for which Alice and Bob have chosen different measurement bases. Alice and Bob can measure these photons in a third base and examine their results. In this way, they can test Bell's inequality which should not be verified for entangled particles (Gisin.N et al 2002). If the inequality is confirmed, we deduce that the photons are not really intricate and therefore imply the presence of a spy.

4.2 Variants of intricate BB84

In the Eckert protocol, if we suppose that Alice and Bob did not perform the Eckert entanglement check, and that Alice is the source, then we end up with exactly BB84. Bennet and Brassard noted that any variant of BB84 could be redesigned to use an entangled photon source instead of Alice being the source (Bennet et al 1992). In particular (Enzer.D et al 2002) described an intricate version of the SSP protocol with increased security. Many researchers have proven that the SARG04 protocol can tolerate fewer errors with a two-photon (intricate) source than with a single-photon (Alice) source (Fung.C et al 2006).

4.3 COW protocol

A new protocol, given by Scarani.A et al in 2004, has been proposed in the QKD framework based on weak coherent pulses at high bit rates. The protocol was called one-way coherent protocol (COW protocol). The main feature of the method is that the setup is experimentally simple and robust to interference visibility and photon number division attacks, making it more efficient in terms of secret bits distilled per qubit.

Alice sends μ-μ decoy sequences for security purposes. Bob measures the arrival time of the photon on his data line, the DB detector to obtain its key. Bob randomly measures the coherence between successive non-empty pulses, -1 -0‖ bit sequence or decoy sequence, with the interferometer and detectors DM1 and DM2. If the laser wavelength and phase in the interferometer are well aligned, we have all detection on DM1 and no detection on DM2. A loss of coherence and thus a reduction in visibility reveals the presence of a listener, in this case the key is simply thrown away, so no information will be lost (Abhishek Parakh 2015)(Inoue.K et al 2002) (M. Lucamarini.S. Mancini, 2005) (M. A. Nielsen and I. L. Chuang, 2000).

4.4. DPS Differential -phase-shift QKD (DPS-QKD) protocol

This is a new quantum key distribution scheme that has been proposed by K. Inoue et al.

From Alice's site, a pulse train of weak coherent states is randomly phase-modulated by $\{0, \pi\}$ for each pulse, and then transmitted to Bob with an average photon number less than 1 per pulse. From Bob's site, the phase difference is measured between the two sequential pulses with a delay of one bit. The Mach-Zender interferometer and photon detectors record the arrival time of the photons and which detector clicked. Bob, after transmitting the optical pulse train, tells Alice the time at which the photon was counted. From this time information and her modulation data, Alice knows which detector clicked on Bob's site. If it is agreed that a click from detector 1 indicates -0‖ and a click from detector 2 indicates -1‖, for example, Alice and Bob get an identical bit string. The DPS-QKD scheme has some advantageous features, including simple configuration, efficient use of the time domain, and robustness against photon number splitting attacks (E. Biham, T.Mor, 1997)(Ekert.A.K 1991)(Inoue.K et al 2002).

We have discussed in this section QKD protocols that use the principle of quantum entanglement. Artur Eckert was the first to propose this idea in his 1991 paper but Brassard and Bennett showed that its principle can be used in the BB84 protocol, many subsequent papers have investigated the use of entangled photons in variants of BB84 protocols.

5. Progress challenges and future perspectives

In the context of experimental or commercial projects, several quantum key distribution networks have been set up, often around BB84 .The DARPA QKD network (Chip Elliott et al 2005), consisting of ten nodes, has been in place since 2004... In 2007, the NIST announced a realization on an optical fiber of 148.7 km (P.A.Hiskett et al 2006). The SECOCQ QKD network (M. Peev et al 2009), was created in 2008 and uses 200 km of standard optical fiber. In 2010 was establishedTokyo QKD (M. Sasaki et al 2011).

In 2015 the distance record for polarized photons transmitted through an optical fiber reached 307 km at 12.7 kbit/s (Boris Korzh et al 2015). In June 2017, the QUESS experiment shows the feasibility of key exchange over longer distances, beyond 1000 km (Juan Yin et al 2017), and with satellites (Sheng-Kai Liao et al 2018).

In 2017, another QKD experiment took place between China's Micius satellite - placed in low Earth orbit - and terrestrial receivers, as reported in a paper in the journal Nature on August 9, 2017. Taking advantage of the vacuum of space, photons carrying quantum information were thus able to travel no less than 1200 kilometers.

In Switzerland, Alberto Boaron managed to transmit a quantum encryption key through 421 kilometers of optical fiber. As stated in an article published on November 3, 2022 in the journal Physical Review Letters (A.Boaron et al 2018), the doctoral student at the Department of Applied Physics (Faculty of Science) thus beats the record of 404 kilometers held for two years by a team from the University of Science and Technology of Hefei in China, while significantly improving the transmission speed.

6. Practical security issues in QKD

The strength of QKD is not the fact that a spy (Eve) is not capable of solving difficult mathematical problems but rather its inability to violate physics (Bruss. D et al 2007). However, the risk of the "man-in-the-middle" attack is always possible, One solution to this attack is a prior mutual authentication between Bob and Alice. In addition, poor quality equipment presents security problems. Finally, the presence of noise in such equipment is also a source of problems. This section examines the security of QKD protocols in practical systems.

6.1 QKD with Noisy Channels - Privacy Amplification

We have already seen that trying to measure or clone photons (the key) by a spy immediately alerts Alice and Bob to the presence of an intruder, (non-cloning theorem) this of course under ideal conditions, however imperfect equipment and the presence of noise in such devices can also lead them to the same conclusion, so how do we tell the difference. Thus Alice and Bob cannot reject all doubtful transmissions, as there will probably always be a natural error not caused by Eve. One solution to this problem is privacy amplification to reduce the information Eve has about the key to an arbitrary level by assuming that Eve was able to learn some of the bits in the key. Alice and Bob must first remove errors from their shared key and then move on to privacy amplification. They will then use an error correction technique to obtain the same key without Eve being able to obtain it. One

technique would be for Alice to randomly choose pairs of bits and send the xor value to Bob (Gisin.N et al 2002). Bob confirms to Alice the similarity of the xor value for these pairs of bits. Thus, they could arrive at the same shared key without revealing the bit values of each compared pair. Once the shared key is identical, Alice and Bob transform their key into a new key without Eve being able to obtain it, unless she also has the same full key. This technique is called 'privacy amplification' and consists of reducing the original key into a new key unknown to Eve. A simple scheme for privacy amplification is for Alice to announce to Bob pairs of bits of the original key (Gisin.N et al 2002). Alice and Bob would then replace these random pairs of bits in the original key with the xor value of each pair to create a new key. Eve will therefore ignore the xor value of a pair of bits even if she is certain of the original two bits, so it is impossible for her to intercept the new key.

6.2 QKD with practical equipment

Photon number splitting attack In practice, many implementations use laser pulses attenuated to a very low level to send the quantum states. These laser pulses contain a very small number of photons, e.g., 0.2 photons per pulse, which are split according to a Poisson distribution. This means that most pulses actually contain no photons (no pulse is sent), some pulses contain 1 photon (which is desired) and a few pulses contain 2 or more photons. If the pulse contains more than 1 photon, Eve can separate the extra photons and transmit the remaining single photon to Bob. This is the basis of the photon number splitting attack (Brassard, Lutkenhaus.N 2000), where Eve stores these extra photons in quantum memory until Bob detects the remaining photon and Alice reveals the coding basis. Eve can then measure her photons in the correct basis and obtain information about the key without introducing detectable errors.

There are several solutions to this problem. The most obvious is to use a real single photon source instead of an attenuated laser. However, since current sources operate at low efficiency and key frequency rates and transmission distances are limited. Another solution is to modify the BB84 protocol, as is done for example in the SARG04 protocol.The most promising solution is decoy states [in which Alice randomly sends some of her laser pulses with a lower average photon count (Lo.H et al 2005). These decoy states can be used to detect a PNS attack, as Eve has no way of telling which pulses are a signal and which are decoys. Using this idea, the secure key rate scales acceptably, the same for a single photon source. In 2004, Gottesman et al published a paper (Gottesman.D et al 2004) describing how the security of BB84-based QKD can be improved against such attacks.

This section examined the security of QKD in the presence of noise and when using imperfect equipment. Privacy amplification was explained to describe how QKD protocols could be secure so that an eavesdropper (Eve) could not record any useful data when errors are detected during measurement. Secondly, the photon number splitting attack, resulting from an imperfect photon source, was also discussed.

7. Conclusion

The principles of quantum mechanics guarantee that no eavesdropper can succeed in measuring the transmitted quantum state without disturbing it in a detectable way. Thus two parties, having access to a quantum and classical unsecured channel, can securely establish a secret key without making assumptions about the capabilities of a spy that might be present. This paper briefly describes the main QKD protocols found in the literature. These include the BB84 protocol and its variants, based on Heisenberg uncertainty. as well as Eckert's approach using quantum entanglement In addition, this paper also provides a brief overview of some of the methods used to achieve practical QKD in the presence of noise and in the face of imperfect equipment. These methods include privacy amplification and detection of SNP attacks.

References

(Gisin.N et al 2002), "Quantum Cryptography", Reviews of Modern Physics, vol. 74, January 2002, pp. 146 – 195 http://www.gap-optique.unige.ch/Publications/Pdf/QC.pdf

(Shor.p 1997), "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.", SIAM Journal of Computing, 26, 1997, pp

(Bruss.D et al 2007)., "Quantum Cryptography: A Survey" ACM Computing Surveys, Vol. 39, No. 2, Article 6, June 2007. http://portal.acm.org/citation.cfm?id=1242474

(Ekert.A. K 1991)"Quantum cryptography based on Bell's theorem", Physical Review Letters, vol. 67, no. 6, 5 August 1991, pp. 661 - 663. http://prola.aps.org/pdf/PRL/v67/i6/p661_1

(Bennett, C. H. and Brassard, G 1984), "Quantum Cryptography: Public key distribution and coin tossing.", International Conference on Computers, Systems &Signal Processing, Bangalore, India, 10-12 December 1984, pp. 175-179. http://www.research.ibm.com/people/b/bennetc/bennettc198469790513.pdf

(Bechmann-Pasquinucci, H,Gisin, N 1999), "Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography." Phys. Rev. A 59, 4238-4248, 1999.http://prola.aps.org/pdf/PRA/v59/i6/p4238_1

(Bruss, D., and Macchiavello, C 2002),"Optimal eavesdropping in cryptography with three-dimensional quantum states." Phys. Rev. Lett. 88, 2002, 127901(11)-127901(4).http://prola.aps.org/pdf/PRL/v88/i12/e127901

(Scarani, A et al 2004), "Quantum cryptography protocols robust against photon number splitting attacks.", Physical Review Letters, vol. 92, 2004. http://www.qci.jst.go.jp/eqis03/program/papers/O26-Scarani.pdf

(Bennet.C et al 1992), D., "Quantum cryptography without Bell's theorem.", Phys. Rev. Lett. 68, 1992, pp. 557-559.http://prola.aps.org/pdf/PRL/v68/i5/p557_1

(Enzer.D et al 2002), "Entangled-photon six-state quantum cryptography.", New Journal of Physics, 2002, pp 45.1-45.8.http://www.iop.org/EJ/article/1367-2630/4/1/345/nj2145.pdf?request-id=OpIrFjGh3BGSdSAC3Ai7Kg

(Fung.C et al 2006), "On the performance of two protocols: SARG04 and BB84.", Phys. Rev., A 73, 012337, 2006. http://arxiv.org/pdf/quant-ph/0510025

(AbhishekParakh, 2015), ―New Protocol for Quantum Public Key Cryptography‖, IEEE ANTS 2015 1570203267 .

(M. A. Nielsen and I. L. Chuang, 2000), ―Quantum Computation and Quantum Information‖, Cambridge, UK: Cambridge University Press.

(E.Biham, T.Mor, 1997) ―Security of quantum cryptography against collective attacks‖, Physical Review Letters 78 (Y11) 2256–2259.

(Inoue.K et al 2002), ―Differential phase shift quantum key distribution‖, Phys. Rev. Lett. 89037902.