International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2018): 7.426

Prominent Security of the Quantum Key Distribution Protocol

Mohit Shukla[1], **Sarvesh Patel**[2]

Department of Computer Science & Engineering, Rama University, Kanpur (U.P), India

Abstract: ***This paper provides an overview of quantum key distribution targeted towards the computer science community. A brief description of the relevant principles from quantum mechanics is provided before surveying the most prominent quantum key distribution protocols present in the literature. In particular this paper describes the BB84 protocol and its many variants as well as Eckert's approach through quantum entanglement. A brief discussion of some of the issues arising in practical implementations are also presented including privacy amplification and the photon number splitting attack.***

Keywords: Quantum Cryptography, Quantum Key Distribution, QKD, survey, BB84, Eckert, Bennet, Brassard, photon number splitting attack, PNS, privacy amplification.

1. Introduction

Classical cryptography can be divided into two major branches; secret or symmetric key cryptography and public key cryptography, which is also known as asymmetric cryptography. Secret key cryptography represents the most traditional form of cryptography in which two parties both encrypt and decrypt their messages using the same shared secret key. While some secret key schemes, such as one-time pads, are perfectly secure against an attacker with arbitrary computational power , they have the major practical disadvantage that before two parties can communicate securely they must somehow establish a secret key. In order to establish a secret key over an insecure channel, key distribution schemes basd on public key cryptography, such as Diffie-Hellman, are typically employed.

In contrast to secret key cryptography, a shared secret key does not need to be established prior to communication in public key cryptography. Instead each party has a private key, which remains secret, and a public key, which they may distribute freely. If one party, say Alice, wants to send a message to another party, Bob, she would encrypt her message with Bob's public key after which only Bob could decrypt the message using his private key. While there is no need for key exchange, the security of public key cryptography algorithms are currently all based on the unproven assumption of the difficulty of certain problems such as integer factorization or the discrete logarithm problem. This means that public key cryptography algorithms are potentially vulnerable to improvements in computational power or the discovery of efficient algorithms to solve their underlying problems. Indeed algorithms have already been proposed to perform both integer factorization and solve the discrete logarithm problem in polynomial time on a quantum computer.

While the advent of a feasible quantum computer would make current public key cryptosystems obsolete and threaten key distribution protocols such as Diffie-Hellman, some of the same principles that empower quantum computers also offer an unconditionally secure solution to the key distribution problem. Moreover, quantum mechanics also provides the ability to detect the presence of an eavesdropper who is attempting to learn the key, which is a new feature in the field of cryptography. Because the research community has been focused primarily on using quantum mechanics to enable secure key distribution, quantum cryptography and quantum key distribution (QKD) are generally synonymous in the literature.

The focus of this paper is to survey the most prominent quantum key distribution protocols and their security from the perspective a computer scientist and not that of a quantum physicist. In order to understand these protocols, however, we briefly describe the necessary principles from quantum mechanics. From these principles the protocols are divided into two categories; those based primarily on the Heisenberg Uncertainty Principle, and those utilizing quantum entanglement. While much of the recent research focus is on developing practical quantum cryptosystems, only a brief discussion of the practical security aspects of these protocols are included in an attempt to remain within the scope of the provided background on quantum mechanics.

2. Fundamentals of Quantum Cryptography

The basic model for QKD protocols involves two parties, referred to as Alice and Bob, wishing to exchange a key both with access to a classical public communication channel and a quantum communication channel. This is shown in figure 1. An eavesdropper, called Eve, is assumed to have access to both channels and no assumptions are made about the resources at her disposal. With this basic model established, we describe in layman's terms the necessary quantum principles needed to understand the QKD protocols.

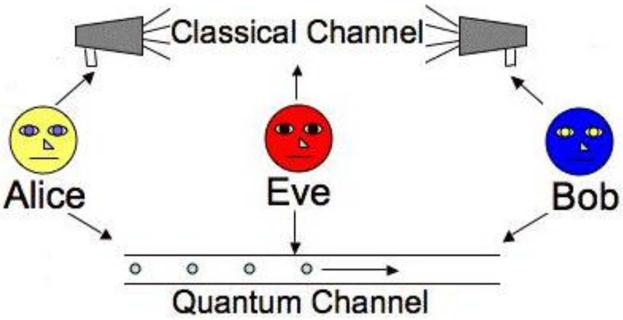


Figure 1: QKD Model

2.1 Heisenberg Uncertainty Principle

As mentioned, the security of quantum cryptography rests on several principles from quantum physics. The most fundamental 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 initially referring to the position and momentum of a particle, described how any conceivable measurement of a particle's position would disturbs its conjugate property, the momentum. It is therefore impossible to simultaneously know both properties with certainty. Quantum cryptography can leverage this principle but generally uses the polarization of photons on different bases as the conjugate properties 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 perform key exchange.

One principle of quantum mechanics, the no cloning theorem, intuitively follows from Heisenberg's Uncertainty Principle. The no cloning theorem, published by Wooters, Zurek, and Dieks in 1982 stated that it is impossible to create identical copies of an arbitrary unknown quantum state.

One could see that without the no cloning theorem, it would be possible to circumvent Heisenberg's uncertainty principle by creating multiple copies of a quantum state and measuring a different conjugate property on each copy. This would allow one to simultaneously know with certainty both conjugate properties of the original quantum particle which would violate HUP.

2.2 Quantum Entanglement

The other important principle on which QKD can be based is the principle of quantum entanglement. It is possible for two particles to become entangled such that when a particular property is measured in one particle, the opposite state will be observed on the entangled particle instantaneously. This is true regardless of the distance between the entangled particles. It is impossible, however, to predict prior to measurement what state will be observed thus it is not possible to communicate via entangled particles without discussing the observations over a classical channel. The process of communicating using entangled states, aided by a classical information channel, is known as quantum teleportation

This section covered the basic key distribution model employed in quantum cryptography. A short overview of the necessary principles from quantum mechanics were also included with an emphasis on the Heisenberg Uncertainty Principle and the principle of quantum entanglement. With this necessary background, the next section describes the QKD protocols based on the first of these key principles.

3. Protocols Utilizing Heisenberg's Uncertainty Principle

In 1984 Charles Bennett and Gilles Brassard published the first QKD protocol [BB84]. It was based on Heisenberg's Uncertainty Principle and is simply known as the BB84 protocol after the authors names and the year in which it was published. It is still one of the most prominent protocols and one could argue that all of the other HUP based protocols are essentially variants of the BB84 idea. The basic idea for all of these protocols then is that Alice can transmit a random secret key to Bob by sending a string of photons where the secret key's bits are encoded in the polarization of the photons. Heisenberg's Uncertainty Principle can be used to guarantee that an Eavesdropper cannot measure these photons and transmit them on to Bob without disturbing the photon's state in a detectable way thus revealing her presence.

3.1 BB84 Protocol

Figure 2 shows how a bit can be encoded in the polarization state of a photon in BB84. We define a binary 0 as a polarization of 0 degrees in the rectilinear bases or 45 degrees in the diagonal bases. Thus a bit can be represented by polarizing the photon in either one of two bases.

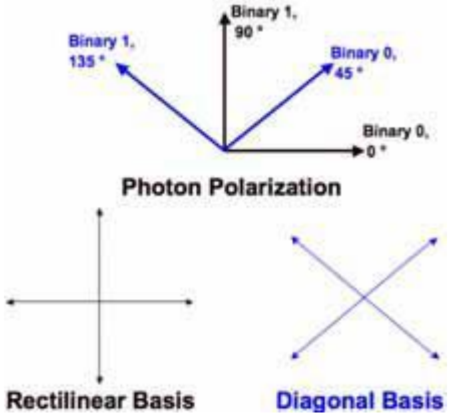
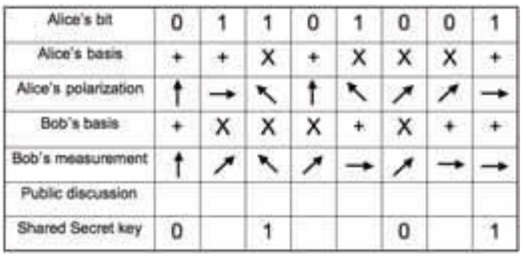


Figure 2: BB84 Bit Encoding

In the first phase, Alice will communicate to Bob over a quantum channel. Alice begins by choosing a random string of bits and for each bit, Alice will randomly choose a basis, rectilinear or diagonal, by which to encode the bit. She will transmit a photon for each bit with the corresponding polarization, as just described, to Bob. For every photon Bob receives, he will measure the photon's polarization by a randomly chosen basis. If, for a particular photon, Bob chose the same basis as Alice, then in principle, Bob should measure the same polarization and thus he can correctly infer the bit that Alice intended to send. If he chose the wrong basis, his result, and thus the bit he reads, will be random.

In the second phase, Bob will notify Alice over any insecure channel what basis he used to measure each photon. Alice will report back to Bob whether he chose the correct basis for each photon. At this point Alice and Bob will discard the bits corresponding to the photons which Bob measured with a different basis. Provided no errors occurred or no one manipulated the photons, Bob and Alice should now both have an identical string of bits which is called a sifted key. The example below shows the bits Alice chose, the bases she encoded them in, the bases Bob used for measurement, and the resulting sifted key after Bob and Alice discarded their bits as just mentioned



Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	+	X	+	X	X	X	+
Alice's polarization	↑	→	↖	↑	↖	↗	↗	→
Bob's basis	+	X	X	X	+	X	+	+
Bob's measurement	↑	↗	↖	↗	→	↗	→	→
Public discussion								
Shared Secret key	0		1			0		1

Figure 3: Sifted Key

Before they are finished however, Alice and Bob agree upon a random subset of the bits to compare to ensure consistency. If the bits agree, they are discarded and the remaining bits form the shared secret key. In the absence of noise or any other measurement error, a disagreement in any of the bits compared would indicate the presence of an eavesdropper on the quantum channel. This is because the eavesdropper, Eve, were attempting to determine the key, she would have no choice but to measure the photons sent by Alice before sending them on to Bob. This is true because the no cloning theorem assures that she cannot replicate a particle of unknown state Since Eve will not know what bases Alice used to encoded the bit until after Alice and Bob discuss their measurements, Eve will be forced to guess. If she measures on the incorrect bases, the Heisenberg Uncertainty Principle ensures that the information encoded on the other bases is now lost. Thus when the photon reaches Bob, his measurement will now be random and he will read a bit incorrectly 50% of the time. Given that Eve will choose the measurement basis incorrectly on average 50% of the time, 25% of Bob's measured bits will differ from Alice If Eve has eavesdropped on all the bits then after n bit comparisons by Alice and Bob, they will reduce the probability that Eve will go undetected to $¾^n$. The chance that an eavesdropper learned the secret is thus negligible if a sufficiently long sequence of the bits are compared.

3.2 B92 Protocol

In 1992, Charles Bennett proposed what is essentially a simplified version of BB84 in his paper, "Quantum cryptography using any two non-orthogonal states" The key difference in B92 is that only two states are necessary rather than the possible 4 polarization states in BB84. As shown in figure 4, 0 can be encoded as 0 degrees in the rectilinear basis and 1 can be encoded by 45 degrees in the diagonal basis Like the BB84, Alice transmits to Bob a string of photons encoded with randomly chosen bits but this time the bits Alice chooses dictates which bases she must use. Bob still randomly chooses a basis by which to measure but if he chooses the wrong basis, he will not measure anything; a condition in quantum mechanics which is known as an erasure. Bob can simply tell Alice after each bit she sends whether or not he measured it correctly.

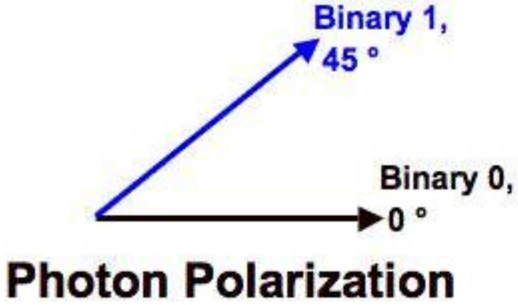


Figure 4: B92 2-State Encoding

Types of Security

There are two types of cryptographic security which will be relevant in this report: computational security and information-theoretic security (also termed unconditional or perfect security.

3.2.1 Computational Security

This describes a crypto-system which is theoretically breakable (by trying every possible key– the brute-force attack) but the computational effort required to do so is so time consuming and expensive that it is not economically viable for an attacker to consider (i.e.*computationally infeasible*).

3.2.2 Information-theoretic Security

This describes cases when, even if an attacker has infinite resources at their disposal, the crypto-system simply cannot be broken. This is clearly much stronger than computational security, but is not necessarily practically achievable. The founding father of Information Theory, Claude Shannon [CS49], proved that unconditional security was possible if the secret key was the same length as the plaintext message to be encrypted. Information Theory has various uses in cryptography: it can be used to prove the unconditional security of systems, determine the achievability of unconditional security within upper and lower bounds, or reduce the task of breaking a crypto-system down to the equivalence of breaking one of its underlying cryptographic primitives (e.g. a one-way function), which may be an altogether easier task. (Maurer [UM99] gives examples of Information-theoretic security in cryptography).

The One Time Pad and the Vernam Cipher

In his proof, Shannon used a special case of symmetric encryption to provide unconditional security: the One Time Pad (OTP), invented in 1926 by Vernam and Mauborgne [GV26]. There are fundamental requirements for using the OTP:
The key is random and non-repeating
The key is as long as the message
The key is used only once and then discarded – never reused

If these conditions are met, then a simple encryption operation (such as a logical XOR) will produce unbreakable ciphertext. Even if an attacker has infinite computing power, they will not be able to derive any information from an intercepted ciphertext.

However appealing they sound in theory, OTPs have immense practical difficulties: generating long, truly random keys is problematic, distributing the keys to recipients is a logistical nightmare, sender and receiver have to be totally synchronized to make sure that the same keys are used for the same message, and ensuring keys are never reused is a challenging task. For this reason, OTPs are currently seldom used in practice, but in later sections of this report, it will be shown that they become a much more attractive prospect when used in conjunction with QKD protocols.

3.3 Kerckhoff's Principle

Cryptosystems are designed to cope with the worst case scenario: a malefactor has infinite computing resources, can gain access to plaintext/ciphertext pairs (and thus could study the relationship between each pair) and knows the encryption and decryption algorithms, so can choose plaintext or ciphertext values at will. The only element not accessible to this adversary is the secret key, and thus the security of a cryptosystem depends solely on the security of the key. This is a long-standing design philosophy first enunciated by Auguste Kerckhoff in 1883: Kerckhoff's Principle *AK83a, AK83b+ states:

"The security of a cryptosystem must not depend on keeping secret the crypto-algorithm. The security depends only on keeping secret the key"

This is sometimes referred to as Shannon's Maxim – 'the enemy knows the system'. It follows, therefore, that keeping key material away from adversaries is a fundamental requirement of any cryptosystem, be it classical or quantum.

3.4 Key Establishment Protocols

The success of cryptographic processing is ultimately dependent on the quality and security of the key material used. This raises the question: where does this key come from? The answer to this lies in some tried and tested key establishment protocols, which are described extensively in standard cryptography texts [AM01 Ch. 12 for example]. The objective of a key establishment protocol is to provide the communicating parties with a shared secret, and this can be done in one of two ways. In the first method, one party generates a key which is securely delivered to the other party via a ***key transport*** protocol. The second method results in a shared secret derived from information passed openly between the two parties, in such a way that no-one (especially an attacker) can guess the resulting value from the information sent. This is a ***key agreement*** protocol.

There are a number of these protocols in existence, but the most widely known is the Diffie Hellman key agreement scheme. This (and others) is described in detail in Appendix 1 . Technically, QKD is actually a key establishment protocol, but as all the reference literature refers to it as a key distribution method, that terminology is retained in this report for consistency.

3.5 Key Distribution

Key establishment protocols work very effectively: indeed, cryptography itself would probably vanish without trace if keys could not be produced successfully. However, there is another problem regarding keys which isn't so well handled – the so-called "quadratic curse". When a symmetric cryptosystem is in place for a network of users, every pair of users who wish to communicate securely will need to pre-share a distinct key. So theoretically, each party in a network of N users will need to hold (N-1) secret keys: the total number of keys in the system is N(N-1)/2 i.e. proportional to N^2. As the number of users on the network gets bigger, this quickly becomes an unworkably large number of keys to deal with effectively. Protocols and network architectures therefore have to be designed to minimize the number of keys wherever possible.

3.6 Other Uncertainty Based Protocols

Another variant of BB84 is the Six-State Protocol (SSP) proposed by Pasquinucci and Gisin in 1999 [SSP99]. SSP is identical to BB84 except, as its name implies, rather than using two or four states, SSP uses six states on three orthogonal bases by which to encode the bits sent. This means that an eavesdropper would have to choose the right basis from among 3 possibilities. This extra choice causes the eavesdropper to produce a higher rate of error thus becoming easier to detect. Brus and Micchiavello proved in 2002 that such higher-dimensional systems offer increased security

While there are a number of other BB84 variants, one of the more recent was proposed in 2004 by Scarani, Acin, Ribordy, and Gisin. The SARG04 protocol shares the exact same first phase as BB84. In the second phase, when Alice and Bob determine for which bits their bases matched, Alice does not directly announce her bases. Rather she announces a pair of non-orthogonal states, one of which she used to encode her bit. If Bob used the correct basis, he will measure the correct state. If he chose incorrectly, he will not measure either of Alice's states and he will not be able to determine the bit. This protocol has a specific advantage when used in practical equipment as will be discussed in Section 5.

BB84 was the first proposed QKD protocol and it was based on Heisenberg's Uncertainty Principle. A whole series of protocols followed which built on the ideas of BB84. Some of the most notable of these were B92, SSP, and Sarg04. The next section describes the alternate approach to QKD which is based on the principle of quantum entanglement.

4. Protocols Utilizing Quantum Entanglement

Artur Eckert contributed a new approach to quantum key distribution where the key is distributed using quantum teleportation. This section describes his protocol and its application to the protocols based on HUP described in the previous section.

4.1 Eckert's Protocol

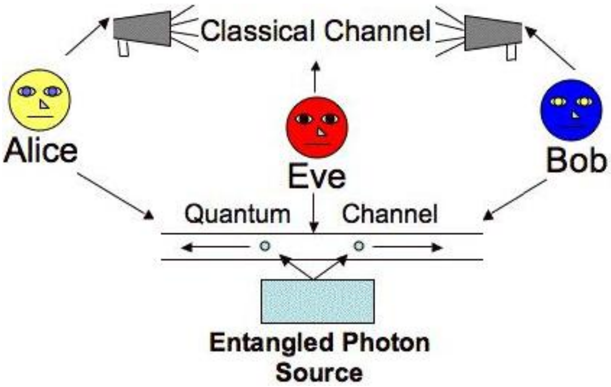


Figure 5: Entangled QKD Model

Eckert describes a channel where there is a single source that emits pairs of entangled particles, which could be polarized photons [Eckert91]. The particles are separated and Alice and Bob each receive one particle from each pair as shown in figure 5. Alice and Bob would each choose a random bases on which to measure their received particles. As in BB84, they would discuss in the clear which bases they used for their measurements. For each measurement where Alice and Bob used the same bases, they should expect opposite results due to the principle of quantum entanglement as described earlier. This means that if Alice and Bob both interpret their measurements as bits as before, they each have a bit string which is the binary complement of the other. Either party could invert their key and they would thus share a secret key.

The presence of an eavesdropper can be detected by examining the photons for which Alice and Bob chose different bases for measurement. Alice and Bob can measure these photons in a third basis and discuss their results. With this information they can test Bell's Inequality which should not hold for entangled particles [Gisin02]. If the inequality does hold, it would indicate that the photons were not truly entangled and thus there may be an eavesdropper present.

4.2 Entangled BB84 Variants

It is important to note the similarity between Eckert's protocol and BB84. If Alice were the source and Alice and Bob did not perform Eckert's entanglement check, we are essentially left with BB84. Bennet and Brassard [BBM92] noted that any variant of BB84 could be adapted to use an entangled photon source instead of Alice being the source. In particular, Enzer et al 2002 [Enzer02] described an entangled version of the SSP protocol with added security. Work has also been done that shows that the SARG04 protocol can tolerate fewer errors with a two-photon source (entangled) than a single-photon source (Alice) [Fung06].

This section described the approach to QKD that utilized the principle of quantum entanglement. Artur Eckert was the first to propose the idea in his 1991 paper but Bennett and Brassard pointed out that his ideas could be incorporated into the BB84 protocol. A series of subsequent papers investigated the use of quauntum entangled photons in the variants of the BB84 protocols.

5. Practical Security Concerns in QKD

QKD is unconditionally secure in the sense that no assumptions are made about Eve's inability to compute hard mathematical problems but rather her inability to violate physics [Bruss07]. Even with this security, however, the QKD protocols are still susceptible to a man-in-the-middle attack where Eve pretends to be Bob to Alice and simultaneously pretends to be Alice to Bob. Such an attack is impossible to prevent under any key distribution protocol without Alice and Bob authenticating each other first. Furthermore it is not immediately obvious whether QKD protocols are perfectly secure when used with imperfect equipment and in the presence of noise. This section examines the security of the QKD protocols in practical systems.

5.1. Security definition

A good definition of security would allow the key generated by a QKD protocol to deviate by a small parameter ε, from a perfect key [2]. This definition should be able to bound Eve’s knowledge about the final key. A perfect key refers to a uniformly distributed bit string whose value is completely independent and remains unknown to an eavesdropper [16]. The main requirement that the definition of security must fulfil is composability [5]. The composable Security of Quantum Key Distribution Protocols http://dx.doi.org/10.5772/intechopen.74234 7 definition characterises the security of a protocol with respect to the ideal functionality. This means that the security of the key generated could be used in any subsequent cryptographic task such as the one-time pad for message encryption, where an ideal key is expected. However, there always exist some challenges in constructing security proofs without making any assumptions either about the devices or the parties. For example, attacks against practical schemes exist, such as photon-number-splitting attacks (PNS) [37], time-shift attacks [38], large pulse attacks [17, 39], blinding attacks [40] and high-power damage attack [41]. Some of the assumptions made in the definition of QKD security are as follows: a. there should be no side channels. Side channels are basically discrepancies between the theoretical model and a practical implementation. They always exist if some information about the raw key is encoded in degrees of freedom not considered in the theoretical model. Therefore, this leads to a wrong assessment of the dimension of the Hilbert space which describes the protocol, b. there should be access to perfect or almost perfect randomness (locally) and c. quantum theory is correct and complete. If there is randomness and quantum theory is correct, then this leads to completion of the security proofs. However, in classical cryptography, the security is based on the difficulty or complication of a certain mathematical algorithm to afford security of the protocol. Therefore, the security is mainly based on the failure to solve the algorithm. This can fail in four ways that are as follows: a. conjecture of hardness/difficulty in this case is wrong, b. underlying computation model could be wrong or could be unphysical, c. the algorithm is easy for many instances and. d. the computation could be small. 5.2. Security requirements In this section, we follow closely the definitions in [5, 42]. A QKD protocol outputs a key SA on Alice’s side and also a key SB on Bob's side. The length of the key is l > 0, otherwise no key is extracted. The length of the key depends on the noise level of the communication channel as well as security and on the correctness requirements of the protocol. Depending on the deviation of the output key from the ideal one, the protocol aborts in which case SA = SB = ⊥ [42]. 1. Correctness: A QKD protocol is called "correct", if, for any strategy by the eavesdropper SA = SB. This occurs whenever Alice and Bob output the classical keys SA and SB, respectively, such that Pr[SA 6¼ SB] ≤ εcor. The term εcor is the maximum probability that the protocol deviates from the behaviour of the correct protocol. In order for correctness to be achieved, the QKD devices must perform what they are supposed to do according to a specified model. The devices generate the correct correlations which they are supposed to output, otherwise the protocol aborts. In other terms, the devices should not send any 8 Advanced Technologies of Quantum Key Distribution other information to the outside world, in which it is not supposed to do (i.e. devices work according to their specification), 2. Secrecy: A random variable S drawn from the set S is said to be ε-secure with respect to an eavesdropper holding a quantum system E, if. min∈σE 1 2 tr|rSE rU ⊗ σE| ≤ ε, (1) where rSE = ∑s∈S Ps (s)|s⟩⟨s| ⊗ rE |S = s is the actual state that contains some correlations between the final key and Eve and ε gives the maximum failure probability of the key extraction process. The state rU = ∑s∈S |s⟩⟨s||S| is the completely mixed state on S and |S| is the size of S. Since the trace distance, that is, 1 2 tr|r0 r1| refers to the maximum probability of distinguishing between the two quantum states (r0 ,r1), this composable security definition naturally gives rise to the operational meaning that the protocol is εsecure, that is, S is identical to an ideal key U except with probability ε [5]. Again, according to Helstrom's Theorem, the probability of distinguishing between the two quantum states r0 and r1 is bounded by 1 2 + 1 4 tr|r0 r1| [43]. 3. Robustness: A QKD protocol is said to be "not robust" if the protocol aborts even though the eavesdropper is inactive. While correctness and secrecy are difficult to prove, robustness can simply be proven by running the protocol. 5.3. Infinite-length key security in QKD Over the last decade, a lot of work in QKD has been devoted to the derivation of unconditional security proofs [8, 16, 44–47]. One of the main problems is that Eve has the power to perform any type of eavesdropping strategy. In particular, she can evade detection by attributing noise caused by her eavesdropping attack to normal noise in the channel. Therefore, it remains difficult to accurately bound the amount of information that Eve may obtain from the communication channel. The most important resource which should be determined when constructing security proofs for QKD protocols is the secret key rate. Therefore, all QKD protocols must be able to provide a clear expression for the secret key rate. In the asymptotic limit, the secret key rate is expressed as r ¼ limn!∞ l n , (2) where l is the length of the final secret key and n is a list of symbols called r raw keys [2]. This rate was established by Devetak and Winter [18]. The secret key rate against collective attacks was derived by Kraus, Gisin and Renner [48] and is expressed as r ¼ I Xð Þ : Y χð Þ X : E (3) where I(X: Y) = H(X) (X|Y) quantifies the amount of bits need to be satisfied for error correction. The term χ(X: E) = H(X) + S(E) S(X, E) refers to the Holevo quantity, where H is Security of Quantum Key Distribution Protocols http://dx.doi.org/10.5772/intechopen.74234 9 the Shannon entropy and S is the von Neumann entropy [49, 50]. The Holevo quantity refers to the amount of privacy amplification required in order to eliminate Eve's information. The upper bound on the secret key rate r, can be expressed as. r ≤ I Að Þ : B↓E , (4) where I(A: B ↓ E) is the intrinsic conditional mutual information (intrinsic information for short) between two information sources held by Alice and Bob after Eve has performed an optimal individual attack [51]. The intrinsic information between two information sources A and B given E ̄is defined as , I(A : B ↓ E) = infE ̄I(A : B|E ̄), where the infimum is taken over all discrete random variables E such that AB ! E ! E ̄is a Markov chain [52]. It has been shown that I(A: B ↓ E) is an upper bound on the rate S = S(A;B||E) at which such a key can be extracted [51]. 5.4. Finite-length key security Many efforts have been made to improve the bounds on the secret key rates for a finite amount of resources [5, 16, 53–58]. Since the tools for analysing the security under non-asymptotic regime have become available, there is need to provide new security definitions. In this section, we follow closely the techniques demonstrated in [16] to discuss some of the parameters used in the security of QKD for finite-length key limit. The main goal of finite-length key security is to obtain a secret key rate r, based on a certain number of signals, a security parameter ε, and certain losses from the error correction without making any assumptions about the post processing (sifting, error correction and privacy amplification). For example, one can recognise that the limit in this expression of Eq. (2) is unrealistic because in all implementations of QKD protocols finite resources are used. This is because in this scenario, N is assumed to be large, that is, it approaches infinity, while in practice Alice and Bob exchange a limited number of symbols or signals. In the non-asymptotic limit, the secret key rate can be expressed as. r ¼ n=N S½ ξð Þ XjE △ leakEC=n : (5) This shows that only a fraction of n out of N signals exchanged contributes to the key. This is because of the fact that m = N n is used for parameter estimation thus leading the presence of a pre-factor of n/N. The expression Sξ (X |E) takes into account the finite precision of the parameter estimation. Eve's information is calculated by using measured parameters, for example, error rates. In the finite-key scenario, these parameters are estimated on samples of finite length. The parameter △ is related to the security of privacy amplification. Its value is given by. △ □ ð Þ 2log d þ 3 √½ log 2 2ð Þ =ε =n þ 2=nlog2 1=εPA, (6) where d is the dimension of the Hilbert space , ε ̄is a smoothing parameter and εPA is the failure probability of the privacy amplification procedure. Eve's uncertainty is quantified by a generalised conditional entropy called the smooth min-entropy and is denoted as Hmin ε ̄ (X(n)| E (N)) [5]. The smoothing parameters , ε ̄and εPA, are parameters which should be optimised 10 Advanced Technologies of Quantum Key Distribution numerically. The square-root term corresponds to the speed of convergence of the smooth-min entropy, which is used to measure the key length of an identical and independently distributed (i.i.d) state toward the von Neumann entropy. In the asymptotic limit, the smooth-min entropy of an i.i.d state is equal to the von Neumann entropy.

5.1 QKD with Noisy Channels - Privacy Amplification

In real systems, if Alice and Bob discover their measurements are not perfectly correlated, it is difficult for them to determine whether the discrepancy was caused by using noisy imperfect equipment or whether there was an eavesdropper present creating perturbations in the state of the photons by measuring them. We have already discussed in sections 3 and 4 how the two approaches to QKD would detect an eavesdropper under ideal conditions. In practical systems, Alice and Bob would not want to discard every transmission that wasn't error free since there likely will always be some natural error not caused by Eve. Since there is some error, we must assume that Eve may have successfully learned some of the key's bits. QKD protocols can employ a technique known as privacy amplification to reduce the information Eve has about the key down to an arbitrary level.

Before applying privacy amplification, Alice and Bob must first remove the errors from their shared key. They can use classical error correction to arrive at the same key without giving the key away to Eve. A simple scheme would involve Alice randomly choosing pairs of bits and sending the xor value to Bob [Gisin02]. Bob would tell Alice whether or not he has the same xor value for those pairs of bits. In this way they could arrive at the same shared key without revealing what the bit values were in each pair they compared.

With Alice and Bob sharing an identical key, they can transform their key into a new key in a way that Eve could not unless she also had exactly the same entire key. This technique is called privacy amplification and involves shrinking the original key to a new key unknowable to Eve. A simple privacy amplification scheme is for Alice to announce to Bob pairs of bits from the original key [Gisin02]. Alice and Bob would then replace these random pairs of bits in the original key with the xor value for each pair to create a new key. Eve cannot know the xor value for a pair of bits with certainty unless she is certain of both original bits, thus she cannot know the new key.

5.2 QKD with Practical Equipment - PNS Attack

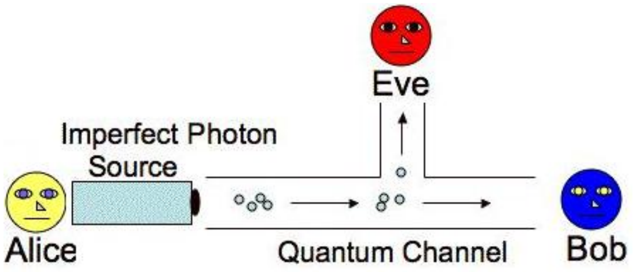


Figure 6: Photon Number Splitting Attack

In addition to noise, it is also currently impractical for equipment to reliably produce and detect single photons. Instead real systems often use a laser producing a small amount of coherent light. Producing multiple photons, however, opens up a new attack known as the photon number splitting (PNS) attack [Brassard00] shown above in figure 6. In PNS, Eve splits off a single photon or a small number of photons from each bit transmission for measurement and allows the rest to pass on to Bob. This would allow Eve to measure her photons without disturbing the photons Bob measures. Lo et al developed a trick to send extra decoy pulses for Alice and Bob to measure allowing them to detect a PNS attack [Lo05]. In addition, the SARG04 protocol is resistant to the PNS because Alice does not directly reveal her bases [Sarg04]. Instead, as described in Section 3, she reveals a pair of non-orthogonal states in which the bit might be encoded. If bob chose the correct bases he will discover that he measured one of these two states that Alice revealed. If not Alice and Bob will drop that bit. This means that Eve does not know which bases to use when measuring her copy of the photon even after Alice and Bob agree on the bases used. This forces Eve to guess which will mean she will not know the bit with certainty. In 2004, Gottesman et al published a paper [Gottesman04] describing how the security of BB84 based QKD protocols hold when using imperfect devices.

This section examined the security of QKD in the presence of noise and when using imperfect equipment. Privacy amplification was introduced to describe how the QKD protocols could be sure Eve maintains no useful information when errors are detected during measurement. The photon number splitting attack, resulting from an imperfect photon source, was also described.

6. Summary

Two parties, given access to an insecure quantum and classical channel, can securely establish a secret key without making any assumptions about the capabilities of an eavesdropper who might be present. This is because the principles of quantum mechanics ensure that no eavesdropper can successfully measure the quantum state being transmitted without disturbing the state in some detectable way. This paper briefly described these underlying principles and provided an overview of the most prominent QKD protocols present in the literature. These included the BB84 protocol and it's variants, which derive their security from Heisenberg's Uncertainty Principle, as well as Eckert's approach using quantum entanglement. In addition, this paper presented a brief introduction to some of the techniques used to achieve practical QKD in the face of noise and imperfect equipment. These included privacy amplficiation and detection of PNS attacks.

References

[1] [CKI-BB84]"The BB84 Quantum Coding Scheme", June 2001. http://www.cki.au.dk/experiment/qrypto/doc/QuCrypt/bb84coding.html
[2] [CKI-BB92]"The B92 Quantum Coding Scheme", June 2001. http://www.cki.au.dk/experiment/qrypto/doc/QuCrypt/b92coding.html
[3] [Lomonaco98] Lomonaco, S., J., "A Quick Glance at Quantum Cryptography", November, 1998. http://xxx.lanl.gov/abs/quant-ph/9811056.
[4] [Wiki-SIFT] Wikipedia-SIFT: http://en.wikipedia.org/wiki/Quantum_cryptography

Papers:

[5] [BB84] Bennett, C. H. and Brassard, G., "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

[6] [Bennet92] Bennett, C., "Quantum cryptography using any two nonorthoganol states.", Phys. Rev. Lett. 68, 1992, pp. 3121-3124. http://prola.aps.org/pdf/PRL/v68/i21/p3121_1

[7] [BBM92] Bennet, C. H., Brassard, G., and Mermin, N., 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

[8] [Brassard00] Brassard, G., Lutkenhaus, N., Mor, T., and Sanders, B., "Security against individual attacks for realistic quantum key distribution. Phys. Rev. A 61, 2000, 052304. http://prola.aps.org/pdf/PRA/v61/i5/e052304

[9] [Enzer02] Enzer, D., Hadley, P., Gughes, R., Peterson, C., Kwiat, P., "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

[10] [Bruss02] Bruss, D., and Macchiavello, C.,"Optimal eavesdropping in cryptography with three-dimensional quantum states." Phys. Rev. Lett. 88, 2002, 127901(1)-127901(4). http://prola.aps.org/pdf/PRL/v88/i12/e127901

[11] [Bruss07] Bruss, D., Erdelyti, G., Meyer, T., Riege, T., Rothe, J., "Quantum Cryptography: A Survey" ACM Computing Surveys, Vol. 39, No. 2, Article 6, June 2007. http://portal.acm.org/citation.cfm?id=1242474

[12] [Eckert91] Ekert, A. K., "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

[13] [Fung06] Fung, C., Tamaki, K., Lo, H., "On the performance of two protocols: SARG04 and BB84.", Phys. Rev., A 73, 012337, 2006. http://arxiv.org/pdf/quant-ph/0510025

[14] [Gisin02] Gisin, N., Ribordy, G., Tittel, W., Zbinden, H., "Quantum Cryptography", Reviews of Modern Physics, vol. 74, January 2002, pp. 146 - 195. http://www.gap-optique.unige.ch/Publications/Pdf/QC.pdf

[15] [Gottesman04] Gottesman, D., Lo, H. Lutkenhaus, N., Preskill, J., "Security of Quantum Key Distribution with Imperfect Devices", ISIT 2004. http://ieeexplore.ieee.org/iel5/9423/29909/01365172.pdf?arnumber=1365172

[16] [Lo05] Lo, H., Ma, X., Chen, K., "Decoy state quantum key distribution.", Phys. Rev. Lett. 94, 230504, 2005. http://arxiv.org/pdf/quant-ph/0411004

[17] [Rieffel00] Rieffel, E., "An introduction to quantum computing for non-physicists.", ACM Computing Surveys, Vol. 32, No. 3, pp. 300-335., September 2000. http://arxiv.org/pdf/quant-ph/9809016

[18] [SSP99] Bechmann-Pasquinucci, H., and Gisin, N., "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

[19] [Sarg04] Scarani, A., Acin, A., Ribordy, G., Gisin, N., "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

[20] [Shor97] Shor, P., "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.", SIAM Journal of Computing, 26, 1997, pp. 1484-1509.

[21] G. Brassard, N. Lutkenhaus, T. Mor, B. Sanders, “Limitations on Practical quantum Cryptography”, Phys. Rev. Lett. 85, p1330-1333, 2000

[22] G. Brassard, ”Brief History of Quantum Cryptography: A Personal Perspective” based on Proceedings of the IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, Japan Oct 2005, arXiv: quant- ph/0604072v1 April 2006

[23] G. Berlın, G. Brassard, F. Bussieres, N. Godbout, J. A. Slater, W. Tittel “Flipping quantum coins” arXiv: quant-ph/0904.3946v2 1 May 2009

[24] Association of German Banks website , June 2010 http://www.german-banks.com/html/19_consumers/consumers_04_2.asp

[25] G. Moore, “Cramming more components onto Integrated Circuits”, Electronics, Volume 38, Number 8, 1965

[26] G. S. Vernam, "Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications", Journal of the IEEE, Vol 55, pp109-115, 1926 http://www.idquantique.com June 2010

[27] http://www.idquantique.com/network-encryption/qkd-security.html, May 2010

[28] http://www.idquantique.com/network-encryption/cerberis-layer2-encryption-and-qkd.html June 2010

[29] J. Bernstein, “Quantum Leaps”, The Belknap Press of Harvard University Press, 2009

[30] J. Bell, “On the Einstein Podolsky Rosen Paradox”, Physics 1, 195-200, 1964

[31] J. L. Carter and M. N. Wegman, “Universal hash functions”, J Comp Syst. Sci 18, 143-154, 1979

[32] J. Cirac, P. Zoller, and H. Briegel, “Quantum Repeaters based on Entanglement Purification”, eprint: arXiv :quant-ph/9808065, 1998

[33] J. L. Duligall, M. S. Godfrey, K. A. Harrison, W. J. Munro, J. G. Rarity, “Low cost and compact quantum key distribution”, New Journal of Physics 8 249, 2006

[34] J. Fenn, M. Raskino, B. Gammage, “Gartner’s Hype Cycle Special Report for 2009” available online http://www.gartner.com/resources/169700/169747/gartners_hype_cycle_special__169747.pdf

[35] J. Kirk, “German Police: Two-factor authentication failing”, Network World, 2009 http://www.networkworld.com/news/2009/032409-german-police-two-factor-authentication.html

[36] J. Kirk, “Nokia: We don’t know why criminals want our old phones”, 2009 http://www.pcworld.com/businesscenter/article/163515/

nokia_we_dont_know_why_criminals_want_our_old_phones.html

[37] J Leyden, "Quantum crypto boffins in successful backdoor sniff", The Register, http://www.theregister.co.uk/2010/05/18/quantum_crypto_attack/ May 2010

[38] J. Manger, "A chosen ciphertext attack on RSA Optimal Asymmetric Encryption Padding (OAEP) as standardized in PKCS #1 v2.0", Advances in Cryptology, Crypto 2001, LNCS 2139, pp. 230-238,Springer-Verlag, 2001

[39] J. Polkinghorne, "Quantum Theory: A Very Short Introduction", Oxford University Press, 2002