International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 1 (2015) pp. 925-935

http://www.ripublication.com

Passive Attack Resistive Key Distribution Scenario: QKD

V. Muni Sekhar[I] , CH. Sravan Kumar[II] and Dr. KVG Rao[III], Dr. N Sambasiva Rao[IV]

Assistant Professor [I,II], Professor [III,IV]
Dept. of Computer Science and Engineering [I,II,III,IV]
Vardhaman College of Engineering, Hyderabad, India [I& II]
GNITS, Shaikpet , Hyderabad, India [III]
SREC, Warangal, India[IV]
chakralasravan@gmail.com[II],munisek@gmail.com[I]

Abstract

It has been widely recognized that the underlying principles of quantum mechanics could be used to enable secure communications, with some additional conventional cryptographic systems, while utilizing the properties of the photons. Many researchers are proposed several algorithms all of them should require an encryption system at sender end and decryption system at receiver end, but all are vulnerable to passive attack prevention. Considerable research efforts have been investigated to develop an efficient Quantum Key Distribution (QKD) scenario and passive attack Resistive scheme.

In this paper we are realizing the key distribution scenarios using quantum cryptography and compare with the existing key distribution scenarios. Here, we make use of photon uncertainty behavior.

Index Terms— Key Distribution, Quantum Cryptography, Passive attacks and Secure Communication

I. INTRODUCTION

As information systems become even more pervasive and essential to the conduct of daily affair in an organization or government or individuals. Accordingly, several aspects of information systems are facing ruthless security challenges in System security or Application security and Network security. To mitigate the security challenges several pre-existing techniques are there among that cryptography is the one of the solution to this problem. The major objective of cryptographic system is to

encrypt the message they send, with the goal of keeping anyone who is eavesdropping on the channel from being able to read the content of the message. In this, the sender applies an encryption functions to the original plain text message, resulting cipher text message is sent over the network, and the receiver applies a reverse function known as decryption to recover plaintext. There are two types of cryptographic systems that exists, they are a). Symmetric key cryptography (only one key is used between sender and receiver called secrete key or shared key). b). Asymmetric key cryptography (their sender and receiver will have two keys called as public and private key. Public key is known to all and private key is known by him/her). The encryption and decryption process shown in figure.1generally depends on key between sender and receiver. When a suitable combination of key and an encryption algorithm is used, it is difficult for an eavesdropper to break the ciphertext and sender and receiver can rest assured that their communication is secured.

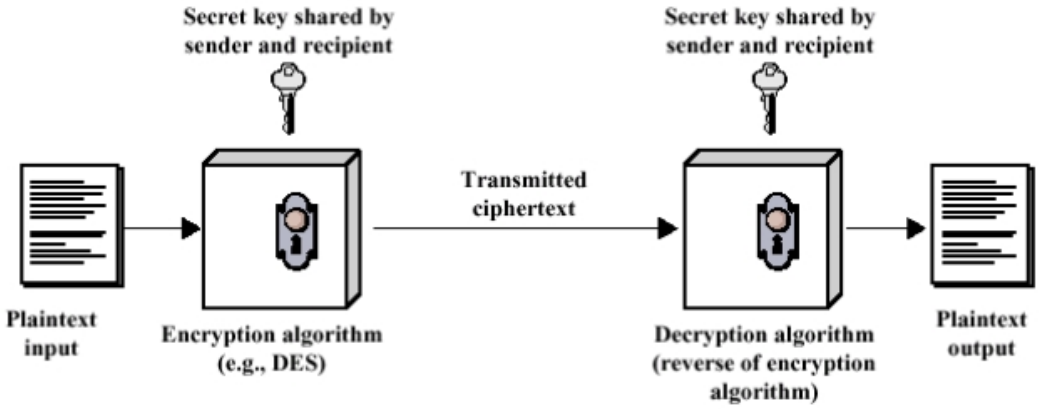

Fig. 1 ENCRYPTION AND DECRYPTION PROCESS

Various key distributions protocols are used to facilitate sharing secrete keys or public keys between users on communication networks. There are two types of key distribution protocols that are exists, they are a) Two party key distribution protocols and b) Third party key distribution protocols as shown in figure. 2. By using these shared keys, secure communication is possible on unsecured public networks. It consists of following problems in key distribution, they are a) Malicious attacker may derive the shared key from the key distribution process and b) A legitimate participant cannot ensure that the received shared key is correct or fresh and legitimate participant cannot confirm the identity of the other participant.

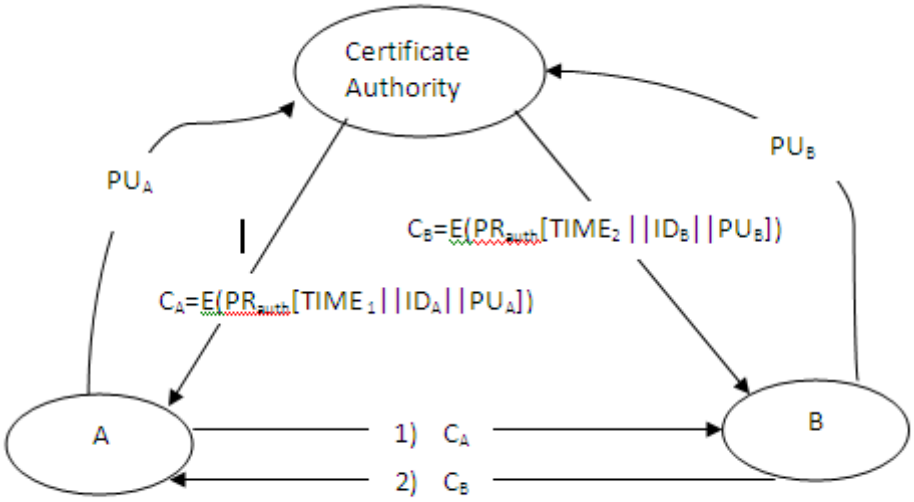

Fig. 2 PUBLIC KEY DISTRIBUTION

II. CLASSICAL CRYPTOGRAPHY

In classical cryptography, such as Diffie-Hellman [1] and third party key distribution protocols [2] utilize challenge response mechanisms or timestamp to prevent replay attacks. However, challenge response mechanisms require at least two communication rounds between the trusted third party and participants, and the timestamp approach needs the assumption of clock synchronization which is not practical in distributed systems (due to unpredictable nature of network delays and potential hostile attacks). Furthermore, classical cryptography cannot detect the existence of passive attacks such as eavesdropping. On the contrary, a quantum channel eliminates eavesdropping and replay attacks. This fact can be used to reduce the number of rounds of other protocols based on challenge response mechanism to a trusted third party.

A. Diffie-Hellman[1]

Two participant A and B can exchange secrete key using Diffie-Hellman key exchange protocol. Here, two publicly known numbers: a prime number ‘q’ and ‘α’ an integer that is primitive root of ‘q’. Suppose user ‘A’ and ‘B’ want to exchange secrete key. The sequence of steps for a shared key distribution between ‘A’ and ‘B’ is as follows:

	USER A	**USER B**
1.	User A selects a random integer $X_A < q$	User B selects a random integer $X_B < q$
2.	Compute $Y_A = \alpha^{X_A} mod\ q$	Compute $Y_B = \alpha^{X_B} mod\ q$
3.	Send Y_A to user *B*.	Send Y_B to user *A*.
4.	Compute $K = Y_B^{X_A} mod\ q$	Compute $K = Y_A^{X_B} mod\ q$

B. Third Party Key Distribution Protocols[2]

Let us assume that the user 'A' wishes to establish a logical connection with user 'B' and requires one time session key to protect data transmitted over the connection. User 'A' has master key 'K_A' known to only itself and KDC. Similarly, user 'B' has master key 'K_B' known to only itself and KDC. The process of exchanging the keys as shown in figure.3.

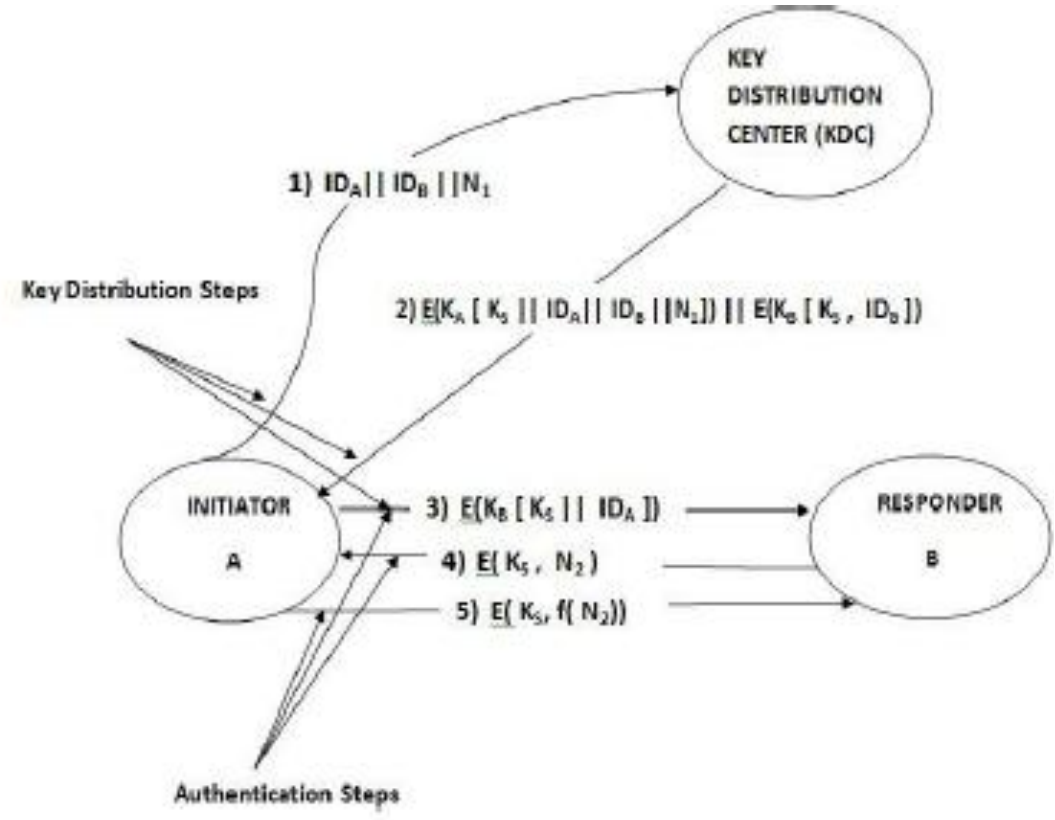

Fig. 3 SESSION KEY DISTRIBUTION SCENARIO

Above two scenarios detecting eavesdropping and Man-In-the-Middle attacks are highly difficult. Because, anonymity nature of the participants. To mitigate such attacks, we need to introduce network sensitive cryptographic systems.

III. QUANTUM KEY CRYPTOGRAPHY

Quantum cryptography is attracting much attention as solution of the problem of Key distribution. Quantum key agreement protocols provide security using laws of quantum physics [3]. This is great advantage, when all the classical key agreement techniques over public channels have been based on unproven mathematical assumptions [4]. A quantum key agreement protocol was first proposed by Bennett and Brassard [5] (BB84). In BB84, Alice generates a random string of bits and sends each

bit to Bob as a photon in a randomly chosen basis (rectilinear or diagonal). Bob, not knowing which of the two bases each photon is in, measures them randomly in rectilinear or diagonal basis. After measuring all the photons, Bob discloses his choice of bases of measurement to Alice and she tells Bob which of their bases agree. The final key is made up of bits that were received by Bob in the matching bases. A subset of these bits is used to check if there was any eavesdropping. Here, disclosure of bases is done over a classical communication channel.

Ekert [6] proposed the use of entangled photons measured randomly in three coplanar axes. While Ekert's protocol used Bell's inequality to demonstrate its security against eavesdropping, Bennett, Brassard and Mermin [7] proposed a protocol that used entangled pairs and did not depend on Bell's inequality for detection of eavesdropping. Bennett [8] in another scheme showed that any two non-orthogonal states suffice for key agreement. A protocol by Kartalopoulus[9] used two quantum channels for key agreement in conjunction with a classical channel. In his protocol, Alice sends same information on both the quantum channels and Bob measures the photons on these channels, randomly, in complementary bases (rectilinear on one and diagonal on other). They compare their chosen bases publicly and Bob retrieves the key.

In quantum cryptography, Quantum Key Distribution Protocols (QKDPs) employ quantum mechanisms to distribute session keys and public discussions to check for eavesdroppers and verify the corrective of a session key.

A. QKDPs Contributions

By integrating the advantages of both classical and quantum cryptography, this work present 2 QKDPs with following contributions:

i. Man-in-the-Middle attacks can be prevented, eavesdropping can be detected, and reply attacks can be avoided easily.
ii. User authentication and session key verification can be accomplished in one step without public discussions between sender and receiver.
iii. The secret key pre shared by Third Party and user can be long term which is repeatedly used.

The proposed schemes are first probably secure QKDPs under the random oracle model.

IV. QUANTUM KEY DISTRIBUTION PROTOCOLS

Many of QKD protocols have been proposed all have similarities. The legitimate communicators known as Alice and Bob communicate over a public channel in following phases. Step 1 is dedicated to raw key extraction, step 2 to error estimation, step 3 to checking eavesdropping, step 4 to reconciliation, i.e., to reconciled key extraction, and step 5 to privacy amplification, i.e., extraction of final secret key.

A. QUANTUM KEY DISTRIBUTION PROTOCOLS

Step 1: Quantum transmission over quantum communication channel.

The communicators set up a quantum channel, then they transmit quantum states (Qubits) over the quantum channel. It is noted that the transmission model is different for different QKD protocol. Two typical transmission are BB84 protocol and EPR protocol. The former transmits non-commute quantum states, and the latter transmits one of each EPR pairs

Step 2. Extraction of raw key over a public channel

After Alice and Bob obtain what is call the raw data by the quantum transmission, the raw data must be sifted because it consists of those bits which Bob either did not receive at all or did not correctly measure in the basis used to transmit them. Such non-receptions" could be caused by Eve's intrusion or by dark counts in Bob's detecting device. The locations of the dark counts are, of course, communicated by Bob to Alice over the public channel. By comparison publicly the basis between Alice and Bob, the data sifting procedure is completed.

Step 3. Check of eavesdropper

This step depends on the di_erent QKD protocols. In BB84 protocol, Alice and Bob now use the public channel to estimate the error rate in raw key. They publicly select and agree upon a random sample of raw key, publicly compare these bits to obtain an estimate R of the error-rate. These revealed bits are discarded from raw key. If R exceeds a certain threshold $RMax$, then it will be impossible for Alice and Bob to arrive at a common secret key. If so, Alice and Bob return to stage 1 to start over. On the other hand, If the error estimate R does not exceed $RMax$, then Alice and Bob move onto phase 3. In EPR protocol, one may use the correction of EPR pairs to check eavesdropping.

Step 4. Extraction of reconciled key

In step 2, Alice and Bob's objective is to remove all errors from what remains of raw *6* key to produce an error free common key, called reconciled key. This phase is of course called reconciliation, and takes place in two stage.

In stage 1, Alice and Bob publicly agree upon a random permutation, and apply it to what remains of their respective raw keys. Next Alice and Bob partition the remnant raw key into blocks of length l, where the length l chosen so that blocks of this length are unlikely to contain more than one error. For each of these blocks, Alice and Bob publicly compare overall parity checks, making sure each time to discard the last bit of the compared block. Each time a overall parity check does not agree, Alice and Bob initiate a binary search for the error, i.e., bisecting the block into two subblocks, publicly comparing the parities for each of these subblocks, discarding the right most bit of each subblock. They continue their bisective search on the subblock for which their parities are not in agreement. This bisective search continues until the erroneous bit is located and deleted. They then continue to the next l- block.

Stage 1 is repeated, i.e., a random permutation is chosen, remnant raw key is partitioned into blocks of length *l* parities are compared, etc. This is done until it becomes inefficient to continue in this fashion.

Alice and Bob then move to stage 2 by using a more refined reconciliation procedure. They publicly select randomly chosen subsets of remnant raw key, publicly compare parities, each time discarding an agreed upon bit from their chosen key sample. If parity should not agree, they employ the binary search strategy of step 1 to locate and delete the error.

Finally, when, for some fixed number *N* of consecutive repetitions of stage 2, no error is found, Alice and Bob assume that to a very high probability, the remnant raw key is without error. Alice and Bob now rename the remnant raw key reconciled key, and move on to the final and last phase of their communication.

Step 5. Privacy amplification

Alice and Bob now have a common reconciled key which they know is only partially secret from Eve. They now begin the process of privacy amplification, which is the extraction of a secret key from a partially secret one [12].

Table.1 PHOTON POLARIZATION

Polarization	Symbol	Photon	
Rectilinear	+	→	↑
Diagonal	**X**	↖	↗

Table.2 PHOTON TRANSMITTION

Bits	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Random Bits	0	1	1	1	0	1	1	0
Shared Key	X	+	+	X	X	X	+	+
Polarization at sender	\	|	|	/	\	/	|	-
Shared Key	X	+	+	X	X	X	+	+
Polarization at Reciever	\	|	|	/	\	/	|	-
Decrypted Bits	0	1	1	1	0	1	1	0

B. THE DRAWBACK OF PREVIOUS QKD PROTOCOLS

Obviously, the above procedure is based on the legitimate users, referred to as Alice and Bob. However, the practical existence of impersonation of Alice or Bob by eavesdropper, make us have to take some action to against the eavesdropper, an efficient way is to verify the communicators' identity. Unfortunately, there is no known way to initiate authentication without initially exchanging secret key over a secure communication channel in previous protocols.

In fact, quantum key distribution protocol is completely insecurity under the Man-in-the-Middle attack. When Alice communicates Bob, Eve intercepts all qubit

sent by Alice, and communicates Bob with impersonating Alice. Finally, Eve obtains two keys K_{AE} , K_{EB}, where K_{AE} represents the secret key between Alice and Eve, and *KAE* represents the secret key between Bob and Eve. As a result Eve can easily decrypt the ciphertext sent by Alice or Bob.

Of course, Alice and Bob may use the classic (where `classic' contraposes quantum) authentication technology to prove the legitimated identity. However, because Alice and Bob cannot simultaneously complete the identity verification and quantum key distribution, Eve may avoid the authentication procedure. So, practically, QKD protocol with identity verification is necessary. In the follows, we improve the previous quantum key distribution scheme to guarantee the security of quantum key for truly legitimate users.

V. IMPLEMENTATION OF QUANTUM KEY DISTRIBUTION PROTOCOL

Assume that Alice wishes to send Bob, over a public channel, a random bit string of length n to be used as a one-time pad. We assume that Alice and Bob have, long before the start of the protocol agreed to use polarized photons for communications and two bases for measurements. For example, photons in states |0> and |1> are implemented using photons polarized at 0^o degrees (→) and 90^o degrees (↑), respectively, and are said to represent 0 and 1 in rectilinear basis (+). Similarly, photons in diagonal basis are implemented using polarized photons at 45^o degrees (↗) and 135^o degrees (↖) as above.

- The Data bit size should be approximately 512 bit size so as to make the encryption easily.
- The data bits send through the channel are encrypted with 8-bit key and the 8-bit key is shared by sender and receiver. The encrypted data are marked as photons in polarized manner in such way that the data bits as 1's and 0's are encrypted using polarized photons at 0^o degrees (→) and 90^o degrees (↑) will be polarized at rectilinear basis and the data bits as 1's and 0's are encrypted using polarized photons at 45^o degrees (↗) and 135^o degrees (↖) in diagonal basis respectively.
- The data which is marked as a photon at 0^o degrees (→) and 90^o degrees (↑) under rectilinear basis and 45^o degrees (↗) and 135^o degrees (↖) under diagonal basis respectively are decrypted to data bits at receiver end with same key length of 8-bits.
- At receiving end the data bits are transferred back to the sender with extra added bits to the original data as to acknowledge that the given data has been received by the receiver as well as with the ID of the receiver so as to make that a proper channel is established between sender and receiver.
- If any attack been made by the intruder the attack will be reflected back at the data at particular locations specifying the intensity of the attack on the data bits.

A. B92 Protocol [9]

In 1992, Bennett proposes a protocol for QKD based on two non orthogonal states and known under the name of B92 or protocol of two states [9]. The quantum protocol B92 is similar to the BB84 protocol but it uses only two states instead of four states. B92 protocol is also based on the on Heisenberg's Uncertainty Principle. B92 protocol is proven to be unconditional secure. A remarkable proof of the unconditional security of B92 is the proof of Tamaki[10]. That is mean that this proof guaranteed the security of B92 in the presence of any enemy who can perform any operation permitted by the quantum physics; consequently the security of the protocol cannot be compromised by a future development in quantum calculation. Others results related to unconditional secure of B92 are discussed in [10, 11]. The use of a quantum channel that Eve (enemy) cannot monitor without being detected makes possible to create a secret key with an unconditional security based on the laws of the quantum physics. The presence of Eve is made manifest to the users of such channels through an unusually high error rate. B92 is a protocol of quantum key distribution (QKD) which uses polarised photons as information carriers. B92 supposes that the two legitimate users, Alice and Bob, communicate through two specific channels, which the enemy also has access to:

A classical channel, which can be public; Eve can listen passively (without being detected);

A quantum channel that (by its nature) Eve cannot listen passively

B. QUANTUM KEY ENCRYPTION ALGORITHM

```
1       Declare key, input file, output file
2       Initialize key and input file with plaintext.
3       for i=0 to size of the input file by step 1  do
3.1     ch = (char)fin.read();
3.2     s1=s1+(char)ch+" ";
3.3     if(key[i%8]=='X' && ch=='0')
3.3.1   crypt='\\';
3.4     else if(key[i%8]=='X' && ch=='1')
3.4.1   crypt='/';
3.5     else if(key[i%8]=='T' && ch=='1')
3.5.1   crypt='|';
3.6     else if(key[i%8]=='T' && ch=='0')
3.6.1   crypt='-'
3.7     Write crypt into output file
4       Close input and output file
```

C. QUANTUM KEY DECRYPTION ALGORITHM

1 Initialize key same as senders key and input file with crypted text that is send by the sender.
2 for i=0 to size of the input file by step 1 do
2.1 ch = (char)fin.read();
2.2 if(key[i%8]=='X')
2.2.1 if(ch=='\\')
2.2.1.1 decrypt='0', Write decrypt to output file;
2.2.2 else if(ch=='/')
2.2.2.1 decrypt='1', Write decrypt to output file;
2.3 else if(key[i%8]=='+')
2.3.1 if(ch=='|')
2.3.1.1 decrypt='1, Write decrypt to output file;
2.3.2 else if(ch=='-')
2.3.2.1 decrypt='0', Write decrypt into output file;
3 Close the input and output file

CONCLUSION

QKD protocols are based on combinations of principles from Quantum physics and information theory and made possible thanks to the tremendous progress in quantum optics and in the technology of optical fibers and of free space optical communication. Their security relies on deep theorems in classical information theory and on a profound understanding of the Heisenberg's uncertainty principle. Quantum cryptography protocols have some important contributions to classical cryptography: privacy amplification (Bennett, 1995) and classical bound information are examples of concepts in classical information whose discovery were much inspired by Quantum Cryptography protocols. Also, the fascinating tension between quantum physics and relativity, as illustrated by Bell's inequality, is not far away.

Quantum Cryptography protocols could well be the first application of quantum mechanics at the single quanta level. Many experiments have demonstrated that keys can be exchanged over distances of a few tens of kilometers at rates at least of the order of a thousand bits per second. There is no doubt that the technology can be mastered and will find commercial applications.

REFERENCES

[1] Diffie, W.; Hellman, M. (1976). "New directions in cryptography". *IEEE Transactions on Information Theory* **22** (6): 644–654. Doi:10.1109/TIT.1976.1055638 .

[2] Chang, I. ; IBM Thomas J. Watson Res, ext., "Key management for secure lnternet multicast using Boolean function minimization techniques", *INFOCOM '99. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings*, 21-25 March 1999.

[3] P. W. Shor and J. Preskill. "*Simple proof of security of the bb84 quantum key distribution protocol*". Phys. Rev. Lett., 85:441{444, Jul 2000.

[4] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot. "*Handbook of Applied Cryptography*". CRC Press, Inc., Boca Raton, FL, USA, 1st edition, 1996.

[5] C. H. Bennett and G. Brassard. "*Quantum cryptography: Public key distribution and coin tossing*". In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, pages 175:179, New York, 1984. IEEE Press.

[6] A. K. Ekert. "*Quantum cryptography based on bell's theorem*". Phys. Rev. Lett., 67:661{663, Aug 1991.

[7] C. H. Bennett, G. Brassard, and N. D. Mermin. "*Quantum cryptography without bell's theorem*". Phys. Rev. Lett., 68:557559, Feb 1992.

[8] C. H. Bennett. "*Quantum cryptography using any two nonorthogonal states*". Phys. Rev. Lett., 68:3121{3124, May 1992.

[9] S. V. Kartalopoulos. K08: "*a generalized bb84/b92 protocol in quantum cryptography*". Security and Communication Networks, 2(6):686:693, 2009.

[10] Tamaki.K , Lütkenhaus.N, "*Unconditional Security of the Bennett 1992 quantum key-distribution over lossy and noisy channel*," *Quantum Physics Archive*: arXiv:quantph/0308048v2, 2003.

[11] Tamaki.K, Lütkenhaus.N, Koashi.M, and Batuwantudawe.J, "*Unconditional security of the Bennett 1992 quantum key-distribution scheme with strong reference pulse* ", *Quantum Physics Archive*: arXiv:quant-ph/0607082v1,2006.

[12] C.H. Bennett, G. Brassard, C. Crepeu and U.M.Mauruer, "Generalized privacy amplification", IEEE Trans. Information Theory, 41, 1995.