SCI-PUBLICATIONS Author Manuscript

Science Publications

Open Access
Author Manuscript

American Journal of Applied Sciences 5 (2): 93-96, 2008
ISSN 1546-9239
© 2008 Science Publications

A New Quantum key Distribution Protocol

Essam Al-Daoud,
Faculty of Science and Information Technology,
Computer Science Department,
Zarka Private University, Jordan

Abstract: A new quantum key distribution protocol is proposed. The suggested protocol has two advantages. First: whenever an eavesdropper is present, the error rate increases obviously. Second, the eavesdropper can get only 2/n from the total information for an arbitrary n. Hence, eavesdropper has less information and can be detected easier. Moreover, the new protocol effectiveness is discussed and shown to be essentially higher than those of the other known protocols.

Keywords: Quantum key distribution, error rate, error correction, privacy amplification.

INTRODUCTION

Quantum key distribution (QKD) enables Secret Key Establishment between two users, using a combination of a classical channel and a quantum channel. QKD is based on laws of quantum physics. More precisely, it is based on the fact that an eavesdropper, trying to intercept the quantum communication, will inevitably leave traces which can thus be detected. In this case, the QKD protocol aborts the generation of the key, this property allows to perform Key Establishment with an extremely high security standard which is known as unconditional security. Experimental quantum key distribution was demonstrated for the first time in 1989 (it was published only in 1992)[2, 5]. Since then, tremendous progress has been made. Today, several groups have shown that quantum key distribution is possible, even outside the laboratory. For example, a team from BBN Technologies, Boston University, and Harvard University has recently built and begun to operate the Quantum Key Distribution network under DARPA sponsorship. Moreover, many Quantum Key distribution products are already commercially available such as ID Quantique and MagiQ [7, 8, 9].

In this paper, a novel quantum key distribution is proposed, which reduces an eavesdropper information for a given error rate. For example if n=10, then the eavesdropper information is about 20% and the error rate about 80%. The rest of this paper is arranged as follows: Section 2 introduces the most well known quantum key distribution protocols, Section 3 describes the new quantum key distribution protocol and its advantages, and Section 4 proves the correctness of the suggested protocol.

QUANTUM KEY DISTRIBUTION

In 1984 Bennett and Brassard suggested the first key distribution protocol based on quantum physics principles, and called BB84 after them[1]. Since then, many other protocols have been suggested to enhance BB84 security or to avoid some practical problems, for example SAGE04 is suggested to avoid photon-number splitting attack.

In BB84 protocol Alice and Bob use two channels, the first is a quantum channel which is used to send the qubits, while the second channel is used to announce the transforms that have been applied on the qubits, this channel is not assumed to be secure. At the begin of BB84 protocol, Alice sends Bob a random sequence of quantum qubits, which are equally likely to be in one of four possible states:

$$|\psi_1\rangle=|0\rangle,\ |\psi_2\rangle=|1\rangle,\ |\psi_3\rangle=1/\sqrt{2}\,|0\rangle+1/\sqrt{2}\,|1\rangle \text{ and } |\psi_4\rangle=1/\sqrt{2}\,|0\rangle-1/\sqrt{2}\,|1\rangle.$$

Bob and Alice agree that the corresponding bit values of the previous four states are 0, 1, 0, and 1, respectively. From these four states there are two possible orthogonal bases: + (or rectilinear) basis formed from the $|\psi_1\rangle$ and $|\psi_2\rangle$ states and the × (or diagonal) basis formed from the $|\psi_3\rangle$ and $|\psi_4\rangle$ states. The BB84 protocol goes as follows:

Corresponding Author: Essam Al-Daoud, Faculty of Science and Information Technology, Computer Science Department, Zarka Private University, Jordan, Tel: +962-796680005

SCI-PUBLICATIONS Author Manuscript

1- Alice randomly prepares m qubits, each in one of the four states $|\psi_1\rangle$, $|\psi_2\rangle$, $|\psi_3\rangle$ *or* $|\psi_4\rangle$ and sends them to Bob over a quantum channel.
2- For each qubit that Bob receives, he chooses at random one of the two bases ($\{|\psi_1\rangle, |\psi_2\rangle\}$ denoted by + *or* $\{|\psi_3\rangle, |\psi_4\rangle\}$ denoted by × and measures the qubit with respect to that basis. (Equivalently, Bob measures the qubit randomly with respect to the standard basis or performs a Hadamard transform on qubit and then measures it with respect to the standard basis).
3- Alice announces (over a classically insecure channel) the sequence of the bases has used.
4- Bob tells Alice at which times he measured the correct bases. If he chooses the same basis as Alice, his measurement result is the same as the classical bit that Alice prepared. If the bases differ, Bob's result is completely random.
5- Alice and Bob discard the times when they did not use the same bases.
6- Alice and Bob then test the security of their key by using a randomly chosen subset of their key. Results of their subset are compared and if errors are detected, the transmission is insecure and they abort and start again.
7- Classical error correction and privacy amplification techniques are used to generate a secure key.

An example of BB84 Protocol from Alice to Bob is given in Table 1. In perfect conditions Alice and Bob generate and share identical random keys, but because device imperfection and background noise can not be avoided, Alice and Bob can never guarantee that Eve has no information at all about their keys, for example, if Eve applies Intercept-resend attack on all the qubits, she gets 50% information, while Alice and Bob have about 25% of error in their sifted key. They can easily detect the presence of Eve. If, however, Eve applies Intercept-resend attack to only a 40% of the communication, then the error rate will be only 10% and Eve information will be about 20%. This error rate and the communication noise cannot be distinguished (experimental studies indicate that the error rate generated by the noise and the devices imperfection is about 10% see[4, 5]) , and so to be on the safe side Alice and Bob have to assume that all errors are due to Eve. If the error rate is more than an agreed threshold, 10% let's say, then they must regenerate the key, but if the error rate is less than an greed threshold, they must perform error correction to remove the disagreement in their keys and privacy amplification to decrease the amount of information held by Eve.

Another important protocol is SAGE04[3, 6], which is proposed to avoid photon-number-splitting attack (PNS). This can be done by replacing step 3 in BB84 protocol, instead of announcing the sequence of the bases used, Alice announces publicly one of the four sets $\{|\psi_1\rangle, |\psi_3\rangle\}$, $\{|\psi_2\rangle, |\psi_3\rangle\}$, $\{|\psi_1\rangle, |\psi_4\rangle\}$ *or* $\{|\psi_2\rangle, |\psi_4\rangle\}$, that contains the state of the photon sent out by her. In this case, an eavesdropper can not determine the bases that must be used.

THE PROPOSED PROTOCOL

The proposed protocol has a fundamental, qualitatively new feature, which allows secure data transmission through practically any noisy quantum channel. Unlike the pervious protocols, the new protocol allows to the sender and the receiver to apply arbitrary number of a unitary operation on random states, which is not chosen in advance by either party. The suggested protocol goes as follows:

1- Alice randomly prepares *m* qubits, each in one of the two states:

$$|\psi_1\rangle = |0\rangle$$
$$|\psi_2\rangle = |1\rangle$$

2- For each qubit, Alice applies the unitary operator
3-
4- $R(\phi)$ *i* times on the state $|\psi_k\rangle$ where

$$R(\phi)=\begin{bmatrix}\cos\phi & -\sin\phi\\ \sin\phi & \cos\phi\end{bmatrix},\ i\in\{0,1\ldots.n-1\}$$

and $\phi=\pi/n$.

Thus the sent qubit is $|\psi\rangle = R(\phi)^i |\psi_k\rangle$ where k=1 or 2 and $i\in\{1,2,\ldots n-1\}$.

5- Bob applies the unitary operator $R(\phi)$ *j* times on the received states, $j\in\{0,1\ldots.n\}$, and then measures it with respect to the standard basis.
6- Alice announces publicly the number of times she applies the operator $R(\phi)$ on each qubit, thus she announces a sequence of integer numbers.
7- Bob tells Alice to discard the times when the output of the measurement is confusing, in this protocol the output is confusing if (i+j) mod n ≠ 0 or (i+j) mod n≠ n/2.
8- Alice and Bob then test the security of their key by using a randomly chosen subset of their key. Results of their subset are compared and if errors are detected, the transmission is insecure and they abort and start again.
9- Classical error correction and privacy amplification techniques are used to generate a secure key.

SCI-PUBLICATIONS Author Manuscript

Table 1: An example of BB84 Protocol from Alice to Bob

The Bit	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Alice's Random Bits	1	0	0	1	1	1	0	1	0	0	0	1	1	0	1
Alice's Random Basis	×	+	×	×	+	+	×	×	×	+	+	×	×	×	+
Alice's States	ψ_4	ψ_1	ψ_3	ψ_4	ψ_2	ψ_2	ψ_3	ψ_4	ψ_3	ψ_1	ψ_1	ψ_4	ψ_4	ψ_3	ψ_2
Bob's Random Basis	×	+	+	×	×	+	×	+	×	+	×	×	×	+	+
Bob's Result	1	0	1	1	1	1	0	0	0	0	0	1	1	1	1
Same Basis?	Y	Y		Y		Y	Y		Y	Y		Y	Y		Y
The sifted Key	1	0		1		1	0		0	0		1	1		1

Table 2: The Proposed Protocol from Alice to Bob where n=10

The Bit	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Alice's Random Bits	1	0	0	1	1	1	0	1	0	0	0	1	1	0	1
Alice's Random integer *i∈ {0,1...n-1}*	3	9	8	2	5	0	1	7	4	5	9	8	6	0	4
Bob's Random integer *j∈ {0,1….n-1}*	4	6	5	8	1	3	9	8	5	2	0	7	4	7	2
Bob's Result	0	1	1	1	0	1	0	0	0	1	0	0	1	1	0
Is *(i+j)mod 10 = 0* or *(i+j)mod 10 =5*		Y		Y			Y					Y	Y		
The sifted Key		0		1			0					1	1		

An example of the Proposed Protocol from Alice to Bob is given in Table 2. In this protocol, Eve can get only 2/n information, while Alice and Bob have about (n-2)/n of error in their sifted key. For example if n=10, then Eve information is about 20%, which means that, Eve information is reduced about 60% (in comparison with BB84). Moreover, Alice and Bob have about 80% of error in their sifted key, which means that the error rate is increased about 70% (in comparison with BB84). For estimation of the Eve's intervention into the data transmission through a quantum channel we apply a unitary operator on random states, which adequately reflects the information aspect of the eavesdropping and can be effectively used for both constructing and analyzing the quantum key distribution protocol.

CORRECTNESS OF THE PROPOSED PROTOCOL

It is easy to prove that (by using induction):

$$R(\phi)^x = \begin{bmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{bmatrix}^x = \begin{bmatrix} \cos x\phi & -\sin x\phi \\ \sin x\phi & \cos x\phi \end{bmatrix}$$

x is an integer number greater than zero. Now Let $\phi = \pi/n$ then

$$R(\pi/n)^{i+j} = \begin{bmatrix} \cos\pi/n & -\sin\pi/n \\ \sin\pi/n & \cos\pi/n \end{bmatrix}^{i+j}$$

$$= \begin{bmatrix} \cos(i+j)\pi/n & -\sin(i+j)\pi/n \\ \sin(i+j)\pi/n & \cos(i+j)\pi/n \end{bmatrix}$$

In case $(i+j)$ mod $n=0$, then $(i+j) = kn$ and

$$R(\pi/n)^{i+j} = \begin{bmatrix} \cos k\pi & -\sin k\pi \\ \sin k\pi & \cos k\pi \end{bmatrix}$$

$$= \begin{bmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{bmatrix}.$$

The sign $\pm$ depends on k whether it is odd or even. In this case, if the original state is $|\psi_k\rangle$ then Bob state is $\pm |\psi_k\rangle$ and his measurement equals to the corresponding Alice bit.

In case $(i+j)$ mod $n=n/2$ and n is an even integer, then $(i+j) = kn+n/2$ and

SCI-PUBLICATIONS Author Manuscript

$$R(\pi/n)^{i+j} = \begin{bmatrix} \cos(k\pi+\pi/2) & -\sin(k\pi+\pi/2) \\ \sin(k\pi+\pi/2) & \cos(k\pi+\pi/2) \end{bmatrix} = \begin{bmatrix} 0 & \pm 1 \\ \pm 1 & 0 \end{bmatrix}.$$

The sign (±) depends on k whether it is odd or even, In this case, if the original state is |*0*> then Bob state is ± |*1*> and if the original state is |*1*> then Bob state is ± |*0*>, hence, Bob measurement is the opposite of the corresponding Alice bit, and therefore bob can guess Alice's original bit.

In case $(i+j) \bmod n \neq 0$ or $(i+j) \bmod n \neq n/2$, Bob cannot determine the original state whether |*0*> or |*1*>

CONCLUSION

It is shown that the proposed protocol surpasses all known quantum key distribution protocols by a number of criteria. For instance, the eavesdropper has less information and can be detected easier. This means that the new protocol can basically work at high level of external errors or eavesdropping attacks, which is a new feature of the quantum key distribution protocols.

REFERENCES

1. Al-Daoud E., 2007. Unconditionally Secure Quantum Payment System. International Journal of Applied Mathematics an Computer Science, 4(2): pp 566 -569.
2. Al-Daoud E., 2007. Comparing Two Quantum Protocols: BB84 and SARG04. European Journal of Scientific Research, 17 (1): pp.25-30.
3. Branciard C., and el at., 2005. Security of two quantum cryptography protocols using the same four qubit states. Phys. Rev. A 72, 032301.
4. Gobby C., and et al., 2004. Quantum key distribution over 122 km standard telecom fiber. Appl. Phys. Lett., 84 :3762-3764.
5. Panthong P., and et al., 2005. Experimental Free Space Quantum Key Distribution. The 4th International Conference on Optical Communication and Networks, Thailand, 14-16, ICOCN2005, pp 159-161.
6. Scarani V., A. Acin, G. Ribordy and N. Gisin, (2004). Quantum Cryptography Protocols Robust Against Photon Number Splitting Attacks for Weak Laser Pulses Implementation. Phys. Rev. Lett. 92, 057901.
7. www.bbn.com/Solutions_and_Technologies/Information_Security/Quantum_Cryptography.html. last access on January 2007.
8. www.idquantique.com. last access on January 2007.
9. www.magiqtech.com. last access on January 2007.