In the name of God

An Entanglement-based Quantum Key Distribution Protocol

Monireh Houshmand
Saied Hosseini-Khayat

Summer 1390

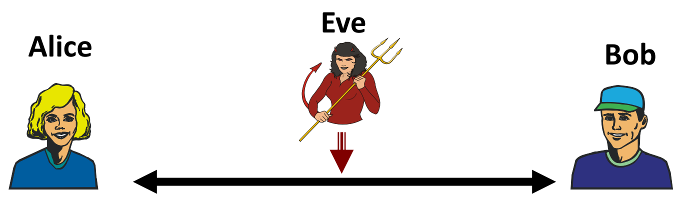
Introduction

- **Quantum Key Distribution (QKD)**
  - one of the most successful application of quantum information theory
  - its security is based on **laws of quantum mechanics,** not based on the complexity of factoring integers
- **BB84** protocol
  - most well-known QKD
  - Bennett and Brassard in 1984
- In this paper, a novel QKD protocol is presented
  - which has advantages over BB84

2

QKD Scnario

- Alice communicates with Bob via a quantum channel
- They discuss results using a public classical channel
  - allows them to verify that the key has not been intercepted
- Eavesdropper
  - tamper with the quantum channel
  - listen to the classical channel
- Quantum Bit Error Rate (QBER)
- **Intercept-resend attack**
  - Eve intercepts each qubit sent by Alice, measures the qubit state and resends to Bob the result of her measurement



3

Proposed Protocol

- Alice and Bob publicly agree on two **2-qubit** unitary transformations

$$U_1 = \text{CPHASE}\,(I \otimes H)\,\text{CNOT}\,(H \otimes I),$$
$$U_2 = (\text{CPHASE})'(I \otimes H)\,\text{CNOT}\,(H \otimes I),$$

where

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

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

- These two unitary transformations generate **entanglement**

4

Alice

- generates a number of random bits divided in groups of 2: $a = a_1 a_2$
- prepares $|\Phi\rangle = |a_1 a_2\rangle$ and applies randomly one of the unitaries
- transmits the two qubits one at a time
  - waiting for Bob to acknowledge the reception of the previous qubit
  - prevents Eve from perfectly undoing the transformation
- discloses her choice of transformation

5

Bob

- undoes the transformation by applying

  $U_1^\dagger$ or $U_2^\dagger$
- measures the qubits in the computational basis
- obtains the raw key bits

6

Eavesdropping Phase

- Alice randomly selects one qubit of each group
  - discloses them on a public channel to compare with Bob measurement result
- If more than a predetermined number of bits disagree
  - abort the protocol and start over
- Otherwise they share secret keys

Figure of Merit (*F*)

- Eve wants to **maximize her information** of Alice's key with the **minimum increase in *QBER***.
- The amount of knowledge that Eve obtains about Alice's bit sequence
  - quantified by **Shannon's mutual information**

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

=> ***F=I(A,E)/QBER***

- BB84:
  - *I(A,E)*=1/2
  - *QBER*=1/4 **=>** F=2
- Proposed protocol
  - is analyzed in three cases

- **Eve measures both qubits in the *Z* basis**
  - Our analysis shows that

    I(A,E)=0 and *QBER*=1/2 **=>** *F=0.*
- **Eve measures only one qubit in each pair in an arbitrary basis**
  - This is equivalent to allowing Eve to apply arbitrary gates to one qubit and then measure the qubit in the *Z* basis
- **Genetic algorithm** is used to find Eve's optimum transformation

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

$$F_1 = \frac{0.204}{0.391} = 0.5217$$

9

- **Eve measures both qubits in a pair in an arbitrary basis**
  - This is equivalent to allowing Eve to apply arbitrary gates to each qubit and then measure both qubits in the *Z* basis.
- **Genetic algorithm** is used to find Eve's optimum transformations

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

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

$$F_2 = \frac{0.265}{0.43} = 0.6162$$

10

Comparison with BB84

Protocol	I(A,E)/QBER (F)
BB84	$F = 2$
Our protocol	$F_1 = 0.5217$ $F_2 = 0.6162$

- Value of metric *F* is decreased by a factor of 3.83 and by the factor of 3.24 when Eve measures one and both of qubits of each group

11

Conclusion

- A novel QKD protocol that utilizes entanglement to provide advantage against eavesdropper
- The metric *F*, of the proposed protocol is better than that of BB84.
- Our protocol is easily extendable to N>2
  - Alice and Bob agree on two N-qubit transformations.
  - Alice applies one of these transformations to an N-tuple of qubits
  - In the checking phase, half of qubits of each group are disclosed

12