An Approach of Quantum Cryptography Network Simulator

Norabdawahi Wahab[†] Hidekazu Tsuji[†] Hiroshi Yamamoto[†]
Graduate School of Engineering, Tokai University[†]

1. Introduction

In quantum cryptography, two parties, traditionally called Alice and Bob, wish to create a shared secret key that they can use to encrypt and decrypt their messages to each other. In future network based on quantum computer, spin used to create and polarize photon to build a secure quantum key. In the future of quantum network system, encrypted key could be transfer by cables and open air (laser beam). But without quantum computer, today's network quantum cryptography could be developing by transfer-encrypted key through optical fiber. Main of our research is to develop a secure network based on quantum cryptography through today's network cables. New approach of quantum key simulator using 3 computers Alice, Bob and Eve created to show the effective of quantum cryptography key transfer using today's network cables.

2. Rules and Ideas

Main idea is we are not developed spin photon and transfer it through quantum channel, but we develop a communication based of idea of quantum cryptography. Key transfer through today's network between two parties Alice and Bob while Eve is an eavesdropper. The idea is shown as Figure 1. Based on Quantum Cryptography principle, approach of communication simulation created. Protocol used is BB92 Protocol.

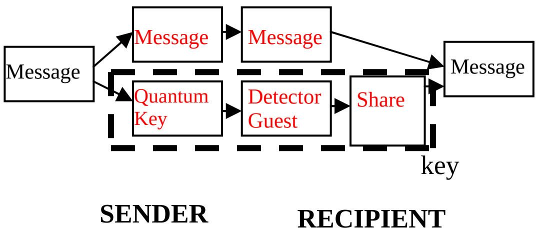


Figure 1

3. Rules of BB92 Protocol [1]

(1) Alice selects a string of random bits.
(2) Alice picks an alphabet (polarization set) for each bit and transmits one photon.
(3) For each photon received, Bob picks a random polarization and measures the photon.
(4) 50% of the time Bob will successfully measure Alice's bit.

4. Communication Rules

Here is the rule of Quantum Cryptography. Normally, it's happen between 2 people, Alice as sender and Bob as a receiver. Middle of their communication, there is Eve as eavesdropper [2].

4.1 Communication Method (Alice – Bob)

(1) Firstly Alice chooses bit's string randomly.
(2) Next Alice polarize set (choose her bases).
(3) Alice send bit's string to Bob
(4) Bob receives bit's string and using his detector, Bob choose randomly his bases.
(5) They compare the bases and make sure it is secure
(6) Bob publicly tells Alice which bits he received and they can both use them to form a key
(7) Lastly they discover and share bit's string and perform a secure key.
(8) Refer to Figure 2

4.2 Communication Method (Alice – Bob - Eve)

(1) Alice choose bit's string (polarize photon).
(2) Next Alice randomly chooses hers bases.
(3) Alice send bit's string to Bob
(4) Eve eavesdrop the bit's string and the photon has only 50% change going through Eve filter.
(5) Eve then has to form haft his bits randomly
(6) Bob receives bit's string and using his detector, Bob randomly choose his bases.
(7) They compare the bases found unusual in their shared bit's string.
(8) Alice send new key again to Bob.
(9) Refer to Figure 3

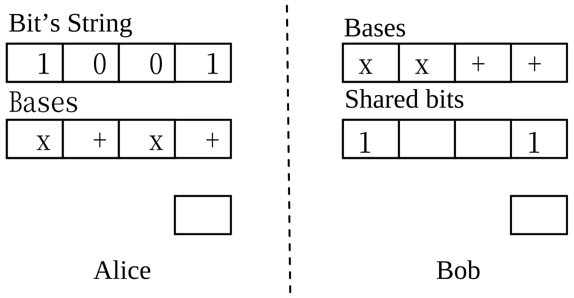


Figure 2

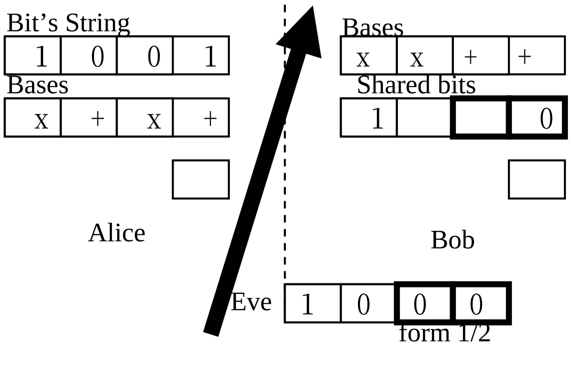


Figure 3

5. Environment

Java used to create random bases, sending secure bits as key, create key, comparing bases, and discover bit's string [3]. Encrypted Java key sent to receiver through networking to receiver port. Eve will try to eavesdrops Alice and Bob communication and when this happened, Alice's bits would automatically become haft (BB92 Protocol) and moves to left side of bits string. This infected key created by Java based on Java security.

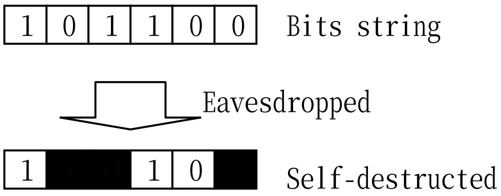
6. Key Infected

How do key distributed? The key transfers between sender and receiver by java class package. Ones the key been eavesdropped, it itself randomly desperate to pieces and haft of it will destroyed. Below shows how key's created.

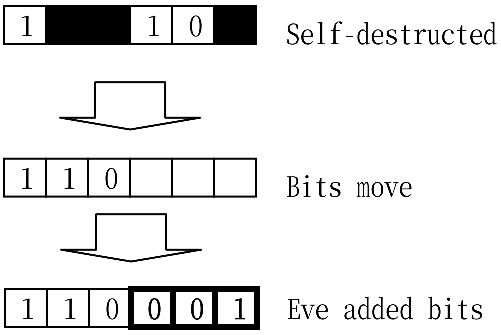
(1) Firstly key distributed by sender (Alice).

1 0 1 1 0 0

(2) Then Alice send the key to Bob but while sending the bits string eavesdropped by Eve.
(3) Eve, using her hacking software, tries to eavesdrop the bits string.
(4) Here is the point. When these bits string been read, randomly haft of the bits will self-destructed (gone).



(5) Even if Eve eavesdrop the bits string she never knows what bases Alice used to make a key. Then cause of half bits been self-destructed, Eve has to add her bits.
(6) Now once again problem came. The non-destructed bits will move to front automatically. So Eve has a problem to replace the empty bits.



(7) This will make unusual happened to bits string sending to Bob
(8) So when Bob and Alice comparing theirs shared bits string, they will the bits have been eavesdropped.
(9) This will make a complete secure transfer.

7. Results

In the one-time pad cipher, the key must be as long as the message itself, totally random, and used only once. Cause of this randomness, there are no patterns for a cryptanalyst to find and crack the key. It was not often used in the past because of the difficulty in making a large number of completely random keys, giving a copy to every sender, receiver and making sure the enemy didn't get a hold of keys. So, in secure way of algorithm, Bob and Alice's effort was directed to solve these problems. Quantum cryptography based network simulator creates a random key in the process of securely transmitting it to both sender and receiver, in such a way that eavesdropping is impossible.

But there will be a question. Is this really practically? So the answer of this question is "YES". We did a complete communication in our lab only used 3 machines and LAN as a cable. It doesn't need any quantum machine, spin photon machine or optical fiber. These 3 simulations (Alice, Bob and Eve) show great results. Low cost and very fast.

8. Conclusion

From our research and results, we had made conclusions as following below:

(1) BB92 Protocol could be used to perform high secure on today's network
(2) The simulations of BB92 Protocol quantum cryptography communication found the way to show a secure key transfer.
(3) New perfect transfer as alternative to quantum spin machine.
(4) Nice, fast, and low cost key transfer found to begin new world of cryptography.

The fact that today's encryption relies on a lack of number crunching power means that foundations of RSA aren't solid. It has never been proven that there are no easier ways to factor numbers. So if a method is discovered, RSA is obsolete. But because the encryption used today can theoretically be broken, given enough time and computational power, it is vulnerable. If useable quantum computer built, the strongest encryption we use today will become obsolete. But this has to change calculations of traditional computer and would cost a lot and takes time. Why don't we take quantum cryptography as a base of perfect key transfer on today's network?

9. References

[1] G. Brassard, R. Cleve et A. Tapp, « Cost of exactly simulating quantum entanglement with classical communication », Physical Review Letters, Vol. 83, no. 9, 30 août 1999
[2] Stephen D. Bartlett and Barry C. Sanders Efficient classical simulation of measurements in optical quantum information - presented at QCMC'02 (MIT, Boston, USA, July 22-26, 2002)
[3] Numerical simulation of information recovery in quantum computers - Pedro J. Salas, Angel L. Sanz - Phys. Rev. A, 2002