A THREE-STAGE QUANTUM CRYPTOGRAPHY PROTOCOL

Subhash Kak

Department of Electrical & Computer Engineering
Louisiana State University,
Baton Rouge, Louisiana 70803
E-mail: kak@ece.lsu.edu

Received 4 May 2005; revised 20 December 2005

We present a three-stage quantum cryptographic protocol based on public key cryptography in which each party uses its own secret key. Unlike the BB84 protocol, where the qubits are transmitted in only one direction and classical information exchanged thereafter, the communication in the proposed protocol remains quantum in each stage. A related system of key distribution is also described.

Keywords: quantum information science, quantum cryptography, secure communication protocol.

1. INTRODUCTION

This paper presents a quantum protocol based on public key cryptography for secure transmission of data over a public channel. The security of the protocol derives from the fact that Alice and Bob each use secret keys in the multiple exchange of the qubit.

Unlike the BB84 protocol [1] and its many variants (e.g., [2-4]), where the qubits are transmitted in only one direction and classical information exchanged thereafter, the communication in the proposed protocol remains quantum in each stage. In the BB84 protocol, each transmitted qubit is in one of four different states; in the proposed protocol, the transmitted qubit can be in any arbitrary state.
Fig. 1. Three-stage protocol for quantum cryptography where $U_A U_B = U_B U_A$.

2. THE PROTOCOL

Consider the arrangement of Fig. 1 to transfer state $X$ from Alice to Bob. The state $X$ is one of two orthogonal states, such as $|0\rangle$ and $|1\rangle$, or $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, or $\alpha|0\rangle + \beta|1\rangle$ and $\beta|0\rangle - \alpha|1\rangle$. The orthogonal states of $X$ represent 0 and 1 by prior mutual agreement of the parties, and this is the data or the cryptographic key being transmitted over the public channel.

Alice and Bob apply secret transformations $U_A$ and $U_B$ which are commutative, i.e., $U_A U_B = U_B U_A$. An example of this would be $U_A = R(\theta)$ and $U_B = R(\phi)$, each of which is the rotation operator:

$$R(\theta) = \begin{pmatrix} \cos \theta - \sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}.$$  

The sequence of operations in the protocol is as follows:

1. Alice applies the transformation $U_A$ on $X$ and sends the qubit to Bob.
2. Bob applies $U_B$ on the received qubit $U_A(X)$ and sends it back to Alice.
3. Alice applies $U_A^\dagger$ on the received qubit, converting it to $U_B(X)$, and forwards it to Bob.
4. Bob applies $U_B^\dagger$ on the qubit, converting it to $X$. 