Quantum Key Distribution: A Resource Letter

Srinivasan Arunachalam
National Institute of Technology
Karnataka, India

ABSTRACT

Quantum key distribution (QKD) is one of the best-known examples of an application of quantum mechanics to cryptography. This article serves as a resource letter, a brief description to the introduction of QKD is provided before surveying the most prominent QKD protocols present in the literature from theoretical initialization by Wiesner to the attempts at practical implementations. We have also given an overview of the different security proofs proposed, for the variations in protocols and highlighted their significance.

Keywords

Quantum Key Distribution, BB84, Quantum Cryptography, Security, Implementation

1. INTRODUCTION

The confidentiality input independent key establishment and unconditional security provided by QKD for secure communication between two parties offering a much stronger security, is what differentiates QKD from classical communication schemes. The advent of Quantum Cryptography in the 1980's has gained widespread interest since then mainly due to the fact that it guaranteed *'*unconditional security*'*. Quantum Cryptography took advantage of the Heisenberg's Uncertainty Rule, which stated that a measurement performed on a quantum state would disturb it and provide partial information about the state. Thus any eavesdropper in the communication channel is bound to create some noise in the channel trying to break in, thus leading to easy detection of intrusion by the communication parties. The article [52] by Gisin et al. covers all aspects of Quantum Cryptography. QKD in specific is a technology, based on the quantum laws of physics. It aims at the creation of a secret key between authorized partners connected by a
quantum and a classical authenticated channel. The security of the key can in principle is guaranteed without putting restrictions on the eavesdropper's power.

1.1 Bibliography of Protocols

1. Quantum Cryptography was born in early 1970's when Wiesner wrote *'*Conjugate Coding*'*, unfortunately this highly innovative paper was unpublished at the time and went mostly unnoticed for over 10 years before it appeared in [1]. Wiesner explained how quantum physics could be used in principle to produce bank notes (what is now known as Quantum money) that would be impracticable to counterfeit and how to put into practice what he called a multiplexing channel a concept markedly comparable to what Rabin was to put forward more than ten years afterward under the name of *'oblivious transfer'* in [2].
2. The concept however gained prominence in 1984 when Charles H.Bennett and Gilles Brassard proposed the BB84 protocol which implemented photon polarization using 2 pairs of conjugate or orthogonal states to transmit the information between two users [3], the protocol being explained later. The security relied on the no-cloning theorem and that information gained by Eve would be at the expense of introducing disturbance or noise to the communication channel, if the two states we are trying to distinguish are not orthogonal, which would be detected by Alice and Bob.
3. In 1990, independently and initially unaware of the previous work, Artur Ekert developed a dissimilar approach to QKD based on quantum entanglement called the E91 protocol [4], where the EPR(Einstein-Podolsky-Rosen) entangled pairs were used for transmission; based on the Bohm's version of the EPR experiment and Bell's theorem employed to check for eavesdropping. The improvement of using entangled states is that the key can remain secure even in storage and not only in transmission, by the uncertainty principal.
4. Intuitively, a variation later was proposed by Bennett in [5] to use only two non-orthogonal states rather than four states as mentioned in [3]. As in BB84, the physical nature of these states was unimportant. Bennett suggested using a dim pulse of coherent light with some phase difference relative to a bright reference pulse instead, which came soon after the practical realization of Quantum cryptography for the first time in [29].
5. Another variant is the Six-State Protocol (SSP) proposed at first in [6]by Bruss and Ginsin and later by Pasquinucci and Gisin in 1999 [8]. SSP uses six states on three orthogonal bases to encode the bits sent; hence an eavesdropper would have to choose the correct basis from among 3 possibilities. The extra choices cause higher error rate and easier detection of intrusion by any eavesdropper. Brus and Micchiavello proved later [7] that such a higher-dimensional system offer amplified security for communication and resulted in easier detection of interference by any eavesdropper.
6. There are numerous variations to the initial BB84 protocol. We shall mention a few here and further reading could be done on [51]. First variation in [9] consists of assigning significantly dissimilar probabilities for different polarization bases during transmission and reception. It was proposed that as the quantity of transmitted signals increases, the efficiency of the proposed scheme can be made to approach 100%.The attacks however in this paper are limited to a biased eavesdropping attack under the assumption that in the near future single-photon measurement attacks by Eve will be the only pragmatic class of attacks.

7. Another variation was presented by Goldenberg and Vaidman in [12]. They suggested preparing the qubits in a superposition of 2 spatially separated states, then sending one component of this superposition and waiting until Bob receives it before sending the second component. They presented a variation also wherein the trend of using non-orthogonal states is removed and present a cryptographic scheme based on orthogonal states, which also assures the detection of any eavesdropper.

8. Inoue K., et al. proposed the novel scheme in [13] wherein a single photon is prepared in a linear superposition state of 3 basis. This protocol is suitable for fiber transmission systems and offers key creation efficiency higher than conventional fiber-based BB84. The features of this scheme are that no photon is discarded during transmission and the protocol exhibits robustness against PNS attack.

9. The protocol proposed by Scarani A. et al. in [10] that differs from the BB84 only in the classical sifting procedure, where Alice reveals a pair of non-orthogonal states instead of revealing the basis. The increased security compared to the other protocols presented earlier for QKD schemes using weak laser pulses has been discussed in the paper. They have gone on to show that this protocol is better than BB84 against PNS attacks at zero error.

10. A new protocol for practical quantum cryptography, presented in [11] by Gisin et al., tailored for an implementation with coherent pulses which are weak. This protocol performs as well as standard protocols with strong reference pulses against zero-error attacks: only as the transmission of the quantum channel the key rate decreases. Few issues not handled in this paper are Trojan-horse and similar realistic attacks, with the assumption of Eve not changing Bob's detection rates in the data channel and in the monitoring line.

1.2 BB84 Protocol

We have given a brief overview of a simple BB84 protocol below for a clear picture adopted from [45].

1. Alice chooses two random $(4 + \epsilon)$n bit strings *a* and *b*.

2. She encodes the bit string *a* in $(4 + \epsilon)$ n qubits this way:

(a) If the corresponding bit in *b* is 0, then she encodes *f*0, 1*g* as *{*|0> , |1>}.

(b) If the corresponding bit in *b* is 1, then she encodes *f*0, 1*g* as {|+>, |->*}*

3. Alice then sends the qubits to Bob.

4. Bob then measures the qubits in random bases, but keeps track of them.

5. Then Alice publicly announces *b*, i.e. her choice of bases.

6. Bob then matches *b* with his measurement bases. He discards the qubits for which the bases disagree.

7. Now Bob has roughly 2*n* qubits.

8. Now Alice selects a subset of these qubits to serve as check bits against the noise and interference of any possible eavesdropper Eve.

9. If more than a specific number of those check bits differ, then they abort the transmission and starts again.

10. If the check passes, then they can place an upper bound on the total number of errors in the remaining *n* qubits.

11. Then they use error correcting codes to obtain *m* flawless shared bits where $m < n$.

2. SECURITY OF QKD SCHEMES

2.1 Security Definition

QKD is often mentioned to provide *'unconditional security'* to emphasis on difference in security it provides compared to other classical protocols which have shown to be computationally secured. Unconditional security often refers to the property of an ideal cryptosystem, as defined by Shannon (1949). The term perfect secrecy and unconditional secure was used synonymously by him. Mathematically, this is expressed as

$$H(M) = H(M|C)$$

where $H(M)$ is the plaintext entropy and $H(M|C)$ is the conditional plaintext entropy of the cipher text C. Unconditional security is independent of computational power of the attacker (as opposed to computational security) and must be secure against any attack permitted by laws of Quantum Mechanics. A composable definition of security for Quantum Cryptography was presented in [46]. Perfect Security: We can say that a QKD Scheme is perfectly secure if following holds under any adversary.

Correctness: The outputs of the protocol on Alice and Bob's side are similar.

Secrecy: If the protocol produces a key, then it should be uniformly distributed and independent of the state of the system held by the adversary.

Robustness: If the adversary is non-responsive then a key is generated.

Security of QKD hence depends on the factors of secure authentication and device-independent communication between the users. With the above considerations there have been numerous proofs of security present in literature. We shall present a few of them and highlight their significance.

2.2 Security Proofs

1. Slutsky et al. in [14] showed the security of BB84 and B92 protocols where the analysis is limited to eavesdropping strategies with each bit of the quantum transmission being attacked individually and independently from other bits. They analyzed the trade-off between the disturbance/induced error-rate and the maximum information the eavesdropper could gain for both the 2-state and 4-state protocol and found an optimal eavesdropping attack.

2. A major issue involving the long distance aspects of QKD ie. the communication over long distances to maintain the unconditional security aspect of QKD was dealt with in the paper by Lo and Chau In [19]. They attempt resolving this problem use of fault tolerant computers [49] and quantum repeaters [43]. They have used the quantum to classical reduction and using classical probabilistic argument to prove the security of BB84 for long distance communication assuming the eavesdropper has complete control of the quantum repeaters and communication channel. They make the nontrivial observation that their security proof can be

combined and applied to QKD to distinguish noise from a malicious Eve in any communication channel.

3. Shor and Preskill in [15] proposed a QKD protocol dependent on entanglement purification using Calderbank-Shor-Steane (CSS) codes and proved the security of BB84 protocol using Lo and Chau's proof of security. They carry on showing the security of this protocol implies the security of BB84. The only drawback in this paper was that it doesn't take care of imperfect sources and also the security of QKD using weak coherent sources hasn't been discussed. A proof avoiding this difficulty was presented by Michael Ben-Or showing that any source sufficiently close to a single-photon source will still be secure.

4. Norbert Lutkenhaus in [18] proved the security of QKD against individual attacks for realistic signals sources, including weak coherent pulses, down conversion sources and obtained a formula for the secure bit rate per time slot of an experimental setup, not mentioned in [15]. It also takes into account the non-ideal signal sources and detectors. The limitations of this paper being that attacks were limited to individual attacks have been addressed in other papers.

5. Mayers in [23] proves unconditional security of QKD schemes by concentrating on the problem of noisy channel with photons being lost during transmission. No restriction is imposed on the detector/receiving side of the communication channel. The Shor-Preskill proof is weaker than the result here because their proof requires the assumption that Bob's measuring apparatus is perfect (or closes to perfect eventually). This assumption certainly helps to simplify the proofs for security, but it's a step backward with respect to the ultimate objective, which is to trust only restricted and simple properties of the apparatus used and place no restrictions on them. The problem of non-trusted source is addressed in [24] and [25].

6. Security of quantum key distribution involving qudits has been discussed in [41]. In the paper they have analyzed 2 cryptosystems, the initial cryptosystem uses two mutually unbiased bases (thereby extending the BB84 scheme), and while the other exploits all the $d + 1$ available such bases (extending the six-state protocol for qubits). They have derived a very straightforward security proof of quantum cryptography with qudits that exploits an intuitive information inequality constraining the simultaneous measurement of conjugate observables resulting in an upper bound on the acceptable error rate.

7. Gottesmann and Lo in [21] contrast proofs of security of QKD schemes, BB84 and the six-state scheme, against general attack, by using the techniques of two-way entanglement purification. They conclude that six state scheme can tolerate a higher bit error rate. The most general paper by Acin,Pirano, et al. [22] where they have found the optimal collective attack on a QKD protocol in the device-independent scenario, in which no further assumptions are made than the validity of quantum physics. The general QKD schemes are proven secure against eavesdropping action if quantum mechanics is correct. A theoretical discussion is made in [28] of the effects on QKD if the quantum regime were ever to fail. They describe a key distribution scheme provably protected against general attacks by a post-quantum eavesdropper who is restricted only by the impossibility of superluminal signaling and security stemming from violation of Bell inequality.

8. The design of key-reusability after a joint attack was highlighted in the paper by Ben-Or et al. in [20], providing security definition of QKD using the concept of Universal Composability. They provide a new privacy condition which is composable and sufficient for security. Firstly they derive a composable security definition for QKD and go on to show that the key produced in a QKD run which is unconditionally secure can be reused but degrade slowly with repeated runs.

9. In 2004, Gottesmann,Preskill et al. in [17] proposed the security of BB84 QKD scheme where the adversary had limited control over the source-detector by having knowledge of the basis used by Alice and Bob. They give a lower bound on the asymptotic key generation rate depending on the minute basis-dependant flaws in the source detectors. They nevertheless do not discuss how to improve the rate of key generation beyond the rate given in the paper through privacy amplification schemes using two-way communication. Finally, the security analysis applies to the asymptotic limit of an infinite key – and has not been analyzed for the practical aspects of error correction and privacy amplification in the case of finite key length.

10. Renato Renner in his Thesis [16] on Security of QKD proposed the Post Selection Technique and using DeFinetti Theorem proved the security of QKD scheme. The basic idea is that using the DeFinetti theorem, proving the security of THE Hilbert Schmidt State implies security against collective attacks and Post Selection guarantees that any scheme is secure against general attacks will be secure against collective attacks, with necessary conditions like channels being permutation invariant.

11. The article [50] provides a general security proof for a large class of protocols in a model in which the raw key is generated by independent measurements. They also showed how to compute a bound on the key rate of a large class of Device Independent QKD protocols. The DIQKD model considered here represents a relaxation of standard QKD, and thus can only be more secure.

3. IMPLEMENTATION OF QKD

Since that first prototype was constructed in 1989, other developments have followed at such places as the Los Alamos National Laboratory in New Mexico, the UK Defense Evaluation and Research Agency, and at the University of Geneva at Switzerland. These institutions have worked to push the limits of quantum transmission both through the atmosphere via satellite connections and through fiber optical cables. Few successful implementations have been mentioned below.

1. Quantum Cryptography came into the experimental forefront in 1989 [29] when the first experimental quantum exchange (quantum channel being 32 cm of free air) was conducted by Bennett and Brassard. A LED generated light pulses that were subsequently attenuated by an interference filter and polarized by a polarizer. The qubits were encoded in the polarization of photons by means of Pockels cells.

2. In [31] polarized photons is used to code the key. The photons remain guided from the semiconductor laser diode until the photon counter module. The feasibility of establishing a key over more than 1 km by this method was experimentally demonstrated. [33] contains a setup using only two non-orthogonal polarization states and polarizes instead of analyzers were proposed.

3. British Telecom in 1993 showed in [32] with high visibility (v=0.985) single photon fringe measurements in a 10 km long, optical fiber-based, time- and polarization-division Mach-Zehnder interferometer were reported, where the system's ability to transmit key data was assessed.

4. Longer distance over 48km of QKD was achieved [34] where it was demonstrated that quantum key distribution with useful key rates is feasible over extended distances of installed optical fiber in a real world environment. In this article, key material is built up using the transmission of a single-photon per bit of an initial secret random sequence.

5. A detailed analysis of QKD scheme employing entangled states is presented in [37]. They had implemented an asymmetrical Franson type experiment for photons entangled in energy-time and use a key distribution protocol analogous to BB84. With Alice and Bob directly connected, a sifted bit sequence of 1.7 Mbits was distributed at a raw rate of 450 Hz, and exhibited a QBER of 5.9 %. With an 8.45 km-long fiber between them, we distributed a sequence of 0.41 Mbits at a raw rate of 134 Hz, and with an error rate of 8.6 %.

6. Jennewein, Simon et al. for the first time in[48] show the full scale implementation of quantum cryptography system based on polarization entangled photon pairs(a variant to the BB84 protocol) where they establish highly secure keys. The proposed system had two completely independent users separated by 360 m, and generated raw keys at rates of 400 - 800 bits/second with bit error rates around 3%.

7. Martin Hendrych in his Thesis [36] experimentally investigated the phenomenon of quantum interference and non-local correlations involved in the practical applications of quantum cryptography like QKD, quantum secret sharing and quantum identification. The quantum key distribution experiment was based on interference of weak coherent states in a time-multiplexing interferometer. An extended and experimentally shown, 0.5 km long, optical-fiber-based interferometer was built with visibility reaching 99.6%.

8. The first demonstration of QKD in [38] reports over a standard telecom fiber exceeding 100 km in length. They achieved a quantum bit error ratio of 8.9% for a 122km link, allowing a secure shared key to be formed after error correction and privacy amplification. The dominant contributions to the QBER were recognized as arising from phase modulation errors, false counts due to stray clock laser photons in addition to detector dark counts.

9. In [35] they have distributed entangled photons directly through the atmosphere to a receiver station 7.8 km away over the city of Vienna, Austria at night. The polarization correlations contained in the measured time tags were sufficient to convincingly infringe a CHSH-Bell inequality. Results show that high-fidelity transfer of entangled photons is possible under these real-world conditions.

10. The distance and secure key generation rate was improved in [30] by employing decoy photons. It was shown that with rather uncomplicated modifications (by adding commercial acousto-optic modulators, AOM) to a commercial QKD system, a secure key generation rate of 165bit/s, which is 1/4 of the theoretical limit, could be obtained over 15km of a Telecom fiber. In this regard, [42] also proposes a decoy state method to overcome the PNS attack for BB84 QKD protocol in the presence of high loss in the practical case of coherent pulses sources.

11. The use of low-noise detectors could both be used to increase the secret bit key rate of long-distance QKD and dramatically extend the length of a fiber optic link over for secure key could be distributed was demonstrated in [40]. They demonstrated the production of secret key at distance separation of 184.6 km and this also surpassed by several km the maximum PNS-secure transmission distance inferred in the previous "decoy state" protocol implementation with conventional detectors.

12. A major challenge was to achieve a QKD system with a 40 dB channel loss, which is required if we are to realize global scale QKD networks using communication satellites [39] They report the first QKD experiment in which secure keys were distributed over 42 dB channel loss and 200 km of optical fiber employing the differential phase shift quantum key distribution. They achieved a 17 kbit/s secure key rate at 105 km, which is two orders of magnitude larger than the previous record. The error threshold for a 200 km transmission using SSPDs with 1.4% quantum efficiency is the longest transmission achieved through QKD till date.

13. The papers [27] and [26] present a complete protocol for BB84 QKD. The former talks about the issue of perfect single photon sources not being available and, therefore, practical implementations using either dim laser pulses or post-selected states from parametric down conversion. The latter provides security including practical implementation for a realistic setting taking into consideration (noise, loss, multi photon signals of the source) that covers many of today's experimental implementations. Both of them also prove the security of the proposed protocols in their respective settings.

4. LIMITATIONS

Authentication: 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 . Even with this security, however, the QKD protocols are still vulnerable to a man-in-the-middle attack where Eve impersonates 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. Hence Authentication either Symmetric-key, Public -Key or using Trusted Third party is an integral part of secure QKD.

Affordable Technology: Although security proofs exist for the theoretical BB84 protocol, no engineering representation exists for it. Such engineering models would be necessary to determine when an implementation's parameters stray too far from the theoretic and are no longer covered by the security proofs. Without solutions to these limitations, QKD may not be a viable alternative security technology and may be limited to niche markets. The precincts of QKD are that it's currently a costly technology and requires dedicated hardware; it's still in its infancy. Engineering shrinks and mass production could make the hardware small and more affordable, while future research may solve many of the current limitations.

Key Rate and Distance: The fundamental limitations that come along with QKD are key generation rate and distance of communication channel. The different key rates achieved in the implementations have been discussed in the previous section. Basically smaller distances guarantee more secure and secret keys. The longer the quantum channel the more photons are going to be lost to decoherence which leads to a lesser secure and secret key formation. The maximum guaranteed transmission distance between remote parties for QKD is about 200 km. Because optical fibers are not absolutely transparent, a photon will at times get absorbed and therefore not reach the end of a fiber. While this distance restraint may be suitable for business and academic campuses, it is not practical for deployment on a global level.

Alternatives and Solutions: Continued research and development in the areas of "quantum repeaters" is essential to increase transmission distances. Quantum repeaters [43],[43] would prevail over the distance limitation, allowing shared quantum states to be established between distant parties. An alternative proposed is the use of low-orbit satellites which can serve as intermediates stations, the advantage also being photons are less attenuated in the atmosphere. Secondly, quantum key distribution is not the weakest link in a security system. What malicious attackers cannot break directly, they simply bypass and identify easier means of attack, such as social engineering, weak passwords, or poorly implemented security policies. Since the solutions available in the marketplace today for key distribution are "good enough" for most companies, many business executives may feel that there is no significant business driver for a company to implement QKD Technology. Various factors like which are part of limitations to QKD implementation have been discussed in [47] and necessary conditions for secure QKD using current experimental implementations are shown.

5. CONCLUSIONS

Quantum Cryptography is the first application of quantum mechanics at the single quanta level. It might still be in its infancy and the technological advances so far look very promising. In this survey we have gone through most of the protocols from the birth of Quantum Cryptography by Wiesner, different security proofs and models and the implementations of QKD. The security of any QKD system depends on no computational assumptions and has potential to offer security against any form of attackers with infinite computational power or "*unconditional security*". Considering the potential of QKD and the effect it will have if implemented successfully, research in this field still goes on. [53] argues that QKD will be an vital part of future cryptography and although there are few issues to be handled QKD overall still has to offer stronger security than classical key agreement This technology has the potential to make a valuable contribution to ecommerce and business security, personal security, and security among government organizations. The current commercial systems are aimed mainly at governments and corporations with high security requirements. Many experiments have demonstrated that keys can be exchanged over distances of a few tens of kilometers at rates at least of the order of a thousand bits per second. There is no doubt that with time and ongoing research, the technology can be mastered and will find commercial applications. If Quantum cryptography turns out to eventually meet even some of its expectations, it will have a profound and revolutionary affect on all of our lives.

6. REFERENCES

[1] S.J. Wiesner; "Conjugate Coding" ; SIGACT News 15:1; 1983. pp. 78-88

[2] Michael O. Rabin; "How To Exchange Secrets with Oblivious Transfer"; Harvard University Technical Report 81

[3] C. H. Bennett and G. Brassard; "Quantum Cryptography: Public key distribution and coin tossing"; in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore; 1984 pp.175

[4] Ekert A.K.; "Quantum Cryptography based on Bell's Theorem"; Physical Review Letters, vol.67, no.6, 1991 pp. 661-663

[5] Bennett C.H.; "Quantum cryptography using any two nonorthogonal states" ; Physical Review Letters, vol. 68, no. 21, 1992, pp. 3121 - 2124.

[6] N. Gisin, talk presented at the Workshop on Quantum Computation, Torino,D. Bruss, Phys. Rev. Lett. 81, 3018, 1998.

[7] Bruss.D, Macchiavello.C; "Optimal eavesdropping in cryptography with three-dimensional quantum states"; Phys. Rev. Lett. 88, 127901 (2002)

[8] 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.

[9] Mohammed Ardehali, Gilles Brassardt , H. F. Chaut , Hoi-Kwong Lo; "Efficient Quantum Key Distribution" ; Manuscript, 1992.

[10] Scarani A., Acin, A., Ribordy, G., Gisin, N.; "Quantum cryptography protocols robust against photon number splitting attacks."; Physical Review Letters, vol. 92, 2004

[11] Nicolas Gisin, Gregoire Ribordy, Hugo Zbinden, Damien Stucki, Nicolas Brunner, Valerio Scarani; "Towards practical and fast Quantum Cryptography"; arXiv:quant-ph/0411022v1

[12] Lior Goldenberg and Lev Vaidman; "Quantum Cryptography Based on Orthogonal States" ; Phys.Rev.Lett.75:1239-1243,1995

[13] Kyo Inoue,H. Takesue, T. Honjo; "Differential-Phase-Shift Quantum Key Distribution"; Amer. Math. Monthly 110 (2003) 435-437

[14] Boris A. Slutsky, Ramesh Rao, Pang-Chen Sun, and Y. Fainman; "Security of quantum cryptography against individual attacks"; Phys. Rev. A 57, 2383-2398 (1998)

[15] Shor P. , Preskill J.; "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol"; Phys.Rev.Lett.85:441-444,2000

[16] Renato Renner; "Security of Quantum Key Distribution"; arXiv:quant-ph/0512258v2

[17] Daniel Gottesman, Hoi-Kwong Lo, Norbert Ltkenhaus, John Preskill; "Security of quantum key distribution with imperfect devices" ; Quant.Inf.Comput. 5 (2004) 325-360

[18] Norbert Ltkenhaus "Security against individual attacks for realistic quantum key distribution"; Physical Review A, Vol. 61, 052304(2000);

[19] Hoi-Kwong Lo, H. F. Chau; "Unconditional Security Of Quantum Key Distribution Over Arbitrarily Long Distances"; Science 283 (1999) 2050-2056

[20] M. Ben-Or, Michal Horodecki, D. W. Leung, D. Mayers, J. Oppenheim; "The Universal Composable Security of Quantum Key Distribution"; Theory of Cryptography: Second Theory of Cryptography Conference, TCC 2005, J.Kilian (ed.) Springer Verlag 2005, vol. 3378 of Lecture Notes in Computer Science, pp. 386-406

[21] Daniel Gottesman , Hoi-Kwong Lo; "Proof of security of quantum key distribution with two-way classical communications"; IEEE Transactions on Information Theory, Vol. 49, No. 2, p. 457 (2003).

[22] Stefano Pironio, Antonio Acin, Nicolas Brunner, Nicolas Gisin, Serge Massar, Valerio Scarani; "Device-independent security of quantum cryptography against collective attacks"; New J. Phys. 11, 045021 (2009).

[23] Mayers, D.; "Unconditional security in Quantum Cryptography"; JACM, vol 48, no 3, May 2001, p 351-406.

[24] Mayers D., and Yao A.; "Quantum cryptography with imperfect apparatus"; In Proceedings of the 39th IEEE Conference on Foundations of Computer Science. IEEE Computer Society Press.

[25] Mayers, D.; "Self-Checking Quantum Apparatus and Violation of Classical Locality"; Manuscript

[26] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Du, Norbert Lutkenhaus, Momtchil Peev; "The Security of Practical Quantum Key Distribution"; Rev. Mod. Phys. 81, 1301 (2009)

[27] Hitoshi Inamori, Norbert Ltkenhaus, Dominic Mayers; "Unconditional Security of Practical Quantum Key Distribution"; European Physical Journal D, Vol 41, p.599 (2007)

[28] Jonathan Barrett, Lucien Hardy , Adrian Kent; "No Signalling and Quantum Key Distribution"; Phys. Rev. Lett. 95, 010503 (2005)

[29] Bennett, C. H. and Brassard, G.; "The dawn of a new era for quantum cryptography: The experimental prototype is working!"; Sigact News, vol. 20, no. 4, 1989, pp. 78 – 82

[30] Yi Zhao, Bing Qi, Xiongfeng Ma, Hoi-Kwong Lo, Li Qian; "Experimental Quantum Key Distribution with Decoy States"; Physical Review Letters 96, 070502 (2006).

[31] A. Muller, J. Breguet and N. Gisin; "Experimental Demonstration of Quantum Cryptography Using Polarized Photons in Optical Fibre over More than 1km"; Europhysics Letters Volume 23 Number 6, 1993 .

[32] Townsend, P. D., Rarity, J. G. and Tapster, P. R; Enhanced single photon fringe visibility in a 10 km-long prototype quantum cryptography channel; Electronics Letters, vol. 29, no. 14, 8 July 1993, pp. 1291 - 1293.

[33] A. Muller, J. Breguet and N. Gisin; "Quantum Cryptography with Polarized Photons in Optical Fibers: Experimental and Practical Limits"; Journal of Modern Optics Volume 41, Issue 12, 1994

[34] Richard J. Hughes, George L. Morgan, C. Glen Peterson; "Practical quantum key distribution over a 48-km optical fiber network"; Journal of Modern Optics,LA-UR-99-1593, 1999.

[35] K. J. Resch, M. Lindenthal, B. Blauensteiner, H. R. Boehm, A Fedrizzi, C . Kurtsiefer, A. Poppe, T. Schmitt-Manderbach, M. Taraba, R. Ursin, P.Walther, H.Weiner, H.Weinfurter, A. Zeilinger; "Distributing entanglement and single photons through an intra-city, free-space quantum channel"; Opt. Express 13, 202-209 (2005).

[36] Martin Hendrych; Experimental Quantum Cryptography; PhD. Thesis 2002

[37] Gregoire Ribordy, Juergen Brendel, Jean-Daniel Gautier, Nicolas Gisin, Hugo Zbinden; Long distance entanglement based quantum key distribution; Phys. Rev. A 63, 012309 (2000)

[38] C. Gobby, Z. L. Yuan, and A. J. Shields; "Quantum key distribution over 122 km of standard telecom fiber"; Applied Physics Letters 84, 3762-3764(2004)

[39] Hiroki Takesue, Sae Woo Nam, Qiang Zhang, Robert H. Hadfield, Toshimori Honjo, Kiyoshi Tamaki, Yoshihisa Yamamoto; "Quantum key distribution over 40 dB channel loss using superconducting single photon detectors"; Nature Photonics 1, 343 (2007) (revised version)

[40] P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam,E. Lita, A. J. Miller, J. E. Nordholt; "Long-distance quantum key distribution in optical fiber"; New J. Phys. 8 193, 2006

[41] Nicolas J. Cerf, Mohamed Bourennane, Anders Karlsson, Nicolas Gisin; "Security of quantum key distribution using d-level systems"; Phys. Rev. Lett. 88, 127902 (2002).

[42] W.-Y. Hwang; "Quantum Key Distribution with High Loss: Toward Global Secure Communication"; Physical Review Letters 91, 057901 (2003);

[43] [43] H.-J. Briegel, W. Dr, J. I. Cirac, P. Zoller; "Quantum repeaters for communication"; arXiv:quant-ph/9803056v1

[44] Zhen-Sheng Yuan, Yu-Ao Chen, Bo Zhao, Shuai Chen, Joerg Schmiedmayer, Jian-Wei Pan; "Experimental demonstration of a BDCZ quantum repeater node"; Nature 454, 1098 (2008)

[45] Michael A. Nielsen and Isaac L. Chuang; Quantum Computation and Quantum Information; 10th edition.

[46] Joern Mueller-Quade, Renato Renner; "Composability in quantum cryptography"; New Journal of Physics, 11, 085006, 2009 (Focus on Quantum Cryptography: Theory and Practice)

[47] Gilles Brassard, Norbert Ltkenhaus, Tal Mor, and Barry C. Sanders; "Limitations on Practical Quantum Cryptography"; Physical Review Letters, Volume 85, No. 6

[48] Thomas Jennewein , Christoph Simon , Gregor Weihs , Harald WeinfurterD, Anton Zeilinger; "Quantum Cryptography with Entangled Photons"; Phys. Rev. Lett. 84, 4729-4732 (2000)

[49] John Preskill; "Fault-tolerant quantum computation"; arXiv:quantph/ 9712048v1

[50] Llus Masanes, Stefano Pironio , Antonio Acn; "Secure deviceindependent quantum key distribution with causally independent measurement devices"; Nature Communications 2, Article number:238, 2011

[51] G Brassard ; "Bibliography of Quantum Cryptography";

[52] Nicolas Gisin, Grgoire Ribordy, Wolfgang Tittel, Hugo Zbinden; "Quantum cryptography"; Rev. Mod. Phys. 74, 145-195 (2002)

[53] Douglas Stebila, Michele Mosca and Norbert Ltkenhaus; "The Case for Quantum Key Distribution"; arXiv:0902.2839v.