Abstract

Authentication is one of the security services that ensure sufficient security of the system by identification and verification. Also, it assures the identity of the communicating party to be that the claimed one. To build a quantum channel between two unauthenticated to each other users, a trusted authority is needed to create a mutual authentication with each party before they communicate. Using Bell measurement and entanglement swapping, we present a protocol that mutually authenticates the identity of the sender and the receiver then, constructs a quantum channel based on Bell basis. The sender and the receiver use the quantum channel to communicate using entanglement-assisted quantum communication protocols. Additionally, the protocol renews the shared secret key distribution to create a quantum channel between the sender and receiver.

Quantum Bases

Computational Basis:

| Φ+ | 1,0,1,1,0 |
| Φ− | 0,1,1,0,1 |

Qubit Basis:

| Φ+ | 1,0,1,1,0 |
| Φ− | 0,1,1,0,1 |

Quantum Entanglement

Quantum cryptography depends on the laws of quantum mechanics for sending and receiving data using quantum states such as atoms, photons or molecules.

Quantum Entanglement:

A pair of particles share the same properties, measurement on one particle determines the value of the other particle even if they are spatially separated.

Bell States:

| Φ+ | 1,0,1,1,0 |
| Φ− | 0,1,1,0,1 |

Secret Key Distribution

Trent sends to users $\lbrack Y(L) \rbrack_{TA} = \{ [Y(1)]_{TA}, [Y(2)]_{TA}, ..., [Y(L)]_{TA} \}$ where $Y \in \{ |\Psi^+ \rangle, |\Psi^- \rangle, |\Phi^+ \rangle, |\Phi^- \rangle \}$. Let $i = j + q + p = L$.

In each $[Y(L)]_{TA}$ Trent keeps $[Y(L)]_{TA}$, and sends $[Y(L)]_{TA}$ to Alice. Alice chooses $(t + q)/2$ then perform bell measurement, for example: $[\Phi^+]_{12} \otimes [\Phi^+]_{34} = [\Phi^+]_{1234}$, $[\Phi^-]_{1234}$, $[\Psi^-]_{1234}$, $[\Psi^+]_{1234}$

Trent meet with Alice on the classical channel and verify $t/2$ pairs if the pairs were correct then, the rest pairs $q/2$ become the new key.

Building the Communication Channel

Trent reorders the $p$ remaining pairs between him and the users $[Y(\{i\})]_{TA} = \{ [Y(1)]_{TA}, [Y(2)]_{TA}, ..., [Y(p)]_{TA} \}$ for Alice, $j$=Bob, Trent make entanglement swapping for each $[Y(j)]_{TA} \otimes [Y(j)]_{TB}$.

The result is an entanglement between Alice and Bob.

Alice and Bob communicate using Teleportation,$E91$ or RSP

References: