Security Aspect of Quantum Key Distribution

Anand Sharma
MITS,Lakshmangarh
Sikar,Rajasthan

Vibha Ojha
IITM,Gwalior
M.P.

Vishal Goar
ECB,Bikaner
Rajasthan

ABSTRACT
Is the newly born quantum cryptography the ultimate solution for information security? A technique needs to be both theoretically strong and practically viable. But quantum cryptography comes to naught in the latter. Unlike many of the classical cryptosystems in use today, whose security often draws on unproven assumptions about the computational complexity of mathematical problems, the security of quantum cryptography is based on—and employs—the laws of physics. The term "unconditional security"is used to emphasize the fact that it does not rely on the presumed, yet unproven hardness of somemathematical problem. In this Paper, we present the proof of the unconditional security of the BB84 protocol, as devised by Peter Shor and John Preskill [1].

Category and Subject Descriptor
Quantum Computing.

General Terms
Quantum Cryptography, BB84 Protocol.

Keywords
Qubit, Quntum Key Distribution, Security.

1.INTRODUCTION
Quantum cryptography uses quantum mechanics to guarantee secure communication. It enables two parties to produce a shared random bit string known only to them, which can be used as a key to encrypt and decrypt messages. An important and unique property of quantum cryptography is the ability of the two communicating users to detect the presence of any third party trying to gain knowledge of the key. This results from a fundamental part of quantum mechanics: the process of measuring a quantum system in general disturbs the system. A third party trying to eavesdrop on the key must in some way measure it, thus introducing detectable anomalies. By using quantum superpositions 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 key can be produced which is guaranteed as secure, otherwise no secure key is possible and communication is aborted.

The security of quantum cryptography relies on the foundations of quantum mechanics, in contrast to traditional public key cryptography which relies on the computational difficulty of certain mathematical functions, and cannot provide any indication of eavesdropping or guarantee of key security. Quantum cryptography is only used to produce and distribute a key, not to transmit any message data. This key can then be used with any chosen encryption algorithm to encrypt and decrypt a message, which can then be transmitted over a standard communication channel. The algorithm most commonly associated with QKD is the one-time pad, as it is provably secure when used with a secret, random key.

2. QUANTUM CRYPTOGRAPHY
Rather than depending on the complexity of factoring large numbers, quantum cryptography is based on the fundamental and unchanging principles of quantum mechanics. In fact, quantum cryptography rests on two pillars of 20th century quantum mechanics –the Heisenberg Uncertainty principle and the principle of photon polarization. According the Heisenberg Uncertainty principle, it is not possible to measure the quantum state of any system without disturbing that system. Thus, the polarization of a photon or light particle can only be known at the point when it is measured. This principle plays a critical role in thwarting the attempts of eavesdroppers in a cryptosystem based on quantum cryptography. Secondly, the photon polarization principle describes how light photons can be oriented or polarized in specific directions. Moreover, a polarized photon can only be detected by a photon filter with the correct polarization or else the photon will be destroyed. It is this "one-way-ness" of photons along with the Heisenberg Uncertainty principle that make quantum cryptography an attractive option for ensuring the privacy of data and defeating eavesdroppers. Charles H. Bennet and Gilles Brassard developed the concept of quantum cryptography in 1984 as part of a study between physics and information. Bennet and Brassad stated that an encryptionkey could be created depending on the amount of photons reaching a recipient and how theywere received. Their belief corresponds to the fact that light can behave with the characteristics of particles in addition to light waves. These photons can be polarized at various orientations, and these orientations can be used to represent bits encompassing ones and zeros. These bits can be used as a reliable method of forming onetime pads and support systems like PKI by delivering keys in a secure fashion. The representation of bits through polarized photons is the foundation of quantum cryptography that serves as the underlying principle of quantum key distribution.
Thus, while the strength of modern digital cryptography is dependent on the computational difficulty of factoring large numbers, quantum cryptography is completely dependent on the rules of physics and is also independent of the processing power of current computing

systems.Since the principle of physics will always hold true, quantum cryptography provides an answerto the uncertainty problem that current cryptography suffers from; it is no longer necessary to make assumptions about the computing power of malicious attackers or the development of a theorem to quickly solve the large integer factorization problem.

3. QUANTUM KEY DISTRIBUTION

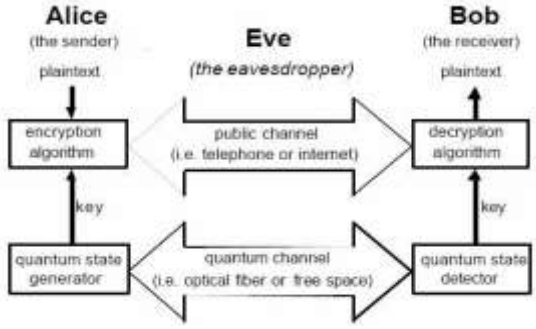

Fig 1 Quantum Key Distribution

The following is an example of how quantum cryptography can be used to securely distribute keys. This example includes a sender, "Alice", a receiver, "Bob", and a malicious eavesdropper, "Eve".

Alice begins by sending a message to Bob using a photon gun to send a stream of photons randomly chosen in one of four polarizations that correspond to vertical, horizontal or diagonal in opposing directions (0,45,90 or 135 degrees). For each individual photon, Bob will randomly choose a filter and use a photon receiver to count and measure the polarization which is either rectilinear (0 or 90 degrees) or diagonal (45 or 135 degrees), and keep a log of the results based on which measurements were correct vis-à-vis the polarizations that Alice selected. While a portion of the stream of photons will disintegrate over the distance of the link, only a pre-determined portion is required to build a key sequence for a onetime pad. Next, using an out-of-band communication system, Bob will inform Alice to the type of measurement made and which measurements were of the correct type without mentioning the actual results. The photons that were incorrectly measured will be discarded, while the correctly measured photons are translated into bits based on their polarization. These photons are used to form the basis of a onetime pad for sending encrypted information. It is important to point out that neither Alice nor Bob are able to determine what the key will be in advance because the key is the product of both their random choices. Thus, quantum cryptography enables the distribution of a one-time key exchanged securely.

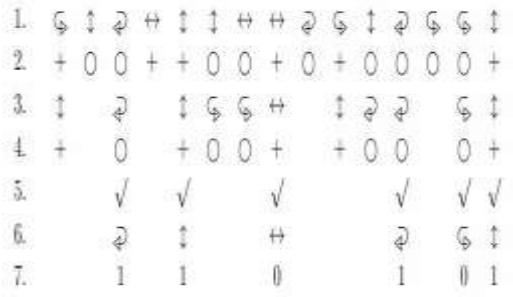

Fig 2 Basic QKD Protool

1. Alice sends a random sequence of photons polarized horizontal (↕), vertical (↔), right-circular (↻) and left-circular (↺);
2. Bob measure the photon's polarization in a random sequence of bases, rectilinear (+) and circular (O);
3. Results of bob's measurements (some photons may not be received at all);
4. Bob tells Alice which basis he used for each photon he received;
5. Alice tells him which bases were correct;
6. Alice and Bob keep only the data from these correctly-measured photons, discarding all the rest;
7. This data is interpreted as a binary sequence according to the coding scheme ↔ = ↻ = O and ↕ = ↺ = 1.

Now let us suppose that a malicious attacker attempts to infiltrate the cryptosystem and defeat the quantum key distribution mechanisms. If this malicious attacker, named Eave, tries to eavesdrop, she too must also randomly select either a rectilinear or diagonal filter to measure each of Alice's photons.

Hence, Eve will have an equal chance of selecting the right and wrong filter, and will not be able to confirm with Alice the type of filter used. Even if Eve is able to successfully eavesdrop while Bob confirms with Alice the protons he received, this information will be of little use to Eve unless she knows the correct polarization of each particular photon. As a result, Eve will not correctly interpret the photons that form the final key, and she will not be able to render a meaningful key and thus be thwarted in her endeavors. In sum, there are three significant advantages of this system. First, the Heisenburg Uncertainty principle means that information regarding photons cannot be duplicated because photons will be destroyed once they are measured or tampered with. Since photons are indivisible, once it hits a detector, the photon no longer exists. Secondly, Alice and Bob must calculate beforehand the amount of photons needed to form the encryption key so that the length of the one-time pad will correspond to the length of the message. Since mathematically Bob should receive about 25 percent of transmitted photons, if there is a deviation for the pre-determined fixed number, Bob can be certain that traffic is being sniffed or something is wrong in the system. This is the result of the fact that if Eve detects a photon, it will no longer exist to be detected by Bob due to Eve's inability to copy an unknown quantum state. If Eve attempts to create and pass on to Bob a photon, she will have to randomly choose its orientation, and on average be incorrect about 50 percent of the time –enough of an error rate to reveal her presence.

4. SECURITY IN QKD

We divide the proof into three parts:

• In the first part, we present the so-called *entanglement-based* version of the BB84 protocol. In contrast, the scheme presented in the previous section is called a *prepare-and-measure scheme*, for obvious reasons. In the entanglement-based version, Alice and Bob's aim is to

share a special entangled state that allows them to obtain perfectly correlated bits upon measuring their half of the state. We will see how they can construct such a state, how they can check whether they were successful, and how they can detect Eve's attempted attack.

• In the second part, we will show that the equivalent entanglement-based version is secure. In contrast to earlier work by Shor and Preskill [1], which is based on a proof by Lo and Chau [2], we use the *universally composable* definition of unconditional security [3]. This general security definition refers to the overall cryptosystem, with any number of subprotocols, including the quantum and the classical stages.

• In the third part, we show that the two schemes are equivalent indeed.

4.1 The Entanglement-Based Version of BB84

The entanglement-based version of the BB84 protocol that we now present is similar to the protocol introduced by Ekert [4] and follows ideas of Bennett et al. [5]. In this version of the protocol, Alice and Bob aim at creating a special entangled state.

Where Alice holds the first particle and Bob holds the second one. An important property of this state is that it has the same form in the rectilinear (+) and circular (O). This means that Alice's and Bob's measurement results are completely correlated whenever they measure the state in one of those bases. (Moreover, their results are random.) Since the state is pure, it cannot be entangled with anything else, in particular not with anything under Eve's control. Thus, whenever Alice and Bob are sure they share a state, they know that (a) measuring in the same basis generates a shared random bit, and (b) Eve has no knowledge about this bit. To generate the whole key, Alice and Bob prepare a large number of these states, and measure each qubit separately.

We will now show how they can achieve this.

We need to take a brief detour to quantum error correction first. In contrast to a classical bit, a qubit can undergo three different errors: bit flips, phase errors, and combinations of these two:

• When a bit flip occurs, the state rectilinear (+) becomes circular (O), and vice versa. This error is described by the Pauli matrix.

• Phase errors transform the state (↻) into (↺), but leave rectilinear (+) unchanged. Such an error is described by the Pauli matrix

• Both these errors can also occur combined. For example, changing (↕) to (↺) and (↻) to (↔).

Let us now recall some elements of classical error correction. A (classical) linear [*n, k*] code C that encodes *k* bits of information by an *n* bit string is a set of 2^k codewords. Each codeword is an *n*-dimensional binary vector. The whole code can be described by an ($n \times k$)-dimensional generator matrix G that maps each message *x* to the encoded message G*x*. Thus, the set of all possible codewords is the vector space that is spanned by the columns of G. We require those vectors to be linearly independent. Error correction for linear codes can be easily described by means of the parity check matrix H. This is an ($(n-k) \times n$) matrix with the property that H*x* = 0 for all codewords *x*.

Suppose now that a message *x* is encoded as *y* = G*x* . Due to an error e, one obtains *y*' = *y*+*e*. Since we have H*y* = 0 for all codewords, it follows that H*y*' = H*e*, which is called the *(error) syndrome.* Thus, if the syndrome is 0, no error has occurred. Otherwise, H is constructed such that the syndrome contains information about the error that should make it possible to correct it.

Finally, we introduce the concept of *duality*: Let C be a linear [*n, k*] code with generator matrix G and parity check matrix H. Then we can define the dual code $C^{\perp}$ of C, which is the set of all codewords that are orthogonal to each codeword in C. The dual code $C^{\perp}$ is an [$n - k, n$] code which is generated by H^T and has a parity check matrix G^T . Dual codes play an important role in the construction of CSS codes.

We have now collected all the ingredients to describe the entanglement-based version of the BB84 protocol:

1. Alice creates 2*n* qubit pairs.
2. She randomly selects *n* of those qubits which will later serve as check qubits.
3. Alice selects a random 2*n* bit string b and applies the Hadamard transformation to her half of each qubit pair whenever the corresponding bit of b is "1."
4. She sends the other half of all qubit pairs to Bob.
5. Alice announces b and which qubits are to serve as check qubits.
6. Bob performs a Hadamard transformation on those of his qubits where b is "1."
7. Alice and Bob measure the check qubits in the rectilinear (+) and circular (O). basis to estimate the error rate. If more than *l* results differ, they abort the protocol.
8. For the remaining qubits, Alice and Bob measure the syndromes for the codes C1 and C2, and correct the errors.
9. They measure this state in the rectilinear (+) and circular (O) basis to obtain a shared secret key.

The point of performing the Hadamard transformation on half of the qubits is that this operation effectively changes the basis, in which the qubits are prepared, from {(↕),(↻)} to { (↔),(↺)}.

This is necessary because if Eve knew the basis, she could launch the intercept-resend attack presented in the previous section and break the protocol.

4.2 Security of the Entanglement-Based Version

Up to this point, we often used the term "security" without providing a rigorous definition. In this section, we will make up for this. Additionally, we need to provide a mathematical framework to cover *all* possible eavesdropping strategies, in particular those where the adversary stores a quantum system that contains information about the classical bit strings obtained by Alice and Bob upon measuring their quantum states. Such a situation, where a quantum system is correlated with classical data, can be described by so-called *classical-quantum states* (cq-states, for short).

In the ideal case, Alice's and Bob's keys are identical and uniformly distributed, i.e., each possiblekey occurs with equal probability. Moreover, the state of Eve's quantum system should be completely independent of the

key.We can now prove the unconditional security of the entanglement-based version of the BB84protocol. Recall that the aim of this protocol is to distribute the state rectilinear (+) and circular (O). In the real world, Alice and Bob are of course not able to *exactly* achieve this; rather, at the end of the protocol, they will hold a state, which hopefully is very similar to previous one. The "distance" to a pure state is measured by means of the so-called *fidelity*, which is defined as F. If F = 1, the two states are identical. Since we do not make any restrictions about the eavesdropper's strategy, we consider the worst case in which Eve holds a purifying system of state This scenario corresponds to the case where the adversary has full control over the quantum channel.

To summarize, we have shown that by random sampling the fidelity of the state shared by Alice and Bob can be lower-bounded, with an exponentially small probability of error. Moreover, this bound directly defines how secure a key generated by measuring this state will be.

4.3 Equivalence of the Two Schemes

We prove the equivalence of the entanglement-based and prepare-and-measure versions of the BB84 protocol by successive simplifications. Each step is very simple, so it is easy to verify that the security of the protocol is not compromised.

A major simplification is that all measurements done by Alice after transmitting the particles can already be done at the very beginning: If Alice measures her part of the state rectilinear (+) , she obtains a random bit as a result, but on the other hand, Bob's part of the state collapses onto the correlated state (↕) or (↻). Thus, instead of sending entangled qubits for the check, Alice can as well prepare single qubits randomly in one of the states (↕) or (↻) , and send those states to Bob.

Of course, it is crucial for the security of the protocol that Eve does not know *a priori* which qubits will serve as check qubits and which as "key qubits"; otherwise, she could treat them differently and thus fudge the error estimation.

Another measurement Alice can do at the beginning is the measurement of her syndrome and her key qubits. This is not very obvious, so let us give some more detail: Given a CSS code CSS(C1,C2), we can define a family of equivalent codes CSS$_{v,w}$(C1,C2), in the sense that they have the same error correcting properties.

As an intermediate result, we rephrase the entanglement-based protocol including all simplifications
introduced so far:

1. Alice creates n random check qubits, each in the state rectilinear (+) and circular (O), a random n bit string k, which will serve as the key, and two random n bit strings v and w. She prepares the state according to k and encodes it using CSS$_{v,w}$(C1,C2).
2. She randomly selects n positions for the check qubits and puts the encoded qubits in the remaining positions.
3. Alice selects a random $2n$ bit string b and applies the Hadamard transformation to her half of
each qubit pair where b is "1."
4. She sends the other half of all qubit pairs to Bob.
5. Alice announces b, v, and w, and which qubits are to serve as check qubits.
6. Bob performs a Hadamard transformation on those of his qubits where b is "1."
7. Bob measures the check qubits in the {(↕),(↻)} basis. If he finds more than l results that disagree with Alice's prepared states, they abort the protocol.
8. Bob decodes the key qubits from CSS$_{v,w}$(C1,C2) and obtains the state of k.
9. He measures the state of k in the {(↕),(↻)} basis and obtains the key k as the result.

We will now simplify this protocol even further: Note that in the original version, Alice and Bob do not care whether they shared the state rectilinear (+) becomes circular (O) because measuring both states provides them with correlated, random bits; the relative phase is irrelevant. Thus, it is unnecessary to send the phase correction information v to Bob. This is why CSS codes are used:

They decouple the bit flip error correction from the phase error correction. If now Bob were to measure his key qubits before the decoding, he would obtain $x_k + y + w + e$, where e denotes the bit errors that occurred during the transmission (or that were introduced by Eve). He can now classically decode this bit string by subtracting w, which was announced by Alice, and correct it to the codeword $x_k + y$, if e did not introduce too many errors. Bob finds the key by computing the coset to which $x_k + y$ belongs.

The whole protocol so far looks as follows:

1. Alice creates $2n$ random qubits, each in the state rectilinear (+) and circular (O), and a random codeword $x_k \in C_1$.
2. She randomly selects n positions to be check qubits and the remaining n positions to define the key qubits.
3. Alice selects a random $2n$ bit string b and applies the Hadamard transformation to her half of
each qubit pair where b is "1."
4. She sends the other half of all qubit pairs to Bob.
5. Alice announces b and $y - x_k$, and which qubits are to serve as check qubits.
6. Bob performs a Hadamard transformation on those of his qubits where b is "1."
7. Bob measures the check qubits in the {(↕),(↻)}basis. If he finds more than l results that disagree with Alice's prepared state, they abort the protocol.
8. Bob measures the key qubits and gets $y + e$, subtracts $y - x_k$, and corrects $x_k + e$ to x_k.
9. He calculates the coset to which x_k belongs to get the key k.

Finally, we can remove the Hadamard transformation, and let Alice choose randomly one of the four states in {(↕),(↻), (↔),(↺)}Then Bob, instead of waiting for b to be announced, simply chooses one basis at random and measures the arriving qubits. As he will choose the wrong basis in roughly half the cases, Alice should double the number of input qubits to $4n$. After his measurement, Alice announces which basis she used and both discard all instances where they used a different basis. With this last modification, we finally arrived at the prepare-and-measure version of the BB84 protocol, only up to some small twists.

5. CONCLUSION

While there have been substantial advancements in the field of quantum cryptography in the last decade, there are still challenges ahead before quantum cryptography can become a widely deployed key distribution system for governments, businesses, and individual citizens. Namely, these challenges include developing more advanced hardware to enable higher quality and longer transmission distances for quantum key exchange. The security of quantum key distribution relies on the inviolable laws of quantum mechanics: nonorthogonal quantum states are used as signal states in the BB84 protocol. The impossibility of perfect cloning of nonorthogonal states implies the security of this protocol. In the security proof for the BB84 protocol, we have employed an equivalent entanglementbased protocol. The main idea is that local measurements on a maximally entangled state, shared by Alice and Bob, have perfectly correlated outcomes that can be used as the key. A maximally entangled state is necessarily pure, and a pure state cannot be entangled with an eavesdropper's state—thus Eve cannot learn anything about the key. The idea for quantum cryptography with entangled states goes back to Artur Ekert [4], who suggested to confirm the existence of quantum correlations in the state of Alice and Bob by a Bell inequality test.

However, the advances in computer processing power and the threat of obsolescence for today's cryptography systems will remain a driving force in the continued research and development of quantum cryptography. In fact, in is expected that nearly $50 million of both public and private funds will be invested in quantum cryptography technology over the next three years3. Quantum cryptography is still in its infancy and so far looks very promising. This technology has the potential to make a valuable contribution to e-commerce andbusiness security, personal security, and security among government organizations. 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. ACKNOWLEDGMENTS

We express our profound gratitude to all faculty members of MITS Lakshmangarh, and ECB, Bikaner at all the times to help us and whose critical suggestions, discussions and guidance can not be valued in words to the logical conclusion of this work. Again with a profound sense of gratitude, we record our indebtedness to all the colleagues. The nurturing and blossoming of the present work was mainly due to their valuable guidance, astute udgment, constructive criticism and an eye for perfection, Without their overwhelming interest, the present workwould not have seen the light of the day. finally we express our gratitude to our parents for their support and wishes.

7. REFERENCES

[1] P. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 85:441–444, 2000.

[2] H. Lo and H. Chau. Unconditional security of quantum key distribution over arbitrarilylong distances. *Science*, 283:2050–2056, 1999.

[3] M. Ben-Or, M. Horodecki, D. Leung, D. Mayers, and J. Oppenheim. The universal composable security of quantum key distribution. In J. Kilian, editor, *Proceedings of the Second Theory of Cryptography Conference*, pages 386–406. Springer- Verlag *Lecture Notes in Computer Science #3378*, February 2005. Also available at http://arxiv.org/abs/quant- ph/0409078.

[4] A. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67:661– 663, 1991.

[5] C. Bennett, G. Brassard, and D. Mermin. Quantum cryptography without Bell's theorem. *Physical Review Letters*, 68:557–559, 1992.

[6] M. Ajtai and C. Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In *Proceedings of the 29th ACM Symposium on Theory of Computing*, pages 284–293. ACM Press, 1997.

[7] E. Allender and R. Rubinstein. P-printable sets. *SIAM Journal on Computing*, 17(6):1193–1202, 1988.

[8] C. 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*, pages 175–179. IEEE Press, 1984.

[9] D. Bouwmeester, A. Ekert, and A. Zeilinger. *The Physics of Quantum Information*.Springer-Verlag, 2000.

[10] W. Hwang. Quantum key distribution with high loss: Toward global secure communication. *Physical Review Letters*, 91:057901, 2003.

[11] H. Inamori, N. L¨utkenhaus, and D. Mayers. Unconditional security of practical quantum key distribution. Technical Report quant-ph/0107017, Computing Research Repository (CoRR), 2001. Available on-line at http://arxiv.org/abs/quant-ph/0107017.

[12] A. Kent. Unconditionally secure bit commitment.*Physical Review Letters*,83:1447–1450, 1999.

[13] A. Kawachi, H. Kobayashi, T. Koshiba, and R. Putra. Universal test for quantum oneway permutations. *Theoretical Computer Science*, 345:370–385, 2005.

[14] K. Ko. On some natural complete operators. *TheoreticalComputerScience*,37(1):1–30,1985.

[15] R. K¨onig, R. Renner, A. Bariska, and U. Maurer. Locking of accessible information and implications for the security of quantum cryptography. Technica lReport quantph/0512021v2, Computing Research Repository (CoRR), 2006. Available on line athttp://arxiv.org/abs/quant-ph/0512021.

[16] D. Bruß and C. Macchiavello. Optimal eavesdropping in cryptography with threedimensional quantum states. *Physical Review Letters*, 88:127901(1)–127901(4), 2002.