A Survey of the Prominent Quantum Key Distribution Protocols

Mart Haitjema, mart.haitjema@wustl.edu

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.

See also: Back to Raj Jain's Home Page

Table of Contents

- 1. Introduction
- 2. Fundamentals of Quantum Cryptography
  - 2.1 Heisenberg Uncertainty Principle
  - 2.2 Quantum Entanglement
- 3. Protocols Utilizing Heisenberg's Uncertainty Principle
  - 3.1 BB84 Protocol
  - 3.2 B92 Protocol
  - 3.3 Other Variants
- 4. Protocols Utilizing Quantum Entanglement
  - 4.1 Eckert's Protocol
  - 4.2 Entangled BB84 Variants
- 5. Practical Security Concerins in QKD
  - 5.1 QKD with Noisy Channels - Privacy Amplification
  - 5.2 QKD with Practical Equipment - PNS Attack
- 6. Summary
- 7. References
- 8. List of Acronyms

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 [Gisin02], 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 [Shor97] [Bruss07].

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 [Bruss07], 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.

The rest of the paper is structured as follows: Section 2 gives a lightweight background on the relevant principles of quantum mechanics. Section 3 describes the approach based on the Heisenberg Uncertainty Principle, in particular the BB84 protocol and its variants. Section 4 focuses on Eckert's approach using

quantum entanglement for secure key distribution. Section 5 discusses the theoretical limitations of quantum cryptography and discusses security in light of practical issues. Finally, we conclude with a summary of the protocols and their security in section 6.

Back to Table of Contents

---

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.

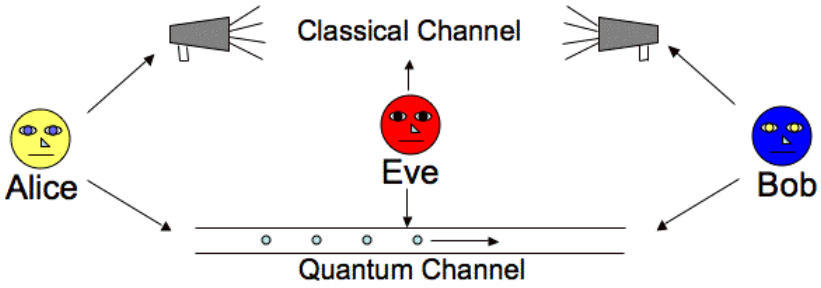

Figure 1: QKD Model

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 [Bruss07] [Wooters82]. 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 and is the basis of Eckert's protocol as will be described in Section 4 [Eckert91] .

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.

Back to Table of Contents

---

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 [CKI-BB84] [Gisin02]. Similarly a binary 1 can be 90 degrees in the rectilinear bases or 135 in diagonal bases.

Thus a bit can be represented by polarizing the photon in either one of two bases.

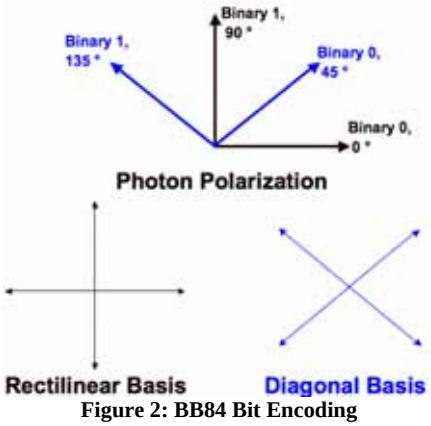

Figure 2: BB84 Bit Encoding

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 [Wiki-SIFT].

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 [Wooters82]. 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 [Rieffel00]. 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 $¾^n$ [Lomonaco98]. 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" [Bennett92]. 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 [CKI-BB92] [Gisin02]. 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 [Bruss07]. Bob can simply tell Alice after each bit she sends whether or not he measured it correctly.

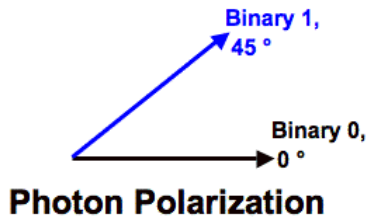

Figure 4: B92 2-State Encoding

3.3 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 [Bruss02].

While there are a number of other BB84 variants, one of the more recent was proposed in 2004 by Scarani, Acin, Ribordy, and Gisin [Sarg04]. 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.

Back to Table of Contents

---

4. Protocols Utilizing Quantum Entanglement

Artur Eckert contributed a new approach to quantum key distribution where the key is distributed using quantum teleportation [Eckert91]. This section describes his protocol and its application to the protocols based on HUP described in the previous section.

4.1 Eckert's Protocol

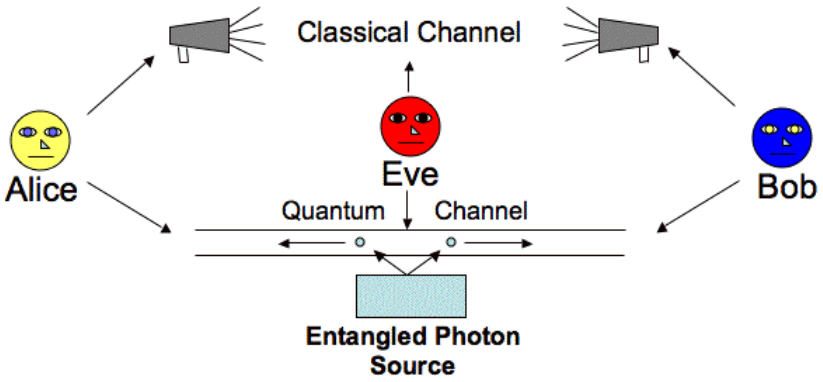

Figure 5: Entangled QKD Model

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.

Back to Table of Contents

---

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 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

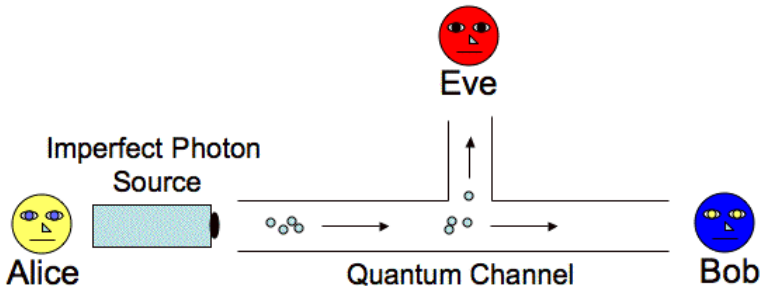

Figure 6: Photon Number Splitting Attack

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.

Back to Table of Contents

---

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.

Back to Table of Contents

---

7. References

URLs:

[CKI-BB84]"The BB84 Quantum Coding Scheme", June 2001. http://www.cki.au.dk/experiment/qrypto/doc/QuCrypt/bb84coding.html

[CKI-BB92]"The B92 Quantum Coding Scheme", June 2001. http://www.cki.au.dk/experiment/qrypto/doc/QuCrypt/b92coding.html

[Lomonaco98] Lomonaco, S., J., "A Quick Glance at Quantum Cryptography", November, 1998. http://xxx.lanl.gov/abs/quant-ph/9811056.

[Wiki-SIFT] Wikipedia-SIFT: http://en.wikipedia.org/wiki/Quantum_cryptography

Papers:

[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

[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

[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

[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

[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

[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

[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

[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

[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

[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

[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

[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

[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

[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

[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

[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.

http://citeseer.ist.psu.edu/cache/papers/cs/5140/http:zSzzSzwww.neci.nj.nec.comzSzhomepageszSzwdszSzshorfactor.pdf/polynomial-time-algorithms-for.pdf

[Wooters82] Wooters, W., Zurek, W., "A single quantum cannot be cloned." Nature 299, 1982, pp. 802-803.
http://www.nature.com/nature/journal/v299/n5886/abs/299802a0.html

Back to Table of Contents

8.Acronymns

Alice - The party transmitting a secret key
BB84 - Bennet and Brassard 1984 protocol
B92 - Bennet's 2-state protocol proposed in 1992
Bob - The party receiving a secret key (from Alice)
Eve - A hypothetical eavesdropper
HUP - Heisenberg Uncertainty Principle
PNS - Photon Number Splitting QKD - Quantum Key Distribution
Sarg04 - Protocol proposed by Scarani, Acin, Ribordy, and Gisin in 2004
SSP - Six-State Protocol

Back to Table of Contents

Last Modified December 2, 2007

Note: This paper is available on-line at http://www.cse.wustl.edu/~jain/cse571-07/index.html