Quantum Mutual Authentication Scheme Based on Bell State Measurement

Muneer Alshowkan, Khaled Elleithy
Department of Computer Science and Engineering
University of Bridgeport, Bridgeport, CT

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 between the trusted authority and each user after authentication process. The protocol provides the necessary authentication and key distribution to create a quantum channel between the sender and receiver.

Mutual Authentication and Registration

In a network of n users $u_i \in U = \{u_1, u_2, \dots, u_n\}$
Trusted authority shares $k_{Tu}^{2m} \in K = \{k_{Tu}^1, k_{Tu}^2, \dots, k_{Tu}^{2m}\}$with everyone
Derive encoding bases $b_{TA}^{2m} = \{b_{TA1}^m + b_{TA2}^m\}$ '0' in B_z & '1' in B_x
Using b_{TA1}^m Trent and Alice generate sequence S_{TA} and S_{AT}
Exchange the sequences then verify through the classical channel
Example:
Key:1,0,1,1,0
S_{AT}: 1,1,0,1,0
S_{TA}: 0,1,1,0,1

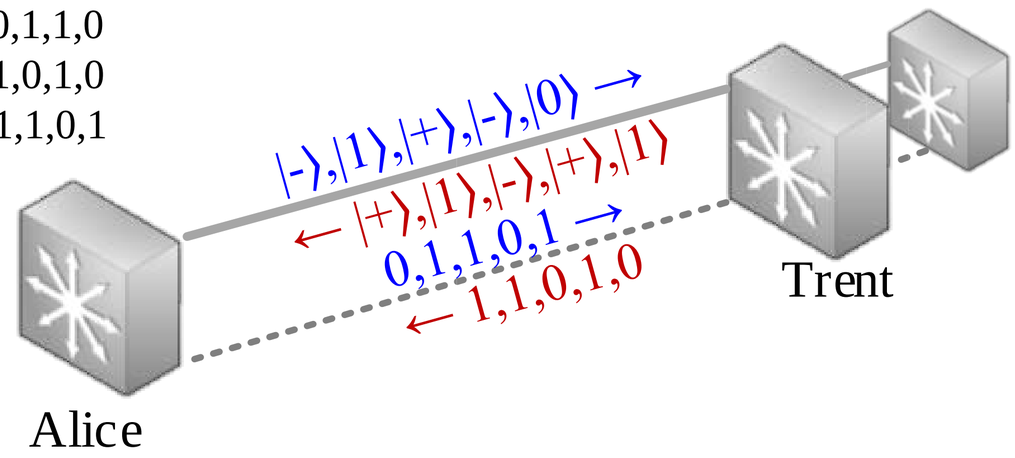

Fig 3: Example of the authentication process between Alice and Trent

Quantum Bases

Computational Basis:
$|0\rangle = cos\,\theta|0\rangle + sin\theta|1\rangle$
$|1\rangle = cos\,\theta|0\rangle - sin\theta|1\rangle$

Qubit Basis:
$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$
$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

$|+i\rangle = \frac{|0\rangle + i|1\rangle}{\sqrt{2}}$
$|-i\rangle = \frac{|0\rangle - i|1\rangle}{\sqrt{2}}$

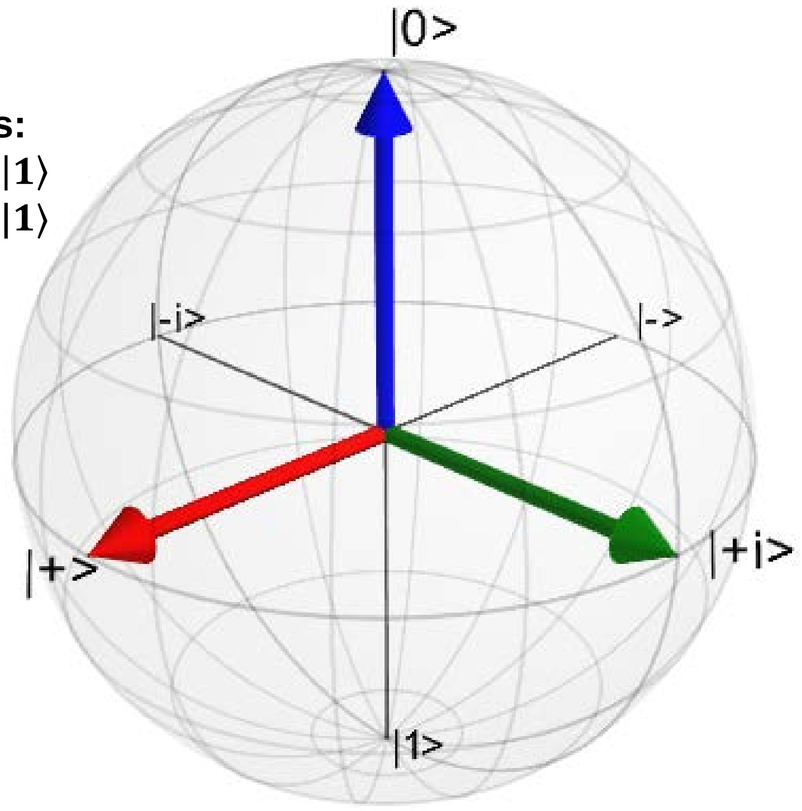

Fig 1: The representation of Quantum Basis in The Bloch Sphere

Secret Key Distribution

Trent sends to users $|\Upsilon(L)\rangle_{Tu} = \{|\Upsilon(1)\rangle_{Tu}, |\Upsilon(2)\rangle_{Tu}, \dots, |\Upsilon(L)\rangle_{Tu}\}$
where $|\Upsilon\rangle \in \{|\Psi^-\rangle, |\Psi^+\rangle, |\Phi^-\rangle, |\Phi^+\rangle\}$ Let $i = j = t + q + p = L$.
In each $|\Upsilon(i)\rangle_{TA}$ Trent keeps $|\Upsilon(i)\rangle_T$ and sends $|\Upsilon(i)\rangle_A$ to Alice
Alice choses $(t+q)/2$ then perform bell measurement, for example:
$|\Phi^+\rangle_{12} \otimes |\Phi^+\rangle_{34} = |\Phi^+\Phi^+\rangle_{1234}, |\Phi^-\Phi^-\rangle_{1234}, |\Psi^+\Psi^+\rangle_{1234}, |\Psi^-\Psi^-\rangle_{1234}$
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

$\|\delta^\pm\delta^\pm\rangle$					
Φ	+	Φ	+	0000
			−	0001
		Ψ	+	0010
			−	0011
	−	Φ	+	0100
			−	0101
		Ψ	+	0110
			−	0111
Ψ	+	Φ	+	1000
			−	1001
		Ψ	+	1010
			−	1011
	−	Φ	+	1100
			−	1101
		Ψ	+	1110
			−	1111

=0
=1

Fig 4: The representation of the states using the classical bits

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:

$|\Psi^-\rangle = |0\rangle|1\rangle - |1\rangle|0\rangle$
$|\Psi^+\rangle = |0\rangle|1\rangle + |1\rangle|0\rangle$
$|\Phi^+\rangle = |0\rangle|0\rangle + |1\rangle|1\rangle$
$|\Phi^-\rangle = |0\rangle|0\rangle - |1\rangle|1\rangle$

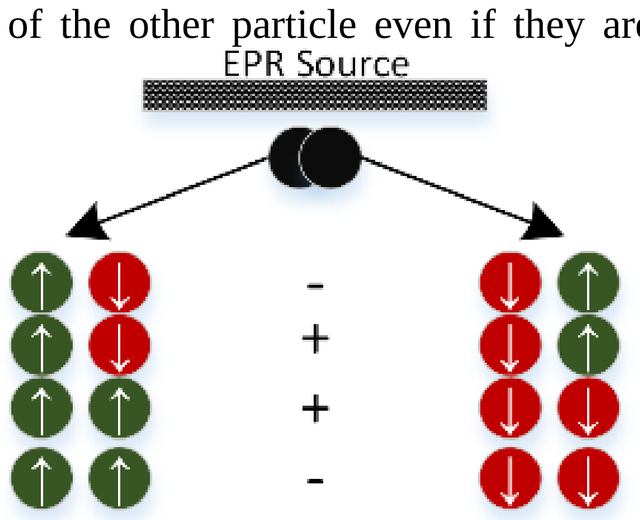

Fig 2: Maximally entangled quantum states

Building the Communication Channel

Trent reorders the p remaining pairs between him and the users
$|\Upsilon(i,j)\rangle_{Tu} = \{|\Upsilon(1)\rangle_{Tu}, |\Upsilon(2)\rangle_{Tu}, \dots, |\Upsilon(p)\rangle_{Tu}\}$ i=Alice, j=Bob
Trent make entanglement swapping for each $|\Upsilon(i)\rangle_{TA} \otimes |\Upsilon(j)\rangle_{TB}$
The result is an entanglement between Alice and Bob
Alice and Bob communicate using Teleportation,E91 or RSP

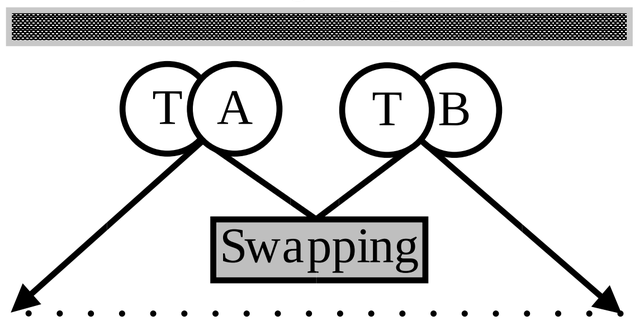

Fig 5: Entanglement swapping to create the quantum channel

References:

1- M. Naseri, "Revisiting Quantum Authentication Scheme Based on Entanglement Swapping," International Journal of Theoretical Physics, pp. 1-8, 2015.
2- L. Hardy and D. D. Song, "Entanglement-swapping chains for general pure states," Physical Review A, vol. 62, p. 052315, 2000.