Is Quantum State in BB84 Protocol Really Unclonable?[1)]

Jeeun Lee, Sungsook Kim and Kwangjo Kim

School of Computing, KAIST

Abstract

Quantum key distribution (QKD) is believed as an unconditional secure solution of key sharing based on no-cloning theorem. The first QKD protocol, BB84, has been developed by resolving known attacks such as random number generators problem and photon number splitting attack which were discovered in practical implementation. In this paper, we introduce the weakness and countermeasure of BB84 with some concluding remarks.

Keywords: No-cloning theorem, quantum key distribution, BB84 protocol, random number generator, photon number splitting attack

I. Introduction

Quantum key distribution (QKD) has been believed to guarantee secure communication by detecting the presence of Eve using its unique quantum mechanical properties. While the traditional public-key cryptography depends on the computational difficulties of certain mathematical functions in key distribution, QKD relies on the foundations of quantum mechanics which makes secure against quantum computers. The most well-known QKD protocol, BB84, introduced a novel way of secure key sharing in theory, however, some attacks still has been discovered in practice. In this paper we explain BB84 protocol and its weakness and countermeasure.

The organization of this paper is as follows: In Section 2 we explain background of this paper. The weakness and countermeasure of BB84 protocol are introduced in Section 3. Finally we make a concluding remark in Section 4.

1) This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (No. NRF-2015R1A2A2A01006812).

II. Background

2.1 No-Cloning Theorem

Herbert [1] claimed a communication method faster than the speed of light using a superluminal communicator based upon a new kind of quantum measurement in 1981. Even if the reviewer of this paper, Peres [2], found theoretical error, he decided to publish Herbert's paper. Peres expected that finding the error would lead to significant progress in quantum information theory, and soon afterwards, the theoretical flaw of Herbert's paper was simply proved using the linearity of quantum mechanics.

If we assume that a device can produce an exact copy of an arbitrary quantum state, Eqs. (1) and (2) hold.

$$U(|\phi\rangle \otimes |s\rangle) = |\phi\rangle \otimes |\phi\rangle \quad (1)$$

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle \quad (2)$$

where U is unitary transformation, $\otimes$ is tensor product, $|\phi\rangle$ and $|\psi\rangle$ are arbitrary quantum states, and $|s\rangle$ is initial quantum state which we would like to make a copy. Taking inner product of Eqs. (1) and (2) gives

$$\langle\phi|\psi\rangle = (\langle\phi|\psi\rangle)^2 \qquad (3)$$

, *i.e.*, $\langle\phi|\psi\rangle = 0$ or 1 shows that U can only copy a set of orthonormal states. Therefore, copying an arbitrary unknown quantum state without altering the original is also impossible which we say *no-cloning theorem* [3,4]. This shows that Herbert's paper is wrong.

While any data has been copied and distributed under some instances, this theorem showed that this will never happen in quantum physics. This theorem was applied for secure key agreement protocol over the classical communication channel, generalized as no-broadcast theorem [5] and contributed to develop QKD.

2.2 BB84 Protocol

Most public-key cryptography is based on the difficulties of number-theoretical problems such as integer factorization or discrete logarithm, which can be broken in polynomial time if quantum computer implementing Shor's algorithm [6] appears. However, QKD depends on the quantum properties which guarantee secure communication against quantum computers. For example, an eavesdropper can be detected with high probability since the act of reading data changes the state.

The first QKD protocol is BB84 by Bennett and Brassard [8] described in Fig. 1, using two photon polarization states, rectilinear and diagonal bases, to transmit the information. In the first stage, Alice begins by choosing a random strings of bits over quantum channel. For each bit, Alice will randomly choose a basis and transmit a photon for each bit with the corresponding polarization to Bob. For every photon Bob receives, he will randomly choose basis and measure the photon's polarization. If Bob chooses the same basis as Alice for a particular photon, Bob should measure the same polarization and thus he can correctly infer the bit that Alice intended to send. In the second stage, Bob will notify Alice what basis he used to measure each photon through a public channel. Then Alice will report back to Bob whether he chose the

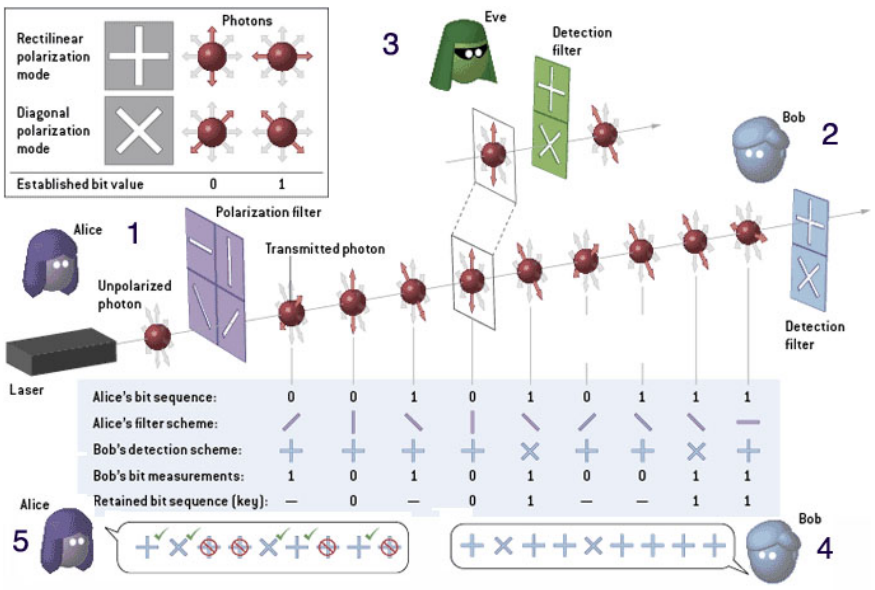

Fig. 1 BB84 Protocol [7]

correct basis for each photon. At this point Alice and Bob will discard the bits corresponding to the photons which Bob measured with a different basis. Provided no errors occurred or no one manipulated the photons, Alice and Bob should now both have an identical string of bits. In order to check the presence of Eve, Alice and Bob agree upon a random subset of the bits to compare to ensure consistency. If the bits agree, they are discarded and the remaining bits form the shared secret key. A disagreement in any of the bits compared would indicate the presence of an eavesdropper on the quantum channel. Finally, we can calculate the probability that identifying the presence of Eve for n bit as $P = 1 - (3/4)^n$, which implies the communication is more secure as n is bigger.

III. Weakness & Countermeasure of BB84 Protocol

3.1 Random Number Generator

A random number generator for cryptography must include that even if everything is known about the generator (schematic, algorithms, *etc.*) it still must produce totally unpredictable bits [9]. It is the most important aspect of cryptographic algorithms since the system could be attacked if the chosen numbers are not totally random. If the algorithms generate "random" sequences by following specific patterns (not completely random) then Eve can use the same algorithm to extract the information.

This problem was resolved in 1991 by Ekert, now called as E91 protocol [10]. This protocol uses peculiar quantum correlations known as entanglement property by simultaneously producing two entangled photon pairs. In this protocol there is a central source creating entangled particles and sending one to Alice and the other to Bob instead of Alice sending particles to Bob [11]. The outcome of Alice's measurement is random since Alice cannot decide which state to collapse the composite system into and cannot transmit information to Bob and solves the problem of random number generator.

3.2 Photon Number Splitting Attack

In practice the transmitted light pulses are not pure single-photon source and contain more than one photon according to a Poisson distribution,

$$p(n,\mu) = \frac{\mu^n e^{-\mu}}{n!} \qquad (4)$$

where n is photon number and μ is the mean photon number of the source [12]. There is always a finite chance that zero, two or even more photons will be emitted even if only one photon is emitted per pulse on average. When Alice sends more than one photon, Eve splits the extra photons, sends one copy to Bob and keeps one copy for herself until Bob detects the remaining single photon and Alice reveals the encoding basis. Then Eve can measure her stored photons in correct basis and obtain information without detection.

There have been several solutions to this problem. The most promising solution is using decoy states protocol that Alice intentionally sends same copy of her laser pulses and compare the final photon numbers Bob received. Eve can be detected by comparison of photon numbers

since she doesn't know which pulses are signal or decoy and tries to steal all of them [12,13].

IV. Concluding Remarks

We introduced the weakness and countermeasure of BB84 protocol which suggested the secure key distribution using no-cloning theorem. However, there are some restrictions in implementation guaranteeing random number generator or pure single-photon source. Several different approaches are being developed to overcome this restrictions but still the practice is not perfect.

In other words, QKD was believed as a perfect solution of key sharing based on no-cloning theorem in 1980s but many possible attacks are discovered until now. In order to provide unconditional security, other conditions should be satisfied such as physically not accessible to Alice and Bob's encoding and decoding devices, unconditionally secure authentication, protocol failure, and message encryption using one-time pad, *etc.* Finding other attacks and their countermeasure which are not discussed here can be a challenging issue.

References

[1] N. Herbert, FLASH-A Superluminal Communicator Based Upon a New Kind of Quantum Measurement, *Found. Phys.* **12**, 1171-1179 (1982)

[2] A. Peres, How the no-cloning theorem got its name, *Fortschr. Phys.* **51**, 458-461 (2003)

[3] W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, *Nature* **299**, 802-803 (1982)

[4] D. Dieks, Communication by EPR devices, *Phys. Lett. A* **92**, 271-272 (1982)

[5] H. Barnum, C. M. Caves, C. A. Fuchs et al., Noncommuting Mixed States Cannot Be Broadcast, *Phys. Rev. Lett.* **76**, 2818-2821 (1996)

[6] P. W. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, *SIAM Rev.* **41**, 303-332 (1999)

[7] https://www.dhushara.com/paradoxhtm/quant/crypt.jpg

[8] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 175-179 (1984)

[9] M. Stipčević, Quantum random number generators and their use in cryptography, *MIPRO Proceedings of the 34th International Convention*, 1474-1479 (2011)

[10] A. K. Ekert, Quantum cryptography based on Bell's theorem, *Phys. Rev. Lett.* **67**, 661-663 (1991)

[11] N. Ilic, http://www.ux1.eiu.edu/~nilic/Nina's-article.pdf

[12] W.-Y. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, Phys. Rev. Lett. **91**, 057901 (2003)

[13] H.-K. Lo, X. Ma and K. Chen, Decoy State Quantum Key Distribution, *Phys. Rev. Lett.* **94**, 230504 (2005)