QUANTUM CRYPTOGRAPHIC PROTOCOLS FOR SECURE COMMUNICATION

N. L. GUPTA[1]
D. R. MEHROTRA[2]
ASHUTOSH SAXENA[3]

[1, 2] Quantum Information Unit, Government College, Ajmer, Rajasthan, India
[3] Software Engineering Technology lab, Infosys Technology Limited, Hyderabad, AP, India
[1, 2] nlgupt@gmail.com [3] ashutosh_saxena01@infosys.com

Abstract: Quantum Cryptography offers a secure method of sharing sequences of random numbers to be used as cryptographic keys. It can potentially eliminate many of the weaknesses of classical cryptographic methods. In this paper, we survey some results in quantum cryptography. After a brief introduction to classical cryptography, some fundamental quantum key distribution protocols are reviewed. The issue of security both from theoretical as well as real life point of view is also addressed. Finally we point out some noteworthy recent advances and some important remaining challenges.

Key words: Cryptography, Quantum Cryptography, Information Security.

(Received Dec. 02, 2008 / Accepted April 26, 2009)

1 Introduction

In human societies, the desire and necessity of secure transmission of information dates back at least as far as the first known societies themselves [20]. With the growth of computer networks for communication of confidential information the importance of cryptography–the art of using coded messages-is growing each day.

Modern cryptographic techniques, based on the availability of ever increasing computational power, and the invention of public key cryptography, provide practical solutions for information security in various situations. But invariably these techniques are only computationally–and not unconditionally secure, that is, they depend on the unproven hardness of certain mathematical problems. As a result, it cannot be guaranteed that future advances in computational power will not nullify their cryptographic protection.

Indeed, it has been shown that quantum computers can factorize integers and compute discrete logarithms much faster than classical computers [31]. Hence all classical cryptosystems whose security is based on the hardness of solving mathematical problems have become vulnerable. However, while quantum computation seems to be a severe challenge to classical cryptography in a possibly not so distant future, at the same time it offers new possibilities to build encryption methods that are safe even against attacks performed by means of a quantum computer. Quantum cryptography extends the power of classical cryptography by protecting the secrecy of messages using the physical laws of quantum mechanics. The development of quantum cryptography is mainly devoted to practical and efficient use of quantum key distribution (QKD) protocols, which has been recently been a major topic of research in the field of communication security. In this paper we discuss the principles of quantum cryptography and review some well known quantum key distribution protocols. We also address the issue of security both from theoretical and real life point of view,

pointing out some noteworthy recent advances and some important remaining challenges.

2 Classical Cryptography

There are two branches of modern cryptographic techniques: public-key or asymmetric cryptography and secret-key or symmetric cryptography. In secret-key cryptography the same key is used for encryption and decryption (or the decryption key is easily derived from the encryption key), whereas public key cryptosystems use a different key for encryption and decryption, and derivation of the decryption key from the encryption key is computationally infeasible. In practice, symmetric cryptography suffers from the logistic problem of key distribution. The secret key must be distributed to two parties before secure communication. This simple fact became the biggest problem of cryptography, especially with the development of the internet and the proliferation of electronic communication systems. Moreover, key distribution represents the most vulnerable phase in the communication process. Due to these significant difficulties in secret key cryptography, public-key cryptographic algorithms are widely used in conventional cryptosystems.

Public-key cryptography is the technological revolution which solves the key distribution problem. It is based on a pair of asymmetric keys. A message is encrypted with the public key of the receiver. The resultant ciphertext is unreadable and can be securely sent. Only the receiver can decrypt the message with his private key. The private key corresponds to the public key via a mathematical one-way function in order to achieve computational infeasibility of its deduction from the public key. Hence, the public key can be published without compromising security. A certification authority authenticates the public key as key of the legitimate user.

Public-key encryption schemes can only be proven secure based on the presumed difficulty of a mathematical problem, such as factoring the product of two large primes. Recent work shows that quantum computers can speed up the solution of these problems [31]. It has not been determined yet, if a quantum computer can ever be developed to a sufficient level. But assuming its construction, it would render all existing classical techniques obsolete except for one.

2.1 The Vernam Cipher

Only one classical cipher, the one-time pad, also called Vernam cipher, offers unconditional security, which was mathematically proven by Shannon [29]. It relies on a secret key known only to Alice and Bob (conventional names of the sender and receiver respectively).The secret key must be the same length as the data to encrypt. By using the secret key only once to encrypt and decrypt the data it is impossible for anyone who receives only the encrypted data to decrypt it without knowing the secret key.

A simple implementation of the Vernam cipher is given in Figure 1. Alice encrypts the message she wishes to send to Bob using her key and the XOR operation as the encrypting operation. Bob receives the encrypted message and performs the inverse operation (the XOR again) with his secret key in order to decrypt and recover Alice's original message.

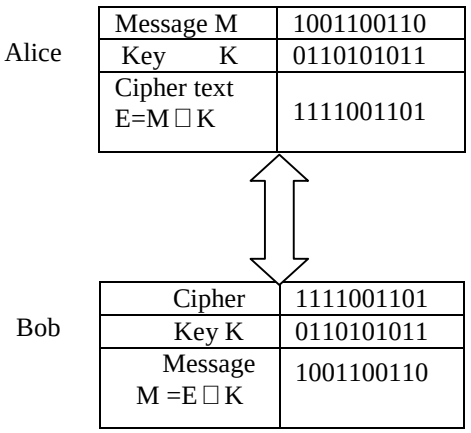

Figure 1: Implementation of the Vernam Cipher with the XOR operation

Despite Shannon's proof of its security, the one-time pad has serious drawbacks in practice. As it is a symmetric cipher based on one private key, key distribution problems are inevitable. To provide unconditional security the key must be real random and of the same length as the message. Furthermore, the same key can be used only once. If one of these conditions is violated, the one-time pad is no longer unbreakable. These implementation difficulties are so critical that they have prevented the one-time pad from being adopted as a widespread tool in information security.

Quantum physics offers a solution to the aforementioned difficulties for the one-time pad. First, the superposition nature of quantum mechanics can generate true randomness. Secondly, quantum cryptography allows two distant parties to generate secure keys.

3 Quantum Cryptography

3.1 Principles of Quantum Cryptography

Quantum cryptography does not base security on unproven mathematical problems. Instead, the foundation of security lies in the properties of quantum mechanics. Three such properties essential for quantum cryptography are:

1. We cannot make a measurement on an unknown quantum system without perturbing it unless the measurement is an eigen operator to the quantum state being measured.

This implies that an eavesdropper (conventionally called Eve) cannot make a measurement of an unknown quantum state in order to obtain some information about the key without introducing disturbances that can in turn be discovered by Alice and Bob.

2. We cannot make a copy of an unknown quantum state. This property is usually referred to as the no-cloning theorem [34].

It prevents an eavesdropper from simply intercepting the transmission and making copies of the transmitted quantum states in order to keep copies to make measurements on, while passing on an unperturbed quantum state to Bob.

3. We cannot measure the simultaneous values of non-commuting observables on a single copy of a quantum state.

It ensures that the eavesdropper cannot construct a measurement that is an eigen operator to all quantum states used for the key distribution, i.e., it guarantees that it is impossible for the eavesdropper to only perform measurements that leave the quantum states unperturbed.

Quantum cryptography cannot securely transmit predetermined information; it can only securely generate a random key. Once generated, this random key can be subsequently used in a symmetric cipher, such as the one-time pad or one of the modern symmetric ciphers, to securely transmit data over a classical communication channel. A running quantum cryptography channel will steadily generate new secret key material. Thus, quantum cryptography is solving the most difficult problem in modern cryptography, that of key distribution.

There are mainly two types of quantum key distribution (QKD) schemes. One is the prepare-and-measure scheme, such as BB84 [4], in which Alice sends each qubit in one of four states of two complementary bases; B92 [6], in which Alice sends each qubit in one of two non-orthogonal states; six-state [9], in which Alice sends each qubit in one of six states of three complementary bases. The other is the entanglement based QKD, such as E91[14], in which entangled pairs of qubits are distributed to Alice and Bob, who then extract key bits by measuring their qubits; BBM92[3], where each party measures half of the EPR pair in one of two complementary bases. We discuss here three important protocols.

3.2 BB84 Protocol

The first and best known protocol, BB84, defined by Bennett and Brassard in 1984, uses four quantum state $\{|0\rangle,|1\rangle$, $|+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle), |-\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\}$ .These states can be represented by any two-level quantum system, for instance photon polarization, phase encoding, or spin ½ systems. For linear polarized photons: the first two states corresponds to vertically (↑) and horizontally polarized (→) photons, the last two to polarization angles 45^o (⊠) and -45^o (⊠) with respect to the vertical axis. Let the states $|0\rangle$ and $|+\rangle$ represent bit value '0', $|1\rangle$ and $|-\rangle$ stands for bit value '1'.The pairs $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle,|-\rangle\}$ form two orthonormal and conjugate bases. We call them rectilinear (⊞) and diagonal basis respectively (⊠).

BB84 requires two communications channels between Alice and Bob. Firstly, there is a public unjammable classical channel, i.e., it is assumed that everyone, including the eavesdropper, can listen to the conversations but cannot change the message. Second, there is a channel for quantum signals. In practice, the transmission can be done through free air or optical fibres. The quantum channel is assumed to be insecure. i.e., the eavesdropper is free to manipulate the signals.

Alice sends qubits to Bob. Eve can operate on them before Bob. However, since she does not know the correct basis, she will, with high probability, disturb some of the states. Once Bob receives the qubits, the no-cloning theorem guarantees that Eve does not have copies. Alice can now freely reveal the correct bases to Bob so that he can gain full information.

The protocol consists of following steps (Table1):

1. Quantum transmission phase

In this phase Alice randomly generates bit string that she wants to transmit. Randomly and independently for each bit she chooses her encoding basis and prepare the states. Alice sends all prepared states to Bob via the insecure quantum channel. Bob, randomly and

independently of Alice, chooses his measurement basis for each qubit he receives. Bob records his measurement bases and the results of the measurements.

2. Bases announcement

Bob announces his bases (but not the results) through the public unjammable channel that he shares with Alice. Observe that it is too late for Eve to use this information to affect Bob's state. Alice and Bob, via public discussion, agree to discard the data bits where they used opposite bases. Statistically, this happens in about half of the cases. Remaining sequence of bits forms their, so called, sifted key.

3. Error estimation

Alice and Bob both hold a string now, which would ideally be equal. But they have to check whether there was an eavesdropper present. This can be determined by the error rate, i.e. the difference between Alice's and Bob's key. Alice and Bob calculate the error rate by comparing some randomly chosen bits. If the calculated error rate is higher than some prescribed threshold value, they abort. Otherwise they perform classical post processing such as error correction and privacy amplification to generate the final key.

Table 1: The BB84 protocol

Alice's random bit sequence	1	0	1	1	0	1	0	1
Alice's random sending basis	⊠	⊞	⊞	⊠	⊠	⊞	⊠	⊞
Alice's photon polarization	□	↑	→	□	□	→	□	→
Bob's random measuring basis	⊞	⊠	⊞	⊞	⊠	⊠	⊠	⊞
Bob's measured polarization	→	□	→	→	□	□	□	→
Bases announcement			OK		OK		OK	OK
Sifted key			1		0		0	1

3.3 B92 Protocol

Unlike BB84 which requires two orthogonal bases, B92 protocol can be implemented in terms of a single non-orthogonal basis or two non orthogonal states [6]. Since the states are non orthogonal neither Bob nor Eve can unambiguously decode all the bits on the quantum channel. However, Bob can perform two separate measurements using the suitable quantum projection operators. By performing measurements using the operators, Bob either detects Alice's transmitted bit correctly, or a random result known as an erasure. The correct measurements are termed non–erasures.

Let us take the basis as $\{|\Phi\rangle, |\bar{\Phi}\rangle\}$ which denote the kets representing the polarization states of a photon linearly polarized at an angle Φ and an angle $-\Phi$ with respect to the vertical, where $0<\Phi<\pi/4$. Let $|\Phi\rangle$ is represented by 1 and $|\bar{\Phi}\rangle$ is represented by 0. Similarly to BB84, in B92 Alice and Bob communicate first over a one-way quantum channel and then over a two-way classical channel.

The B92 protocol can be summarized as below:

Alice sends her random binary sequence to Bob in the form of $|\Phi\rangle$ and $|\bar{\Phi}\rangle$. Bob chooses a strategy to measure it. Bennet [6] uses the projection operators $P_{-\Phi}=1-|\Phi\rangle\langle\Phi|$ and $P_{-\bar{\Phi}}=1-|\bar{\Phi}\rangle\langle\bar{\Phi}|$. Another scheme could be positive operator value measure (POVM) [13], using the operators $A_{\Phi}=\frac{P_{-\Phi}}{1-\|\langle\Phi|\bar{\Phi}\rangle\|}$ and $A_{\bar{\Phi}}=\frac{P_{-\bar{\Phi}}}{1-\|\langle\Phi|\bar{\Phi}\rangle\|}$ and $A_{null}=1-A_{\Phi}-A_{\bar{\Phi}}$.

In the first case Bob randomly chooses $P_{-\Phi}$ and $P_{-\bar{\Phi}}$ to measure incoming bits. The probability of Bob's correctly detecting (non-erasures) Alice's transmission is $\frac{1-\|\langle\Phi|\bar{\Phi}\rangle\|^2}{2}$ and probability of receiving an ambiguous result (erasure) is $\frac{1+\|\langle\Phi|\bar{\Phi}\rangle\|^2}{2}$, where $\|\langle\Phi|\bar{\Phi}\rangle\| = \cos(2\Phi)$. The second scheme is more efficient where the probability of an inconclusive result is $\cos(2\Phi)$.

Bob publicly announces time-slots when he received correct measurements from Alice. Bits in those time slots become the sifted key for Alice and Bob. If there is an unusual error rate in Bob's raw key, it is assumed that an eavesdropper Eve is present and hence the transmission is aborted.

3.4 EPR Protocol

In 1991, Ekert proposed the first entanglement based QKD protocol, commonly called E91 [14]. Einstein, Podolsky, and Rosen (EPR) in their famous 1935 paper challenged the foundations of quantum mechanics by pointing out a paradox. There exist spatially separated pairs of particles, henceforth called EPR pairs, whose states are correlated in such a way that the measurement of a chosen observable A of one automatically determines the result of the measurement of A of the other. Since EPR pairs can be pairs of particles separated at great distances, this leads to what appears to be a paradoxical "action at a distance." Bell [1] gave a means for actually testing for locally hidden variable

theories. He proved that all such locally hidden variable theories must satisfy the Bell inequality. Quantum mechanics has been shown to violate the inequality. Bell's theorem provides a method for checking eavesdropping. The fact, that the entangled photons do not satisfy Bell's Inequality, is exploited to detect the presence of eavesdropper.

The key distribution is performed via a quantum channel that consists of a source that emits pairs of photons in the singlet state of polarizations $|\Phi\rangle = \frac{1}{\sqrt{2}}(|\rightarrow\rangle|\uparrow\rangle - |\uparrow\rangle|\rightarrow\rangle)$. The two photons fly along the z-axis to Alice and Bob, respectively. They perform measurements and register the outcome in one of three bases, obtained by rotating around the z-axis by angles, say, $\Phi_1^a=0$, $\Phi_2^a=\pi/4$, $\Phi_3^a=\pi/8$ for Alice and by $\Phi_1^b=0$, $\Phi_2^b=-\pi/8$, $\Phi_3^b=\pi/8$ for Bob. These angles are chosen independently and randomly for each pair. The outcomes can be ±1 depending on which polarization is measured.

The correlation coefficient of the measurements is given by

$$E(\Phi_i^a,\Phi_j^b) = P_{++}\left((\Phi_i^a,\Phi_j^b\right) + P_{--}(\Phi_i^a,\Phi_j^b) - P_{+-}(\Phi_i^a,\Phi_j^b) - P_{-+}(\Phi_i^a,\Phi_j^b) \quad (1)$$

and quantum mechanics predict

$$E(\Phi_i^a,\Phi_j^b) = -\cos[2(\Phi_i^a - \Phi_j^b)] \quad (2)$$

Where the P's are the probabilities that ±1 are obtained in the respective bases. For the two pairs of bases 1 and 3 quantum mechanics predicts perfect anticorrelations $E(\Phi_1^a,\Phi_1^b)= E(\Phi_3^a,\Phi_3^b) = -1$.

Alice and Bob now define

$$S = E(\Phi_1^a,\Phi_3^b) + E(\Phi_1^a,\Phi_2^b) + E(\Phi_2^a,\Phi_3^b) - E(\Phi_2^a,\Phi_2^b) \quad (3)$$

Which according to generalized Bell theorem [11] should be $S= -2\sqrt{2}$ for maximally entangled state.

They discard measurements in which either or both failed to register a qubit. Alice and Bob can now publicly announce the orientations of the analyzers. Then they announce all results for which their orientations were different. This allows them to establish the value for S which will be $S= -2\sqrt{2}$ if the particles were not disturbed. This assures them that the other measurements, where they used the same orientation of analyzers, are perfectly anticorrelated and can be used to establish a secret key.

An eavesdropper, Eve, cannot extract any information from the particles while in transit from the source to the legitimate users, simply because there is no information encoded there. The information comes into being only after the Alice and Bob perform measurements and communicate in public afterwards. Eve may try to substitute her own prepared data for Alice and Bob to misguide them, but as she does not know which orientation of the analyzers will be chosen for a given pair of particles, there is no good strategy to escape being detected. In this case her intervention will lower the value of S below its expected value for Alice and Bob.

4 Information Reconciliation and Privacy Amplification

The quantum cryptography protocols described above will provide Alice and Bob with nearly identical shared keys, and also with an estimate of the discrepancy between the keys. These differences can be caused by eavesdropping, but will also be caused by imperfections in the transmission line and detectors. As it is impossible to distinguish between these two types of errors, it is assumed all errors are due to eavesdropping in order to guarantee security. Provided the error rate between the keys is lower than a certain threshold, two steps, known as information reconciliation and privacy amplification, can be performed to first remove the erroneous bits and then reduce Eve's knowledge of the key to an arbitrary small value.

4.1 Reconciliation

In this phase Alice and Bob reconcile their keys through public discussion to ensure that there are no errors. This process uses the Cascade Cipher method [2] ensuring high accuracy yet low data lost to Eve. Alice and Bob agree on a random permutation to be applied to the bits. This is to randomize the locations of the errors. The key is split into blocks of a size that ensures an average of one bit error per block. They then perform a parity check on each block. If a discrepancy is discovered the block is broken down binomially until the incorrect bit is found and fixed. For each block compared, the last bit must be dropped to ensure that Eve has not gained useful information. This process is repeated, increasing the block size each iteration, until the statistical probability of remaining errors is very low.

Final confirmation of the key is performed by selecting random subsets of bits and comparing them, again with a parity check. It can be shown [2] that for p subsets the probability that an error in the key remains is

2^{-p}. It can be believed that the share key is now the same may be with error but an acceptable rate if p is large enough.

4.2 Privacy Amplification

At this point Alice and Bob share an *n*-bit identical key, yet it is possible that Eve has derived deterministically some k physical or parity bits. Alice and Bob must ensure that the k subset of bits known to Eve does not help her in determining the key. To achieve this, privacy amplification is performed. The aim of this phase is to minimize as far as possible Eve's information about the key and to generate a shorter but more secure key. There are two methods for realizing this: with a randomly selected hashing algorithm [5] or with entanglement purification scheme [12].

Hashing permutes the key such that any incorrect bits destroy any similarities in compared results. This is very simple and can be performed in O (n) time, though it must assume that the channel is noiseless. Thereby the size of k is equal to the error rate derived in the error estimation phase. This assumption causes the system to be inoperable under high-noise environments; else some level of security must be compromised and therefore no longer guarantees absolute security.

The latter method uses entanglement purification scheme, dubbed Quantum Privacy Amplification [12], which relies on pure-qubit entangled pairs (known as the Bell state). This method allows privacy amplification over noisy channels while still offering protection from Eve.

5 Vulnerabilities

The cryptography and the cryptanalytics are always a pair's contradiction. Once a cryptographic protocol is proposed, eavesdropper will try to break it. Quantum cryptography is also no exception, although each protocol can ensure absolute secure key distribution under perfect quantum conditions, but unfortunately today's quantum equipment for transmission and especially detection is far from perfect, opening these protocols to a number of attacks. The following are the theorized attacks open to Eve in circumventing the quantum cryptography protocol.

5.1 Intercept-Resend Attack

The most common eavesdropping strategy one can think of is the so-called intercept-resend attack. An eavesdropper simply interrupts the quantum channel, measures each incoming photon from Alice in a fixed or random basis and afterwards sends the state which she has measured to Bob. Assuming the BB84 protocol [4], only 50% of Eve's bases choices will be compatible with the signal. These measurements lead to the correct result. The remaining 50% of the results will be random. Bob finds that 25% of all signals are erroneous. This is no problem if the hardware induces an error rate below 25%. The protocol is aborted if this threshold is exceeded. If the errors caused by the hardware alone are above 25% percent, Alice and Bob will not be able to detect an intercept-resend attack, and security cannot be guaranteed any more. If Eve employs more advanced methods of measuring, like positive operator-valued measures (POVM), she can increase her gathered amount of information per introduced disturbance [23]. A result is that the introduced error rate, at which the key transmission is insecure, is reduced to 15%.

5.2 Photon Number Splitting Attack

The security of the BB84 scheme is based on the fact that single quantum particles are used to transmit information. Unfortunately, the existing single photon sources are not in a state where it seems practical to use them for quantum cryptography systems which are supposed to be close to an application. In practice many implementations use weak coherent source to send the quantum states. In the photon number space, the state of a coherent light beam with intensity μ is

$$|\mu\rangle = e^{-\mu}\sum\frac{\mu^n}{n!}|n\rangle \quad (4)$$

Here, n is the photon number. The existing experiments set the intensity around μ = 0.1. This shows that the probability that a non-vacuum pulse contains 2 or more than 2 photons is larger than 5 %.

The fact, that there is a non-vanishing probability to have two or more photons in one pulse, gives rise to new eavesdropping strategy, the so-called photon number splitting attack (PNS attack). In this attack [22] Eve checks the number of photons in each pulse, without disturbing the polarization, a so-called quantum non-demolition measurement. Whenever there are two or more photons in one pulse, Eve keeps one of them in her quantum memory to analyze it after the bases have been announced. She sends the remaining photon(s) of the pulse to Bob, causing no errors. Since the eavesdropper doesn't cause any disturbance in the polarization, so Bob cannot recognize her in the usual way. This is quite a severe problem, because especially when the secret key is distilled from the sifted key, it is important to have a

good estimate of the information Eve has gathered. It has been shown that if average number of photons per pulse, m, is significantly less than 1, then the probability of an eavesdropper being able to split the pulse is approximately $m^2/2$ [2].

5.3 Man in the Middle Attack

Quantum cryptography is vulnerable to a man-in-the-middle attack when used without authentication to the same extent as any classical protocol, since no principle of quantum mechanics can distinguish friend from foe. As in the classical case, Alice and Bob cannot authenticate each other and establish a secure connection without some means of verifying each other's identities. If Alice and Bob 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 small amount of the new key to authenticate the next session. Several methods to create this initial shared secret have been proposed, for example using a third party [35] or chaos theory [19].

5.4 Optimal Attacks

The idea of this attack is that Eve lets a four-dimensional probe (i.e. two qubits) interact unitarily with the photon Alice has sent. She then waits until Alice and Bob announce the used basis, so that she can perform an optimized measurement on the stored probe, depending on the basis. A quantum circuit was proposed in [15], consisting of only two CNOT gates. When optimal individual attacks are taken into account, the key exchange has to be regarded as insecure at an error rate of opt ≥ 0.146 [15].

5.5 Quantum Cloning Attack

A more sophisticated eavesdropping strategy tries to make use of quantum cloning machines proposed by Gisin and Huttner [17]. They suggested using either a machine that they named “pretty good quantum copying machine” (PGQCM) or the universal quantum cloning machine (UQCM). The attack would look like this: Eve intercepts every photon, which Alice sends out and uses a cloning machine to end up with two photons. These have a certain fidelity F with respect to the photon, which Alice had sent. Eve keeps one of the photons in a so-called quantum memory and sends the other one to Bob. When the bases are announced during the sifting procedure, Eve can take her photons from the quantum memory and measure in the correct basis .Of course, she will have introduced errors. The probability that Bob will see an incorrect bit value is QCA =1−F. The fidelity of the PGQCM and the UQCM [17] are FPGQCM ≈ 0.825 and FUQCM ≈ 0.833 respectively, A quantum cloning attack with a universal quantum cloning machine introduces an error rate of QCA = 0.167.

The introduced error is lower than that of an intercept-resend strategy, but a universal quantum cloning machine is a difficult device and a quantum memory with a suitable capacity is also a problem. Eve’s information on the key is also lower than in the intercept- resend attack. Nevertheless, if Alice and Bob want to be secure against such an attack, they should discard the key if the error is QCA.

5.6 Hacking attacks

Hacking attacks target imperfections in the implementation of the protocol instead of the protocol directly. If the equipment used in quantum cryptography can be tampered with, it could be made to generate keys that were not secure using a random number generator attack. Another common class of attacks is the Trojan horse attack [33] which does not require physical access to the endpoints: rather than attempt to read Alice and Bob's single photons, Eve sends a large pulse of light back to Alice in between transmitted photons. Alice's equipment reflects some of Eve's light, revealing the state of Alice's polarizer. This attack is easy to avoid, for example using an optical isolator to prevent light from entering Alice's system, and all other hacking attacks can similarly be defeated by modifying the implementation. Apart from Trojan horse there are several other known attacks including faked state attacks [24], phase remapping attacks [16] and time-shift attacks [26].

5.7 Denial of service

Because currently a dedicated fibre optic line or line of sight in free space is required between the two points linked by quantum cryptography, a denial of service attack can be mounted by simply cutting or blocking the line or, perhaps more surreptitiously, by attempting to tap it.

6 Security Proofs

All good quantum key distribution protocols must be operable in the presence of noise that may or may not result from eavesdropping. The protocols must specify for which values of measurable parameters Alice and Bob can establish a secret key and provide a physically implementable procedure that generates such a key. The design of the procedure must take into account that an eavesdropper may have access to unlimited quantum

computing power. Taking all possibilities into account, along with the effects of realistic imperfections in Alice and Bob's apparatus and channel, has been difficult. A long series of partial results has appeared over the years, addressing restricted sets of strategies by Eve, but only in the past few years have complete proofs appeared.

One class of proofs, by Mayers [25] and subsequently by others, including Biham and collaborators [8] attacks the problem directly and use the complementary principle to prove the security of BB84 protocol. Another approach, by Lo and Chau [21] proves the security of a new QKD protocol that uses the idea of entanglement distillation. The two approaches have been unified by Shor and Preskill [30], who showed that a quantum error-correcting protocol could be modified to become BB84 without compromising its security. More recently, another simple proof of the BB84, which employs results from quantum communication complexity, has been provided by Ben-Or [7] and a general proof based on bounds on the performance of quantum memories has been proposed by Christandl et al. [10].

7 Implementations

QKD is an active experimental field. In fact companies, id Quantique, Geneva (http://idquantique.com), MagiQ Technologies, New York (http://magiqtech.com) and SmartQuantum, France (http://www.smartquantum.com) are already offering commercial quantum cryptography systems, based on the plug-and-play principle. Several other companies also have active research programmes, including Toshiba, HP, IBM, Mitsubishi and NEC. The first working prototype, constructed at IBM in Yorktown Heights, New York, transmitted quantum signals over 32 cm of open air [2]. So far the longest distance over which quantum key distribution has been demonstrated using optic fibre is 148.7 km, achieved by Los Alamos/NIST using the BB84 protocol [18]. Besides optic fibre QKD, a lot of research is going into free space QKD, as it avoids the need to have an optical fibre set up between the communicating parties. The current distance record for free space QKD is 144km between two of the Canary Islands, achieved by a European collaboration using entangled photons (the E91 protocol) in 2006 [32], and using a modified version of the BB84 protocol in 2007 [28]. The experiments suggest transmission to satellites is possible, due to the lower atmospheric density at higher altitudes, which would be of a big practical importance.

DARPA (Defense Advanced Research Projects Agency) has been running and actively developing a 10-node quantum network which includes a 25 km wireless link since 2004 in Massachusetts, USA. In 2004, the world's first bank transfer using quantum cryptography was carried in Vienna [27]. An important cheque, which needed absolute security, was transmitted from the Mayor of the city to an Austrian bank.

8 Challenges and Prospects

Despite the impressive improvements that have been made over the last couple of decades, there is still a long way to go before quantum cryptography will become widely used. The distance with which quantum cryptography is a practical solution must be increased to at least that of currently used systems. Quantum protocols must be incorporated into current network technologies, so that a more transparent use can be made of the technology, and by a wider group of users. However well the intrusion techniques may seem to work, unfortunately we do not currently have a great enough understanding of intrusion and detection techniques to confidently say the protocols are uncrackable. In order to be totally secure though, more extensive intrusion detection algorithms will be needed.

Admittedly, quantum cryptography is not very practical right now, it is still worthy of study for several reasons. Unlike public-key cryptosystems, it provides forward and provable security which will not be compromised with increase in computational speed, or even if P = NP. Currently it works only over short distances, but there are situations in which even short-distance transmission is useful. The concept of privacy amplification by public discussion can be extended to any situation in which Eve has partial knowledge of a string shared by Alice and Bob. In general, the differences between quantum cryptography and other cryptographic techniques are enough to motivate researchers to explore new ideas and techniques for wide spread use of quantum cryptosystem.

Acknowledgements

One of the authors (N L Gupta) is thankful to University Grants Commission, Govt. of India [25-231(12)/06 (TRF/CRO)] for providing financial assistance.

References

[1] Bell, J.S., "On the Einstien Podolsky Rosen paradox", *Physics* , 1,195-200 (1964).

[2] Bennet C.H., F. Bessette,G. Brassard, L.Salvail and J.Smolin, "Experimental quantum cryptography", *J. Cryptology* , 5, 3-28 (1992).

[3] Bennet C.H., G. Brassard and N.D. Mermin, "Quantum cryptography without Bell's theorm", *Phys. Rev. Lett.*, 68, 557-559 (1992).

[4] Bennet C.H., G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", *Proceedings of IEEE International Conference on Computers,Systems and Signal Processing*, Bangalore, India: IEEE, New York, 175-179 (1984).

[5] Bennet C.H., G.Brassard,C.Crepeau and U. Maurer, "Generalized privacy amplification", *IEEE trans. on Info. Theory* , 41, 1915-1923 (1995).

[6] Bennet, C.H. "Quantum cryptography using any two non-orthogonal states", *Phys. Rev. Lett.*, 68, 3121-3124 (1992).

[7] Ben-Or, M., "Simple security proof for quantum key distribution", On-line presentation available at http://www.msri.org/publications/ln/msri/2002/qip/ben-or/1/index.html (2002).

[8] Biham E., M. Boyer, P.O. Boykin, T. Mor and V. Roychowdhary, "A proof of the security of quantum key distribution", *STOC'00: Proceedings of the thirty-second annual ACM symposium on theory of computing*, ACM Press, New York, 715-724(2000).

[9] Bruss, D., "Optimal eavesdropping in quantum cryptography with six states", *Phys. Rev. Lett.*, 81, 3018-3021 (1998).

[10] Christandl M, R Renner and A Ekert, "A generic security proof for quantum key distribution", Online quant-ph/0402131 (2004).

[11] Clauser J.F., M.A.Horne, A.Shimony and R.A.Holt, "Proposed expeiment to test local hidden variable theories", *Phys. Rev. Lett.*, 23, 880-884 (1969).

[12] Deutsch D., A.Ekert, R.Jozsa, C.Macchiavello, S.Popescu and A. sanpera, "Quantum privacy amplification and the security of quantum cryptography over noisy channels", *Phys. Rev. Letters* , 77, 2818-2821 (1996).

[13] Ekert A.K., B.Huttner,G.Massimo Palma and A.Peres, "Eavesdropping on quantum cryptographical systems", *Phys. Rev. A*, 50, 1047-1056 (1994).

[14] Ekert, A.K., "Quantum Cryptography based on Bell's theorm", *Phys. Rev. Lett.*, 67, 661-663 (1991) .

[15] Fuchs C.A., N.Gisin, R.B.Griffiths, C.S.Niu and A. peres, "Optimal eavesdropping in quantum cryptography", *Phys. Rev. A* , 56, 1163-1176 (1997).

[16] Fung C.-H. F., B.Qi, K.Tamaki and H.-K. Lo , "Phase remapping attack in practical quantum key distribution systems", *Phy. Rev. A*, 75, 032314 (2007).

[17] Gisin N., B. Huttner, "Quantum cloning, eavesdropping and Bell's inequality", *Phys. Lett. A*, 228, 13-21 (1997) .

[18] Hiskett P.A., D. Rosenberg, C.G. Peterson, R.J. Hughes, S. Nam, A.E. Lita, A.J. Miller and J.E. Nordholt, "Long distance quantum key distribution in optical fibre", *New J. Phys.*, 8, 193 (2006).

[19] Huang D., Z.Chen, Y.Guo and M.Lee.,"Quantum secure direct communication based on chaos with authentication", *J. Phys. Soc. Jpn.*, 76, 124001, (2007).

[20] Kahn, D. *The Codebreakers: The Story of Secret Writing.* New York: Scribner, 1996.

[21] Lo H.-K. and H. F.Chau, "Unconditional security of quantum key distribution over arbitrary long distances", *Science* , 283, 2050-2056 (1999).

[22] Lutkenhaus, N, "Limitation on practical quantum cryptography", *Phys. Rev.Lett.*, 85, 1330-1333 (2000).

[23] Lutkenhaus, N, "Security against eavesdropping in quantum cryptography", *Phys. Rev. A*, 54, 97-111 (1996).

[24] Makarov V. and D.R. Hjelme, "Faked state attack on quantum cryptosystems", *J. Mod. Opt.*, 52, 691-705 (2005).

[25] Mayers, D., "Unconditional security in quantum cryptography", Online quant-ph/9802025 (1998).

[26] Qi B., C.-H. Fung, H.-K. Lo and X. ma, "Time shift attack in practical quantum cryptosystems", Quant. Info. Compu., 7, 73-82 (2007).

[27] Quantum Cryptography "live": WorldPremiere :Bank Transfer via Quantum Cryptography Based on Entangled Photons, Online press release available http://www.quantenkryptographie.at/QuantumCryptography 21 April 04.pdf.

[28] Schmitt-Manderbach T., et al., "Experimental demonstration of free space decoy state quantum key distribution over 144 km", *Phys. Rev. Lett.*, 98, 010504 (2007).

[29] Shannon, C. E., "Communication theory of secrecy systems", *Bell Syst. Tech. J.*, 28, 656-715 (1949).

[30] Shor P. and J.Preskill, "Simple proof of security of the BB84 quantum key distribution protocol", *Phys. Rev. Lett.*, 85, 441-444 (2000) .

[31] Shor, P., "Polynomial time algorithm for prime factorisation and discrete logarithms on a quantum computer", *SIAM J. Comput.*, 26, 1484-1509 (1997) .

[32] Ursin R, et al, "entanglement based quantum communication over 144 km", *Nature Physics*, 3, 481-486 (2007).

[33] Vakhitov A., V. Makarov and D. R.Hjelme, "Large pulse attack as a method of coventional optical eavesdroping in quantum cryptography", *J. Mod. Opt.*, 48, 2023-2038 (2001).

[34] Wotters W.K. and W.H.Zurek, "A single quantum state cannot be cloned", *Nature*, 299, no. 802-803 (1982).

[35] Zhang Z., J.Liu, D.Wang and S.Shi, "Quantum direct communication with authentication", *Phys. rev. A*, 75, 026301 (2007).