DOI: http://dx.doi.org/10.26483/ijarcs.v8i8.4680

ISSN No. 0976-5697

Volume 8, No. 8, September-October 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

DIFFERENT VULNERABILITIES AND CHALLENGES OF QUANTUM KEY DISTRIBUTION PROTOCOL: A REVIEW

Chinmoy Ghosh
Department of Computer Science & Engineering
Jalpaiguri Government Engineering College
Jalpaiguri, West Bengal, India

Amit Parag, Shrayasi Datta
Department of Information Technology
Jalpaiguri Government Engineering College
Jalpaiguri, West Bengal, India

Abstract: Now days the information become the valuable assets and private information must be protected from being compromised. Today we use different sophisticated, robust encryption algorithm which are vulnerable to classical computational attack as well as the powerful parallel quantum computer. In this paper, we examine limitations and vulnerabilities and attacks to which Quantum Key Distribution can be exposed.

Keywords: Protocol; Quantum Key Distribution; BB84; E91; Quantum Non Demolition; Entanglement; Qubit; Einstein P Rosen (EPR) pairs

I. INTRODUCTION

A Cryptosystem [3] encrypts the data at the Sender' (commonly referred to as Alice) end and transmits it, through a secure channel, to the Receiver' (commonly referred to as Bob) end. The Sender and the Receiver are assumed to have pre-assigned Encryption and Decryption key. In Classical Systems [27], Symmetric and Asymmetric (widely used) algorithms are used to generate random keys. Quantum Cryptography [4][13] while retaining most aspects of Classical Cryptography, uses Quantum Key Distribution [6][9] to generate and transmit the key. The fundamental aspects of Quantum Mechanics, the Uncertainty Principle [1], Entanglement [14][13] and the Measurement Theory [16], provides a unique set of constraints on the communication channel[22]. The key generation can be distributed using protocols [15] such as BB84[32], E91[12], Decoy State Protocol, COW protocol among others. The most famous [10], for historical reasons, are the BB84 and the E91 protocols. A short Study of these two methods and an overview of the laws of Quantum Mechanics are presented below.

A. *The Uncertainty Principle*

Observables are associated to Hermitian operators [1]. Given one such operator A we can use it to measure the properties of any physical system in state Ψ. If the state Ψ is an Eigen state of the operator A, we have no uncertainty in the value of the observable corresponding to the eigen value of the operator A. Uncertainty in the value of the an observable 'A' exists if the state Ψ is not an Eigen state of A, but rather a superposition of various Eigen states with different eigen values. The uncertainty principle is an inequality that is satisfied by the product of the uncertainties of two Hermitian operators, A and B that fail to commute. The uncertainty of an operator on any state can be either greater than or equal to zero, the product of uncertainties in the two observables is, as a result, greater than or equal to zero [2]. The uncertainty inequality gives us a lower bound for the product of uncertainties. If two operators commute, the uncertainty inequality gives no information: it states that the product of uncertainties must be greater than or equal to zero.

The Uncertainty Inequality [1]

$$(\Delta_\psi \boldsymbol{A})^2 (\Delta_\psi \boldsymbol{B})^2 \geq \tfrac{1}{4}|<[\boldsymbol{A},\boldsymbol{B}]>_\psi|^2 + \tfrac{1}{4}|<\{\boldsymbol{A}-<\boldsymbol{A}>_\psi, \boldsymbol{B}-<\boldsymbol{B}>_\psi\}>_\psi|^2$$

Entanglement

Before you Entanglement is a basis-independent property [17]. When the state can be factorized into v∗ ⊗ w∗ for some basis choice in V and W, it can be factorized for any other basis choice by simply rewriting v∗ and w∗ in the new basis. If the state cannot be factorized into v∗ ⊗ w∗ for some basis choice in V and U, it cannot be factorized for any other basis choice because factorization with another basis choice would then imply factorization in the original basis choice[2] An **entangled state** is defined as a state that cannot be separated into a sum of its parts. A separable state is described as a probabilistic distribution over un-correlated states, product states,

$$\rho = \Sigma i p i \rho i V \otimes \rho i W.$$

For pure states the above definition is described in the following way: Consider two quantum systems *V* and *W*, with respective Hilbert spaces H*V* and H*W*. The Hilbert space of the general or entire system is a tensor product H*A* ⊗ H*B*. If the state $|\Psi\rangle AB$ of the composite system can be represented in the form[14]

$$|\Psi\rangle AB = |\psi\rangle V \otimes |\varphi\rangle W$$

Where $|\psi\rangle V \in \mathrm{H}V$ and $|\varphi\rangle W \in \mathrm{H}W$ are the states of the systems *V* and *W* respectively, then this state is called a *separable state*. Otherwise, it is known as an entangled state[14].

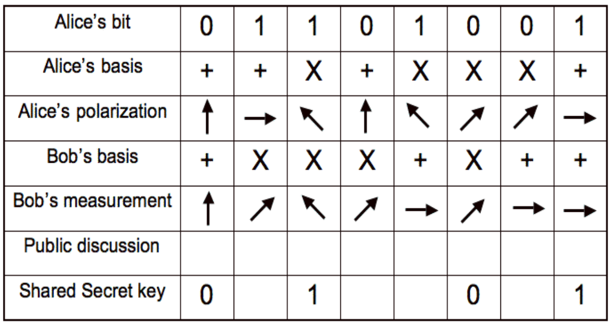
B. *Measurement Theory*

The entire theory of Quantum Mechanics, operators and transformations and observables, is simply the mathematical labeling of measurement results. The measurement of some observable of a quantum system, for instance energy and spin, is assumed to be completely accurate [31]. The state of a system before measurement is presumed to be any possible combination of Eigen States. The action of measurement forces the state to "collapses" into an Eigen state of the operator corresponding to the measurement. Redoing the identical measurement without letting the quantum system to evolve will, theoretically, give the same result [1][13].

However when the preparation of the quantum system is repeated, subsequent measurements will most likely yield completely different results. The expected values of the observables follow a probability distribution, based on the state of the system at the time when measurement is done. This probability distribution can be either continuous (such as momentum) or discrete (such as angular momentum), depending on the quantity being measured. The measurement process is considered to be random. [1].

C. *BB84 protocol*

This protocol, named after its inventors (Bennett and Brassard) and the year of invention, was initially defined using photon polarization states as a means to send information [9]. Nevertheless, any two pairs of conjugate states is sufficient for the execution of BB84[32][33] protocol, and many optical fiber centered cryptic systems implement BB84 using phase encoded states. The sender and the receiver apparatuses are linked by a quantum communication channel through which quantum states are transmitted. If photons are used as information carriers then either an optical fiber or simply free space can function as the communication channel. The sender and the receiver communicate via a public classical channel, for instance through broadcast radio or the Web. Neither of these channels needs to be secure; the protocol is designed with the supposition that an eavesdropper can interfere in any way with both[5][25].



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 1. BB84 Protocol

D. *E91*

The Ekert protocol uses entangled pairs of photons which are created by, not necessarily, the Sender or the Receiver. The photons are distributed in such a way that the Sender and Receiver get one photon of each entangled pair [10].

The Ekert protocol[12] uses two fundamental properties of Quantum Entanglement. First, the entangled states are correlated so that if Sender and Receiver measure the polarity, horizontal or vertical, of their particles, they get the same answer with absolute probability. This also holds for any other pair of complementary (orthogonal) polarizations [25]. However the two parties must have exact directional synchronization. The particular results may be random; consequently the Sender and the Receiver cannot predict the polarization of their photon. Second, any attempt at eavesdropping by an intruder destroys the entanglement correlations while revealing the presence of the Attacker [26].

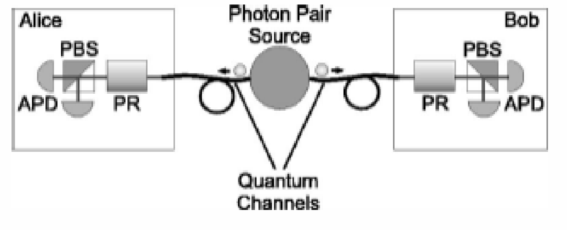


Figure 2. A typical system using entangled photon pair

II. LITERATURE SURVEY

Quantum Cryptographic Systems must necessarily work on protocols which describe Quantum Key Distribution[28]. These protocols are reviewed by Heitjema [15][18] in a summary while the classic texts of Bennet and Bassard [7] detailed the inner workings and the evolution of such systems. The current advancements in the field include laying networks of systems running on Quantum Key Distribution and relaying information through multiple channels [19]. However attacks have been successfully carried out on quantum systems, the latest one uses eavesdropping on a 290m communication channel [6]. On the other hand, the simplistic standard BB84 systems have been installed in metropolitan areas for testing. With the use of high key generation rate most of the usual forms of attack have been thwarted [21] [24][29]. The growth of Quantum cryptography is intricately linked with the evolution of attacks on it as detailed in [13][14][25].

III. DIFFERENT ATTACKS

Though Quantum key Distribution Protocol appears to be more powerful in compare to the conventional protocol they also suffers from different types of attack. Here we tried to provide some idea to the different types of attacks on Quantum key distribution protocols.

A. *Intercept and Resend*

Intercept and Resend is perhaps the simplest form of attack[6]. The Attacker measures the quantum states (photons) sent by Sender and then sends replacement states to Receiver, prepared in the state measured by the Attacker. If this method is used in the BB84 protocol, errors creep in the key which Sender and Receiver share. As the Attacker has no knowledge of the basis of states sent by Sender, he can only guess which basis to measure in. If the Attacker chooses correctly, then he measures the correct photon polarization state as sent by the Sender, and resends the correct encoded state to the Receiver. But if the guess is incorrect, then the state he measures is completely arbitrary, and therefore, the state sent to Receiver can never be identical to the state transmitted by Sender. If the Receiver measures this state in the same basis he gets a random result—since the Attacker has sent him a state in the contrary basis— with a 50% error chance (instead of the correct result he would get without the presence of Eve).

This attack strategy is frequently tested in ideal settings. In a less developed form of the Intercept/Resend (I/R) attack, the Intruder intercepts photons from the Sender who has encoded it with his own predefined basis[13]. Meanwhile, in the perfect environment, the detectors are extremely efficient which help the Intruder to get each incoming photon. In the naïve intercept resend attack, it is assumed that the Attacker is not watching the public channel i.e. sifting phase of BB84 protocol. The information gain in this method is approximately 0.2 bits out of every bit transmitted by Sender.

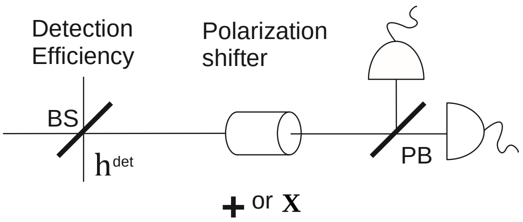


Figure 3. The polarization shifter allows to change the polarization basis (+ and ×) of the measurement as desired. The polarization analyzer consists of a polarizing beam splitter (PB) and two ideal detectors. The PB discriminates the two orthogonal polarized modes. Detection efficiencies are modeled by a beam splitter (BS) of transmittance $\eta_{det.}$

B. *Man-in-the-middle attack*

Quantum key distribution is exposed to Man-in-the-Middle attack when used without establishing proof of identities to the same extent as any classical protocol[30]. If Sender and the Receiver have an initial shared secret then they can use an unconditionally secure authentication scheme along with quantum key distribution to exponentially expand this key, using a new key to validate the next session.

Man-in-the-middle (MITM) attacks can be performed in a couple of ways. The earlier MITM attacks do not work on QC systems because laws of quantum mechanics step in. With traditional MITM attacks, the Interceptor would intercept the transmitted messages and send a copy in its place. However this is impossible due to the physics of QC systems, although non-traditional MITM attacks are possible. The first, comprises the Attacker pretending to be "Sender" to the Receiver and "the Receiver" to Sender. He would then communicate with both the Sender and Receiver simultaneously thereby obtaining two keys, one for Sender and one for the Receiver. Sender' key would be used to decrypt a message from Alice then reencrypted by he Receiver's key. This type of attack is possible, but may be prevented if identities can be authenticated.

The other kind of MITM attack involves the method through which photons are transmitted[17]. A single photon for transmission is difficult to realize in real world, most cryptic systems use small bursts of coherent pulses for transmission. Theoretically, the Attacker may split a single proton from the burst without detection. He could then store the stolen photons until the basis used to create them is announced. EPR pairs can be used for a possibly secure three-stage protocol that can avoid man-in the-middle attack. But distributing the EPR pairs might corrupt them during transit.

C. *Faked States Attack*

This is a special form of Intercept/Resend attack type of attack which focuses on collecting the information by exploiting the imperfections in the Receiver's system[6]. In this method the Attacker sends the self-derived signal to control the entire communication. "Full detector efficiency mismatch" is fundamental in this type of attack. The signal which the Receiver gets from the Attacker after he has intercepted the Sender's signal has a time shift that if the Receiver chooses the basis other than that of the Attacker for that reading signals then, he will not detect signals. In generic terms, his detector will be blinded. And, throughout this process, Attacker remains undetected.

In BB84 protocol, the various steps in this attack are:

- Attacker performs the simple Intercept/Resend attack over transmitted signals and measures in his own basis.
- The Attacker then sends a pulse to the Receiver such that it contains opposite bit value in the opposite state. This sets the time shift of the signal so that the Receiver can only measure the signal if the same basis (as that of the Attacker) is used. Measurement in other bases will result in nothing.
- Now the Attacker measures the signal using the Sender's basis. The Receiver will get identical results, identical to that of the Attacker.
- Therefore the Attacker now has complete control on the Receiver's scheme. This attack strategy depends on Synchronization and efficiency of the Detectors[27].

D. *Denial of service*

The latest implementations of QKD require a dedicated fiber optic line, or a line of sight in free space, between the Sender and the Receiver[3]. A Denial of Service attack can take place by cutting off the cable or obstructing the line of sight. This is one of the motivations for the development of quantum key distribution networks[20], which would route communication via alternate links in case of disruption.

DoS attack in QKD is done in two ways: one, compromises the quantum cryptographic hardware, and second, introduces extra noise in the QKD system. QKD systems which use fiber optic channels can be commissioned out of service by simply cutting off or blocking the optical cable. The fiber-optic channel can be readily made unusable by simply tapping into the line. The QKD equipment itself could be compromised to generate unsecure random photons by using a random number generator algorithm [24].

A DoS attack against a QC system may also be mounted if it is possible to insert noise in the communication system. This noise would be indistinguishable from eavesdropping so that the Sender and the Receiver will be induced to discard a number of photons. If the additional noise can be sustained in the communication channel, then the Sender and the Receiver may increase their error threshold to compensate for noise, which would make render eavesdropping more easily [16].

E. *Trojan Horse Attacks*

Quantum physics cannot protect Sender' and the Receiver's apparatuses. Indeed, as soon as the information is encoded in a classical physics system, it is vulnerable to security flaws and hacks[11]. The Sender and the Receiver have to protect their instruments through usual defenses. Practical implementations of abstract QKD uses present technology (and are bound by economical constrains). This results in a deviation from the ideal scheme.

In Trojan Horse Attacks, the Intruder focuses on the cryptographic devices used by Sender and the Receiver, unlike the previously defined attack which try to extract the information from the photons that are being transmitted in the channel. This strategy is implemented by sending out the light pulses towards the sender's or receiver's setup, which in return comes as the reflected pulse and enter the detection scheme which is also a possession, of Eve. Eve can use the information of the reflected signal and can intercept the basis used by Alice for the preparation of the photon. Now, if Eve is able to get this information before that photon reaches the the Receiver side, then Eve can perform simple Intercept/Resend attack and measure it to get the exact secret string of qubits.

Hence, Eve can get sufficient amount of the information without being detected. It is thus of vital importance for QKD to analyze properly the consequences of these compromises. Indeed, some compromises might render the entire system totally insecure.

Trojan Horse attacks works by attacking target vulnerabilities in the operation of a QKD protocol or deficiencies in the components of the physical devices used in construction of the QKD system. If the equipment used in quantum key distribution can be tampered with, it could be made to generate keys that were not secure using a random number generator attack**.** Trojan Horse attack is also known as light injection attack[20][23].

F. *Photon number splitting attack*

Outside experimental settings, a true single photon source is hard to generate, so the Sender uses weak laser pulses (WLP) generators instead. The coherent light pulse so emitted follows a Poisson distribution. The probability of a pulse to comprise of n photons is Pn = μ^n/(n!e^μ) , where μ is the mean photon number , taken to be a number less than 1 to avoid pulses with more than one photon. But multiple photon pulses will still occur with some probability. This results in the possibility of photon-number-splitting (PNS) attack[14][26].

In this attack, the Attacker replaces the high loss channel used by the Sender and the Receiver with a lossless channel. The Attacker then performs a quantum non-demolition (QND) measurement on each pulse thus obtaining information without disturbing the bases of the encoded pulse. If a pulse with a single photon is transmitted, then the Attacker simulates the loss of the original pulse by blocking a fraction of these pulses. When a pulse with multiple photons arrives, then the Attacker splits and stores a photon from that pulse in a quantum memory. After storing, the Attacker transmits the remaining pulse to the Receiver. When the Sender and the Receiver announce the bases used for each pulse, the Attacker retrieves the photons from the quantum memory and as a result obtains a significant fraction of the key without detection. Typically each signal pulse contains a number of photons. Cryptographic devices generally rely on Weak Coherent Pulses. A WCP is a photon pulse with low mean photon number. PNS attack takes advantage of this limitation and by targeting multiple photons pulses, becomes a potent attack[8]. The PNS attack, however, is quite complex. The probability of a pulse to contain multiple photons is around 5% and the number of dark counts (no photons in the pulse), is quite high. Hence, the Attacker has to check continuously for multiple photon pulses. This requires complex hardware and algorithms.

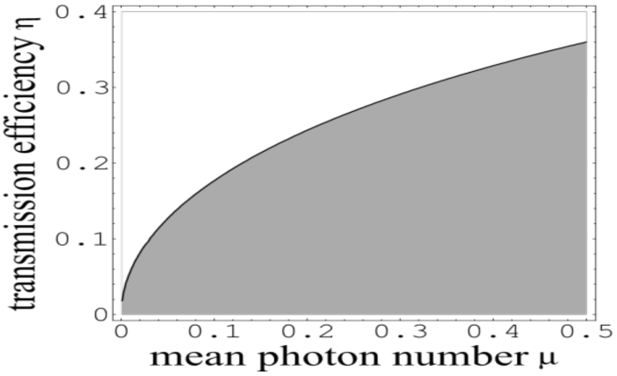


Figure 4. As a function of the mean photon number μ and the transmission efficiency η, we see the area (grey shade) where the original PNS attack yields fewer single-photon signals than the corresponding lossy channel.

G. *Spectral Attacks*

Quantum key distribution has the property to detect the presence of any third party trying to gain knowledge of the key. This result from a fundamental aspect of quantum mechanics: the process of measuring a quantum system in general disturbs the system. Therefore if the Intruder is trying to eavesdrop on the key, then he must measure it in some way thereby resulting in a disturbance of the system. This leaves traces. By using quantum superposition or quantum entanglement and transmitting information in quantum states, a communication system can be implemented which detects eavesdropping. If the level of eavesdropping is below a certain threshold, a secure key can be generated otherwise no secure key is possible and communication is aborted. However a possible way around this is by measuring the spectral characteristics [34] of the photons involved, instead of their polarization. So, if the Attacker measures the color of each photon then the polarization states will be not perturbed to leave traces.

IV. CONCLUSION

Quantum Key Distribution is not entirely failsafe. Loopholes and errors in its implementation can be used to attack and manipulate the cryptic channels. Each of these attacks work by targeting some vulnerable feature of the system in question. The scope of these attacks is therefore limited by the security surrounding the system. Quantum Cryptographic systems are available for closed circuit small range commercial implementations where the Intruder has limited resources to plug into the system with detection. The most powerful of these attacks are the Trojan Horse attacks and the Photon Number splitting strategy. Man-in-the-Middle, Intercept and Resend, and Faked states attacks works in almost all cryptographic systems. However, Quantum Key Distribution provides a powerful way to communicate securely and as such; it is something to look forward to in the future. Every secure system will have attacks to disable its firewall and even Quantum Key Distribution needs a robust wall of defense.

V. REFERENCES

[1] Barton Zwiebach, Quantum Mechanics 2, MIT OCW

[2] Wolfgang Ketterlee, Isaac Chung, Atomic and Optical Physics, MIT OCW.

[3] Kollmitzer, Pivk et al, “Applied Quantum Cryptography”.

[4] D. Mayers, “ Advances in Cryptology”

[5] H. Inamori, N. L¨utkenhaus and D. Mayers, “Unconditional security of practical QKD”, The European Physical Journal, Volume 41, Issue 3, pp 599-62, March 2007.

[6] Ling , Gerhardt, Linares, “Full Field Implementation of a perfect Eavesdropper on a quantum cryptography system”, Nature Communications 2, Article number 349, 2012.

[7] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” IEEE Systems and Signals Processing, Volume 175, 8, 1984.

[8] L. Lydersen Wikkers, Wittman et al, “Hacking Commercial quantum cryptography systems by tailored Bright illumination” Nature Photonics4, 686–689,2010.

[9] QKD, Wikipedia, https://en.wikipedia.org/wiki/Q_k_d

[10] Post-Quantum Cryptography: 5th International Workshop, PQCrypto 2013,edited by Philipe Gaborit.

[11] Nitin Jain, Birgit Stiller, Imran Khan, Vadim Makarov, Christoph Marquardt, Gerd Leuchs, "Trojan-horse attacks Threaten the Security of Practical Quantum", Cryptography,New J. Phys. 16, 123030 (2014).

[12] C.H. Bennett, "Quantum cryptography using any two non-orthogonal states", Physical Review Letters 68 (21), 3121-3124, 1992

[13] David Miller, "Quantum Mechanics for Scientists and Engineers"

[14] Leonard Susskind, "Quantum Entanglement Lectures"

[15] Mart Haitjema, "A Survey of the Prominent Quantum Key Distribution Protocols".

[16] MIT Ocw, Quantum Mechanics 1

[17] Coursera, Quantum Computation

[18] Lo, Cutry, Tamaki "Secure quantum key distribution", Nature Photonics 8, 595-604, 2014.

[19] Elliott, Colvin. et al., "Current status of the DARPA Quantum Network", In Proc SPIE, Quantum Information. Computation III, 138 June 02, 2005

[20] Fröhlich, B. et al. "A quantum access network", Nature 501, 69–72, 05 September 2013

[21] Cao, Zheng et al, "Highly Efficient Quantum Key Distribution Immune to All Detector Attacks", arxiv.org/pdf/1410.2928.

[22] Biham, Boyer ,et al," Security of Quantum Key Distribution Against All Collective Attacks", Quantum Physics, 12th Jan, 1998, pp 1-5

[23] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G Ribordy, "Trojan-Horse Attacks on Quantum-Key- Distribution Systems", Phys. Rev. A 73, 022320 -2006.

[24] Normand J. Beaudry, Marco Lucamarini, Stefano Mancini, Renato Renner, "Security of two-way Quantum key distribution", PHYSICAL REVIEW A 88, 062302 -2013.

[25] Christianson, Bruce , Lecture Notes in Computer Science, 8263

[26] A. Vakhitov, V. Makarov, and RD. Hjelme, Large Pulse Attack as a Method of Conventional Optical Eavesdropping in Quantum Cryptography, J. Mod. Opt. 48, 2023 (2001).

[27] Stallings, "Cryptography and Network Security.

[28] ETSI- Quantum Key Distribution, http://www.etsi.org/technologies--clusters/technologies/quantum-key-distribution

[29] Feihu Xu, Bing Qi, Hoi-Kwong Lo, "Experimental demonstration of phase-remapping attack in a practical Quantum key distribution system". New J. Phys. 12, 2010

[30] "Quantum crack in cryptographic armour", Nature News, http://ww w.nature.com/news/2 010/100520/full/ new.256.html

[31] Measurement In Quantum Mechanics , http://en.wikipedia.org/wiki/Measurement_in_ quantum_mechanics.

[32] Thomas Baign`eres, "Quantum Cryptography: On the Security of the BB84 Key-Exchange Protocol".

[33] M.D.Dang and M. Riguldel, "Usage of secure networks built using quantum technology", 2004

[34] Scarani, Valerio, et al. "The security of practical quantum key distribution." Reviews of modern physics 81.3 (2009): 1301.