انجمن رمز ایران
Iranian Society of Cryptology

8th International ISC Conference
on Information Security and Cryptology
(ISCISC'11)

Ferdowsi University
of Mashhad

Ferdowsi University of Mashhad-September 14-15, 2011

An Entanglement-based Quantum Key Distribution Protocol

Monireh Houshmand
Department of Electrical Engineering
Imam Reza University
Mashhad, Iran

Saied Hosseini-Khayat
Department of Electrical Engineering
Ferdowsi University of Mashhad
Mashhad, Iran

***Abstract*—A novel quantum key distribution protocol using entanglement is presented. In this protocol, the stream of qubits is divided up into a sequence of qubit pairs. It is shown that by entangling the qubits in each qubit pair by randomly applying one of the two predefined unitary transformations before transmission, the protocol reveals less information about the key bit than the BB84 protocol, and the quantum bit error rate is also reduced.**

Keywords: *Quantum cryptography, Entaglment, Quantum key distribution, BB84*

I. INTRODUCTION

The need to communicate secretly is considered as one of the most important challenges of the information age. To fulfill this goal, an encryption algorithm is used to combine a message with some additional information (a key) to produce a cryptogram. Consequently, secure key distribution is at the heart of cryptography. Recently quantum key distribution (QKD) schemes such as the BB84 protocol [1] have emerged to solve this problem. The security of QKDs are based on the quantum physical limitation that any measurement can potentially disturb the observed system [2]. In fact, quantum mechanics strictly forbids passive monitoring of a quantum channel due to the no-cloning theorem. In quantum cryptography, an eavesdropper's ability is only limited by the principles of quantum mechanics.

Since the publication of BB84, there has been much interest in quantum cryptography and many QKD protocols have been introduced [3, 4, 5, 6, 7, 8]. In this paper, a novel QKD protocol is presented in which Alice sends Bob a stream of entangled pairs of qubits, instead of a stream of qubits. Our analysis shows that our protocol has certain advantages over BB84.

This paper is organized as follows: Section II defines the concept of efficiency. In Section III, we review and analyze BB84. In Sections IV and V, our proposed protocol is presented and evaluated. We summarize our contribution in Section VI.

II. DEFINING EFFICIENCY

We use a modified version of Cabello's definition of efficiency [9] of QKD protocols in order to compare our protocol with BB84. Cabello defines efficiency as below

$$E = \frac{b_s}{q_t + b_t},$$

where b_s is the number of secret key bits finally generated by the protocol, and q_t and b_t are the number of quantum and classical bits, respectively, transmitted during a QKD protocol. In that definition, the classical bits used for eavesdrop checking are ignored. However, since the transmission of qubits are more expensive than classical bits, we modify Cabello's definition to give more weight to qubits as follows:

$$\eta \triangleq \frac{b_s}{\alpha q_t + b_t},$$

where $\alpha > 1$ is a weighting factor for the cost of qubits.

III. REVIEW OF BB84

In the BB84 scheme, Alice begins with two random strings of bits $a = a_1 a_2 \cdots a_n$ and $b = b_1 b_2 \cdots b_n$. She then encodes these two strings as a string of n qubits

$$\psi = \bigotimes_{i=1}^{n} \phi_{a_i b_i}$$

where $a_i b_i$ together give an index into the following four states

$$\phi_{00} = |0\rangle, \quad \phi_{10} = |1\rangle,$$
$$\phi_{01} = H|0\rangle = |+\rangle, \phi_{11} = H|1\rangle = |-\rangle,$$

where H is the Hadamard operator. Alice sends ψ over a public quantum channel to Bob. Bob generates a random bit string b' of length n, which determines the basis of measurement, and then measures the string ψ. The outcome is the bit string a'. At this point, Bob announces publicly that he has received Alice's transmission. Then Alice announces b. Bob communicates over a public channel with Alice to determine which b_i and b'_i are not equal. Both Alice and Bob now discard the qubits in a and a' where b and b' do not match which are on the average $n/2$ bits. From the remaining $n/2$ bits, for which both Alice and Bob used the same basis, Alice randomly chooses $n/4$ bits (called check bit) and discloses her choices over the public channel. Both Alice and Bob announce check bits publicly and run a check to see if more than a certain number of them, agree. If this check phase passes, Alice and Bob use the information reconciliation and privacy amplification procedures [11, 12, 13] to create a number of shared secret keys. Otherwise, they discard the sequence and start over.

In quantum cryptography, an eavesdropper (so called Eve) is assumed to have the following capabilities: She can 1) freely tamper with the quantum channel, 2) listen to the classical channel. Any method of eavesdropping causes errors to the quantum transmission, quantified by Quantum Bit Error Rate (QBER). The errors allow Alice and Bob to detect Eve's interference and to obtain an estimate on Eve's maximal information about the key. The Intercept-Resend attack is the most common eavesdropping strategy, which is allowed by the laws of quantum physics. In this type of attack, Eve intercepts each qubit sent by Alice, measures the qubit state and resends to Bob the qubit which is the result of her measurement. In the BB84 protocol, Eve performs her measurements exactly like Bob: For each qubit, she chooses at random between the two measurement bases, i.e., basis of Pauli's Z or X matrices. If Eve uses the Z basis in a measurement, an outcome 0 means that Eve sends $|0\rangle$, and outcome 1 means that she sends $|1\rangle$ to Bob. If Eve's measurement basis is X, she re-sends $|+\rangle$ if the result is 0, and $|-\rangle$ if the result is 1.

Since for transmission of n qubits, it is required to transmit n basis information, and half of the qubits on average are omitted due to basis incompatibility, the efficiency of the protocol will be

$$\eta = \frac{\left(\frac{n}{2}\right)}{\alpha n+n}.$$

The amount of knowledge that Eve obtains about Alice's bit sequence, A (after basis reconciliation) is quantified by Shannon's mutual information [10]

$$I(A,E) = H(A) + H(E) - H(A,E),$$

where E is the random variable denoting the outcome of each of Eve's measurements. The entropy of A is:

$$H(A) = \sum_{a=0}^{1} P(a)\log_2 P(a) = 1.$$

Also we have

$$P(e=0) = P(\text{ wrong basis })P(e=0|\text{ wrong basis })$$

$$+P(\text{ correct basis })P(e=0|\text{ correct basis }) = 1/2$$

And

$$P(e=1) = 1 - P(e=0) = \frac{1}{2}.$$

Therefore:

$$H(E) = \sum_{e=0}^{1} P(e)\log_2 P(e) = 1.$$

Also

$$H(A,E) = -\sum_{a=0}^{1}\sum_{e=0}^{1} P(a,e)\log_2 P(a,e)$$

which is equal to

$$-(\frac{1}{2}\log_2\frac{1}{2} + \frac{1}{2}\log_2\frac{1}{2}) = 1,$$

when Alice's and Eve's bases are the same, and is equal to

$$-4(\frac{1}{4}\log_2\frac{1}{4}) = 2,$$

when their bases are different. Since Eve's choice of basis is correct half the time on average, we have

$$H(A,E) = \frac{1}{2}(1+2) = \frac{3}{2},$$

therefore

$$I(A,E) = H(A) + H(E) - H(A,E) = 1 + 1 - \frac{3}{2} = \frac{1}{2}.$$

It means that Eve gains 0.5 bits of information per key bit. If Eve guesses the basis correctly, there will be no disturbance and Alice and Bob will get the same result, in the other case, in half of the times, on average, Alice and Bob measurement results are different, so the QBER is equal to 0.25. Since in the BB84 protocol, there is no entanglement among the transmitted qubits, interception of one qubit may result in the disturbance of that qubit only and not on the others. Therefore if Eve is lucky enough that none of the qubits she has measured belong to the check set, she will not be detected at all!

IV. PROPOSED ALGORITHM

Before the protocol begins, Alice and Bob publicly agree on two 2-qubit unitary transformations, U_1 and U_2, which are defined as follows

$$U_1 = \text{CPHASE}\,(I \otimes H)\,\text{CNOT}\,(H \otimes I),$$

$$U_2 = (\text{CPHASE})'(I \otimes H)\,\text{CNOT}\,(H \otimes I),$$

where H is the Hadamard gate, CNOT is the controlled-not gate, and CPHASE and (CPHASE) $'$are equal to:

$$\text{CPHASE} = I \otimes |00\rangle + \text{PHASE} \otimes |11\rangle,$$

$$(\text{CPHASE})' = I \otimes |00\rangle + (\text{PHASE})' \otimes |11\rangle,$$

where:

$$\text{PHASE} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix},$$

$$(\text{PHASE})' = \begin{pmatrix} i & 0 \\ 0 & -1 \end{pmatrix}.$$

It is easy to verify that U_1 and U_2 generate entanglement since they cannot be decomposed into $A \otimes B$. Alice generates a number of random bits divided in groups of 2. The bit string $a = a_1a_2$ denotes such a group. In the next step, she prepares $|\Phi\rangle = |a_1a_2\rangle$ and applies randomly one of U_1 or U_2 to it. She then transmits the two qubits one at a time, always waiting for Bob to acknowledge the reception of the previous qubit before she sends the next one. This prevents Eve from perfectly undoing the transformation U_1 or U_2. When Bob receives each qubit, he immediately acknowledges the qubit. Then Alice discloses her choice of transformation.

Bob undoes the transformation by applying $U_1^\dagger$ or $U_2^\dagger$, and then measures the qubits in the computational basis and obtains the raw key bits. In the eavesdropp checking phase, Alice randomly selects one qubit of each group and discloses them on a public channel to compare it with Bob measurement result. If more than a predetermined number of bits disagree, they abort the protocol and start over. Otherwise they proceed to use information reconciliation and privacy amplification procedures to create a number of shared secret keys.

V. ANALYSIS

In the proposed protocol, all transmitted qubits are useful (unlike $BB84$ that half of qubits are discarded on average) and one classical bit is used to acknowledge receiving each qubit and one classical bit is used for determining the basis of each group of qubits so efficiency is equal to

$$\eta = \frac{n}{\alpha n + \frac{n}{2} + n},$$

where n is the number of transmitted qubits.

In the proposed protocol, the basis that Eve chooses for measurement has a significant impact on the information she gains. We analyze the intercept-resend attack in three cases. 1) Eve measures both qubits of a qubit pair in the computational basis, 2) she measures both in an arbitrary basis, and 3) she measures only one qubit of each qubit pair in an arbitrary basis.

Case 1. Eve measures both qubits in the Z basis: The mutual information, $I(A,E)$, that Eve gains about Alice's key is equal to

$$I(A,E) = \frac{1}{2}[H(A) + H(E) - H(A,E)].$$

The factor $\frac{1}{2}$ ensures that the equation yields mutual information per bit, since A,E are both 2-bit entries.

$$H(A) = -\sum_{a=0}^{3} P(a)\log_2 p(a) = -4(\frac{1}{4}\log_2\frac{1}{4}) = 2,$$

$$H(E) = -\sum_{e=0}^{3} P(e)\log_2 p(e) = -4(\frac{1}{4}\log_2\frac{1}{4}) = 2,$$

$$H(A,E) = -\sum_{a=0}^{3}\sum_{e=0}^{3} P(e,a)\log_2 P(e,e)$$

$$= -16(\frac{1}{16}\log_2\frac{1}{16}) = 4$$

Therefore

$$I(A,E) = \frac{1}{2}[H(A) + H(E) - H(A,E)] = 0.$$

This means that Eve gains no information about Alice's key. When Eve measures both qubits of a group, the state collapses to one of the four states $|00\rangle, |01\rangle, |10\rangle$ and $|11\rangle$with the same probability 0.25, so in the check phase, the measurement outcome for each of the check qubits is 0 or 1 with probability 0.5; then obviously in this case QBER is 0.5.

Case 2. Eve measures both qubits in a quibit pair in an arbitrary basis: In this case, we allow Eve to measure each qubit in a possibly different basis. This is equivalent to allowing Eve to apply arbitrary gates to each qubit and then measure both qubits in the Z basis. She then undoes the previously applied single-qubit gate before sending the qubit to Bob. Normally Eve wants to maximize her information of Alice's key with the minimum increase in QBER [15], so she maximizes the metric $F = \frac{I(A,E)}{QBER}$. We used a genetic algorithm to find Eve's optimum transformations. The solution turns out to be

$$U_{e_1} = \begin{pmatrix} -0.8664 & -0.4994 \\ -0.4994 & 0.8664 \end{pmatrix},$$

$$U_{e_2} = \begin{pmatrix} -0.5547 & 0.3379 - 0.7603i \\ -0.8321 & -0.2253 + 0.5069i \end{pmatrix}.$$

In this case, $I(A,E) = 0.265$ and QBER is 0.43 so

$$F_1 = \frac{0.265}{0.43} = 0.6162.$$

Case 3. Eve measures only one qubit in each qubit pair in an arbitrary basis: As mentioned before, the optimization method is used for finding the best measurement that Eve may do. The best solution for her is to apply the following unitary at the first qubit and measure the first qubit, in the Z basis:

$$U = \begin{pmatrix} 0.3846i & 0.9041 - 0.1863i \\ -0.9231 & 0.0776 + 0.3767i \end{pmatrix}.$$

$I(A,E)$ will be 0.204 and QBER will be 0.391. Therefore

$$F_2 = \frac{0.204}{0.391} = 0.5217.$$

Even in a qubit pair that Eve does not measure, QBER is equal to 0.28. This happens because of the entanglement in each qubit pair.

The above analysis allows us now to compare our protocol with BB84. Table I summarizes the results of our analysis.

TABLE I: Comparison of proposed algorithm with BB84

Protocol	Mutual information/QBER(F)
BB84	$F = 2$
Our protocol	$F_1 = 0.6162$ $F_2 = 0.5217$

It is shown that the value of metric F is decreased by a factor of 3.24 when Eve measures both qubits of each group and by the factor of 3.83 when Eve measures both of qubits of each group.

VI. CONCLUSION

In this paper, we introduced and analyzed a novel QKD protocol that utilizes entanglement to provide advantage against eavesdropper. We analyzed the security of the protocol under an intercept-resend attack. We showed that the metric F, of the proposed protocol is better than that of BB84. Our protocol is easily extendable to $N > 2$. In that case, Alice and Bob agree on two N-qubit inseparable transformations. Then Alice applies one of these transformations to an *N-tuple* of qubits. In the checking phase, half of qubits of each group are disclosed.

REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum Cryptography:Public Key Distribution and Coin Tossing," *IEEE International Conference on Computer Systems and Signal Conferences*. New York, 1984, pp 175-179.

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden,*Quantum cryptography*. Rev. Mod. Phys. 74, 2002.

[3] L. Goldenberg and L. Vaidman, "Quantum cryptography based on orthogonal states,"*Phys. Rev. Lett*. 75, 1995.

[4] W. Y Hwang, I. G. Koh and Y D. Han, "Quantum cryptography without public announcement of bases," *Phys. Lett. A*, 1998.

[5] S. Phoenix, S. Barnett, and A. Chefles, "Three-state quantum cryptography*,"J. Mod. Opt.*, vol. 47, p. 507, 2000.

[6] H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and a proof of its unconditional security*,"Journal of Cryptology*,vol. 18, pp. 133–165. 85, 2005.

[7] C.-H. F. Fung, K. Tamaki, and H.-K. Lo, "Performance of two quantumkey- distribution protocols*,"Phys. Rev. A*, vol. 73, p. 012337. 85, 2006.

[8] G.L. Young, X.H. LioC, "Theoretically efficient high-capacity quantum-key-distribution scheme,"*Phys. Rev. A* 65, 032302, 2002.

[9] A.Cabelo, "Quantum Key Distribution in the Holevo Limit,"Phys. Rev. Lett. 85 , 2000.

[10] M. A. Nielsen and I. L.Chuang, *Quantum Computation and Quantum Information.*Cambridge University Press, 2000.

[11] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, "Experimental quantum cryptography*," Journal of Cryptology*, 1992.

[12] T. Sugimoto and K. Yamazaki, "A Study on Secret Key Reconciliation Protocal Cascade,"*IEICE Trans. Fundamentals*, Vol.E83-A, NO.10, 1987-1991, 2000.

[13] Sh. Liu, Henk C. A. V.Tilborg and M. Dijk,"A practical Protocol for Advantage Distillation and Information Reconciliation*,"Codes and Cryptography*, 30, pp. 39-62, 2003.

[14] A. P. Makkaveev, S. N. Molotkov, D. I.Pomozov and A. V. Timofeev, "Practical Error-Correction Procedures in Quantum Cryptography,"*Journal of Experimental and Theoretical, Physics*, Vol.101, pp. 230-252, 2005.

[15] Olli Ahonen, *Quantum cryptography protocol lbased on sending entangled qubit pairs*. Master Thesis, Helsinki University of Technology Physics, 2005.