Proceedings of ICCES'08, pp.1333-1337

The "Transportation" of the Message Using Private Keys

Gabriela Mogos[1]

Summary

This work presents a procedure of safe communication between two parts using a quantum channel. The procedure is based on the phenomenon of the entanglement of the qubits of a private key, and, those of the message which is to be transmitted.

Introduction

This work presents a way of protection of the messages sent between two parts who communicate through a quantum channel, using the qubits of the private key for the "transportation" of the message. The private key is obtained with the help of the Bennett-Brassard protocol, and it is not "one time pad", it is used until compromised by a third person. The first part of the work will present the way of obtaining the private key using the protocol Bennett-Brassard, the second part will present "the mixture" of the state of the qubits belonging to the key with the ones of the message, and the last part will present the extraction of the message from the row of qubits arriving at the receiver.

The transportation of the message with the help of the private key

The safe transportation procedure of the messages has the following steps:

- Setting the connection between the two parts who communicate and exchange messages;
- Obtaining the private key by the procedure Bennett-Brassard;
- Entanglement of the states;
- Transportation, reception and extraction of the message.

Obtaining the private key

The method of obtaining the private key is based on the Bennett-Brassard protocol and it is presented as follows.

The protocol uses four quantum states which form two bases, for example the states up $|\uparrow\rangle$ and down $|\downarrow\rangle$ - which form a base and the states left $|\rightarrow\rangle$ and right $|\leftarrow\rangle$ - another base. The bases are maximal conjugated, meaning that any pair of vectors, one from each base, is in the same state of superposition. Conventionally, the binary value 0 corresponds to the states $|\uparrow\rangle$ and $|\leftarrow\rangle$ and the value 1 corresponds to the other two states, which are called qubits states.

First, Alice is sending Bob individual spins in states chosen randomly from the four states. The random choice will be made by Alice in accordance with her own wish. The individual spins can be sent all at once, or one after the other, the only

[1] Computer Science Department, Al.I.Cuza University, Iasi, Romania

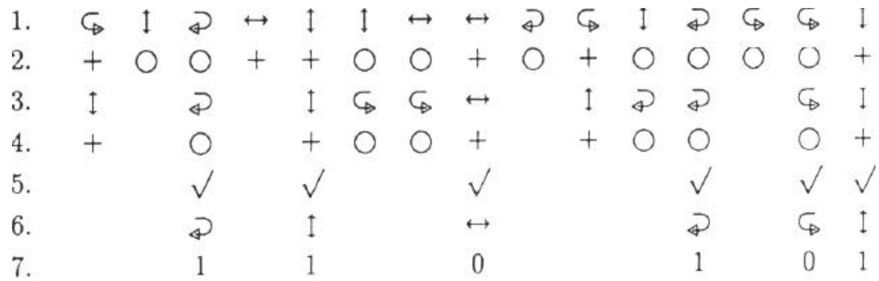

Figure 1: How to obtain the private key

restriction being that Alice and Bob should be capable to establish a one-to-one correspondence between the sending and the receiving of the spins. Then, Bob measures the spins received in one of the two bases, choosing it randomly. Thus, if they use the same base, they will obtain a perfect transmission, and if they use different bases, they will obtain uncorrelated results. Alice and Bob know which qubit is correlated (in one of the bases used by them) and which is not. The error correction scheme is: for every qubit Bob announces publicly in which base he will measure the corresponding qubit (but he will not communicate the result he gets). Then, Alice will say only if that base corresponds with the one she chose. If the state is compatible, they keep the qubit, if not, they will erase it. This way, approximately half of the bits will be lost. This means that Alice and Bob will share the same row of bits, called *raw key*. In the following steps, the two of them must extract the private key starting from the raw key.

Using the classic channel, Alice and Bob announce and compare their part of the raw key. Therefore, they can estimate an error rate R resulted from noises or from a possible intruder. If this rate is too big, they restart the protocol, if not, they execute a reconciliation of the information, of the bits left in their keys. This means the following: dividing the bits from their raw keys in subgroups of a length l. This length is chosen in such a way as to have more than an error on the whole length. On each subgroup, Alice and Bob will have a parity test (the parity P of a binary row $\{b_1, b_2, \ldots, b_l\}$ is defined as$P = b_1 \oplus b_2 \oplus \ldots \oplus b_l$), giving up the last bit every time. If the parity of the subgroups is different, then they will locate and erase the error bits through a binary search. They will divide the subgroup and they will have the parity test in the new groups obtained $(P_1 = b_1 \oplus b_2 \oplus \ldots \oplus b_{(l-1)/2})$ and$(P_2 = b_{(l-1)/2+1} \oplus b_{(l-1)/2+2} \oplus \ldots \oplus b_{(l-1)})$.

They will repeat the division of the groups each time when they realize that the parity is different, and each time they will erase the last bit from the groups whose parity is announced publicly. This way, they will avoid a possible intruder (Eve), and in the end Alice and Bob will share the same row of bits.

Entanglement of the states

How to obtain the private key is the most important step of the procedure. The second step of the procedure is the entanglement of the qubits of the message with the ones of the key, and the transportation of the message to the receiver. In fact, the qubits of the private key will have a very important part in this process, because with their help the transportation of the qubits of the message will be realized from the sender (Alice) to the receiver (Bob). The second step is as follows: after obtaining the key, the sender (Alice) will divide the message in sub-messages whose dimensions are equal to that of the private key (number of qubits from the key = number of the qubits from the sub-message). When the number of the qubits of the last sub-message is lower than the one of the private key, the qubits of the key will be send to the receiver un-entangled.

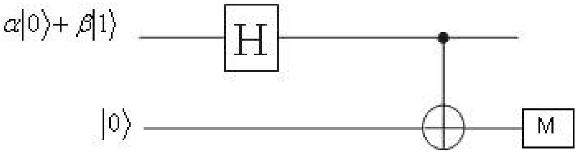

Figure 2: Entanglement of the states – the scheme

We will continue by studying the phenomenon of entanglement of the qubit states from a sub-message, represented by the generic state: $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with α and β unknown and a qubit of the private key considered in the state$|0\rangle$. For the entanglement of the states we will use the circuit from figure 2.

On the line above, the Hadamard gate will apply, and the state:

$$\begin{aligned} H:(\alpha|0\rangle+\beta|1\rangle) &= 1/\sqrt{2}[\alpha(|0\rangle+|1\rangle)+\beta(|0\rangle-|1\rangle)] \\ &= 1/\sqrt{2}(\alpha|0\rangle+\alpha|1\rangle+\beta|0\rangle-\beta|1\rangle) \\ &= 1/\sqrt{2}[(\alpha|0\rangle-\beta|1\rangle)+(\alpha|1\rangle+\beta|0\rangle)] \end{aligned}$$

will be obtained.

The next step is to apply the C-NOT gate, and the state of the qubit from the key will change as follows:

$$\begin{aligned} C-NOT :& 1/\sqrt{2}[(\alpha|0\rangle-\beta|1\rangle)+(\alpha|1\rangle+\beta|0\rangle)]|0\rangle \\ &= 1/\sqrt{2}(\alpha|00\rangle-\beta|11\rangle)+(\alpha|11\rangle+\beta|00\rangle) \\ &= 1/\sqrt{2}[\alpha(|00\rangle+|11\rangle)+\beta(|00\rangle-|11\rangle)] \end{aligned}$$

If we consider that:

$$1/\sqrt{2}(|00\rangle + |11\rangle) = \gamma_{00}$$
$$1/\sqrt{2}(|00\rangle - |11\rangle) = \gamma_{10}$$
$$1/\sqrt{2}(|01\rangle + |10\rangle) = \gamma_{01}$$
$$1/\sqrt{2}(|01\rangle - |10\rangle) = \gamma_{11}$$

are Bell bases, we can write the relation :

$$1/\sqrt{2}[\alpha(|00\rangle + |11\rangle) + \beta(|00\rangle - |11\rangle)] = \alpha\gamma_{00} + \beta\gamma_{10}$$

We can notice that the state of the qubit of the key can be measured using the Bell bases. For the qubits of the key left un-entangled, the measurement cannot be realized using the Bell bases.

Decrypting the message

Bob will receive the qubits and he will "read" them using the Bell bases. Knowing the private key, he will be able to extract the message with the help of the quantum gates used for the entanglement of the states (the quantum gates are reversible). If during the reading of the message Bob will notice the presence of the qubits which cannot be "read" using the Bell bases, he will think that Alice's message ended, and these qubits are in fact the ones left un-entangled of the private key. The communication is considered to be realized through an isolated quantum channel, and in the absence of an intruder (ideal conditions). When the communication is realized through a noisy channel, Bob will take into consideration the errors which can appear during the transmission (decoherence and redundance).

Conclusion

By the use of the quantum phenomena as quantum superposition, entanglement of the states, and quantum links, communication systems can be designed and implemented. They could always avoid intercepting, due to the fact that the measurements for a quantum carrier modify this one for ever, and thus the "traces" of the interception are left behind. Through the Bennett - Brassard method, keys can be created in order to offer "perfect safety". There is still a slight probability that parts of the recordings which were exchanged might be intercepted by a third part. The procedure presented in this work imposes the knowledge of the private key in order to be able to extract the message sent between the two parts who are communicating.

References

1. David P. DiVincenzo, *Quantum Gates and Circuits*, Proceedings of the Royal Society, London, 1997.

2. G. Johansson, *Quantum Algorithms-Lectures in Quantum Informatics*, applied Quantum Physics, MC2, Chalmers, S-412 96 Göteburg, Sweden, 2005.
3. Michael E. Nielsen, Isaac L. Chuang, *Quantum Computation and Quantum Information*, ISBN 0-521-63503-9, 2000.
4. Nikolas P. Papadakos, *Quantum Information Theory and Applications to Quantum Cryptography*, University of Athens, 2001.