A Simulative Comparison of BB84 Protocol with its Improved Version

Mohsen Sharifi[1] and Hooshang Azizi
Computer Engineering Department
Iran University of Science and Technology, Tehran, Iran
Emails: {msharifi, hazizi}@iust.ac.ir

ABSTRACT

Public key cryptosystems can well become void with the advent of incredibly high performance quantum computers. The underlying principles of these computers themselves, namely quantum mechanics, provide the solution to the key distribution problem. This paper explains how cryptography will be benefited from quantum mechanics, through a short introduction to classical cryptography, and the general principles of quantum cryptography and the BB84 protocol for key distribution. Then we review a modification to the BB84 protocol that is logically claimed to increase its efficiency. We then validate this claim by presenting our simulation results for BB84 and its improved protocols and show that the efficiency of the improved protocol could be doubled without undermining the security level of BB84 protocol.

Keywords: Cryptography, BB84 Protocol, Quantum Cryptography, Quantum Key Distribution.

1. INTRODUCTION

Although public-key cryptosystems, especially with large and randomly generated keys, are safe within the context of current technology, they can well become void when incredibly high performance quantum computers come into real existence and use. A quantum algorithm with polynomial time for factorization has already been discovered [1], so if quantum computers become a reality, RSA and other public-key cryptosystems would become obsolete. This is where quantum cryptography comes to the rescue, offering a new solution to the key distribution problem by using the quantum mechanics principles.

Quantum cryptography, better named quantum key distribution, allows Alice and Bob to create a random secret key based on quantum mechanics and to verify that the key has not been eavesdropped [2,3,4]. Quantum cryptography is based on the principles of quantum physics, for example, measurement of photon polarization with incompatible basis modifies the photon polarization. Also one cannot measure simultaneously the polarization of a photon in the rectilinear and the diagonal bases. These facts are the core of quantum key distribution protocols.

Various schemes for quantum cryptography have been proposed, such as B92, BB84, and EPR [2,4]. For brevity, we will consider the well-known scheme BB84. B92 is similar to BB84, and EPR exploit quantum entanglement.

2. BB84 PROTOCOL

BB84 protocol was proposed by Bennett and Brassard [5]. Between Alice and Bob two channels are needed: quantum and classical. Alice sends photons to Bob through quantum channel. Then they use classical channel to agree on the same key based on transmitted photons. BB84 Protocol consists of three steps: raw key extraction, key error correction, and privacy amplification. Raw key extraction is as follows:

1. Alice sends Bob a sequence of photons randomly polarized.

[1] Corresponding Author

2. For each photon, Bob randomly chooses rectilinear or diagonal bases to measure it.
3. Bob announces to Alice his bases (but not results).
4. Alice transmits back which measurements are done in compatible bases.
5. Alice and Bob throw away photons measured in incompatible bases, decoding remaining photons to 0 and 1 that make the raw key.

Their raw keys must be the same if no eavesdropping has occurred. So, they compare some bits of their raw keys for eavesdropping.

For security analysis [6], let us assume Eve eavesdrops and measures a photon. With probability $1/2$, Eve's measurement is done in incompatible basis and modifies the photon polarization. Then Bob measures the modified photon, and photon polarization modifies and with probability $1/2$ become different from Alice's polarization. Thus, Alice and Bob's photon polarization is different with probability $1/2 * 1/2 = 1/4$. This means that the probability of successful eavesdropping is $3/4$. If Eve measures n photons, she does not modify their polarization with the probability $(3/4)^n$ that goes to zero as n grows, therefore her eavesdropping is detected with near certain probability.

Error may appear in raw key due to noisy environment. If raw keys of Alice and Bob differ due to environment noise, they must remove all differences, producing an error free common key. This process is called error correction and various schemes could be applied [2,3], for example 2D parity check scheme. In the scheme, Alice and Bob organize their raw keys into 2D square matrix and exchange parities of the rows and columns. Any row or column that has different parities is discarded. To ensure privacy, also diagonals of matrix are discarded. After error correction, Eve may have partial information of the key. Thus Alice and Bob need to lower down Eve's information to an arbitrary low value using some privacy amplification protocols [2,3].

The data rate and transmission length are two values of interest for quantum key distribution [4,7]. According to quantum bit error rate (QBER) and raw key rate, a general formula could be deduced for them [4,7]. The raw key rate is the product of the pulse rate ν, the average number of photons per pulse μ, the transfer efficiency η_t, and the detector efficiency η_d:

$$R_{raw} = \frac{1}{2} \nu \mu \eta_t \eta_d \qquad \text{Eq. (1)}$$

The factor $1/2$ is due to the bases incompatibility. The transfer efficiency can be expressed as:

$$\eta_t = 10^{-\frac{L_f l + L_B}{10}} \qquad \text{Eq. (2)}$$

where L_f is the losses in the fiber in dB/km, l is the length of fiber, and L_B is internal losses at Bob in dB.

Two factors may cause errors in raw key, imperfect detector and dark count. Imperfect detector introduce $R_{opt} = R_{raw}\ p_{opt}$ errors in raw key where p_{opt} is the probability of wrong detection of polarization. $R_{\det} = \frac{1}{4}\ \nu\ p_{dark}$ errors arise from dark count (photon detection when there are no photons) where p_{dark} is the probability to get a dark count. The QBER is defined as the ratio of wrong bits to total received bits:

$$QBER = \frac{R_{\text{wrong}}}{R_{\text{wrong}} + R_{\text{right}}} \approx \frac{R_{\text{error}}}{R_{\text{raw}}} = \frac{R_{\text{opt}} + R_{\text{det}}}{R_{\text{raw}}} = p_{\text{opt}} + \frac{p_{\text{dark}}}{2\,\mu\,\eta_{\text{t}}\,\eta_{\text{d}}} = QBER_{\text{opt}} + QBER_{\text{det}} \qquad \text{Eq. (3)}$$

Tancevski [7] has estimated the fraction of bits lost due to error correction as:

$$r_{ec} = QBER\ (\tfrac{7}{2} - \log_2^{QBER}) \qquad \text{Eq. (4)}$$

and the fraction of bits lost due to privacy amplification as:

$$r_{pa} = 1 + \log_2^{(\frac{1+4QBER-4QBER^2}{2})} \quad \text{Eq. (5)}$$

So the final bit rate is:

$$R_{final} = (1 - r_{ec})(1 - r_{pa})R_{raw} \quad \text{Eq. (6)}$$

As transmission length l increases, transfer efficiency η_t falls rapidly down, which in turn causes more errors in raw key and a decrease in the final bit rate to zero. So the maximum transmission length could be computed.

The first experimental demonstration of quantum key distribution was performed in 1989 over 30 cm in air [5]. Since then, the field has progressed remarkably. At Los Alamos National Laboratories, secret key have been transmitted in optical fiber over 67 km [8], and up to 10 km in free space [9].

One of the main drawbacks of quantum cryptography though is that it provides no mechanism for authentication. Some drawbacks such as limited distance and limited data rate are technological and must be solved before quantum cryptography can be used widely in the market [10].

3. IMPROVED BB84

Since Alice and Bob choose the two bases with the same probability, the probability of Alice and Bob's basis compatibility is $(½)(½)+(½)(½)=½$, so half of the photons are thrown away. Ardehali et al. [11] has proposed an improvement that decreases discarded photons, thereby increasing the bit rate of the protocol. The basic idea is that Alice and Bob choose the two bases with different probabilities, rectilinear basis with probability α and diagonal basis with probability $1-\alpha$, so they choose the same basis with probability:

$$P_\alpha = \alpha^2 + (1-\alpha)^2 \quad \text{Eq. (7)}$$

which goes to 1 as α goes to zero. This means that Alice and Bob' bases of almost all photons are the same, so the bit rate of protocol could be doubled.

With the modification, the probability of choosing diagonal basis for a photon is:

$$\frac{(1-\alpha)^2}{\alpha^2 + (1-\alpha)^2} \quad \text{Eq. (8)}$$

which goes to 1 as α goes to zero, so bases of almost all photons are diagonal and protocol could be defeated because Eve can use the diagonal basis and measures polarization of many photons without modifying them and causes a few error. To prevent the attack, error estimation is refined. In contrast to the BB84 protocol, which estimates a single error rate, two error rates e_1, e_2 are estimated in the refined protocol: e_1 when Eve uses diagonal basis while Alice and Bob use rectilinear basis, and e_2 when Eve uses rectilinear basis while Alice and Bob use diagonal basis. The final error rate is the maximum of e_1, e_2. Now if Eve measures photons along the diagonal basis, although e_2 is zero, e_1 increase (about 50%), so the final error is high and eavesdropping is detected.

Let us assume Eve measures each photon along the rectilinear basis with probability p_1, along the diagonal basis with probability p_2, and does not measure with probability $1-p_1-p_2$. If Alice and Bob use the rectilinear basis and Eve uses the diagonal basis, Alice and Bob's polarization is different with probability ½, so $e_1 = p_2/2$ because Eve chooses diagonal basis with the probability p_2. Similarly, $e_2 = p_1/2$. Note that e_1, e_2 are independent of the value of α and only depend on Eve's eavesdropping strategy, so the improved protocol is as secure as BB84 protocol. Although smaller α leads to higher bit rate, it leads to fewer rectilinear polarized photons and if number of rectilinear polarized photons is too few, e_1 could not be accurate. Thus according to the number of total photons, the appropriate value of α must be adapted.

4. SIMULATION OF IMPROVED BB84

In this section, we present simulation results of BB84 and its improved protocols that include comparing efficiency and security. Efficiency means key bit rate and security means raw key error rate vs. eavesdropping rate.

We simulate quantum channel and photon transfer, implement error estimation, error correction, and privacy amplification. Also we simulate Eve's eavesdropping when we evaluate security of protocols. We simulate 1300 *nm* fiber optic that its loss is $L_B = 0.35\,{}^{dB}\!/_{km}$. In the 1300 *nm* wavelength, the efficiency of photon detector is $\eta_d = 0.20$ and the probability of dark count is $p_{dark} = 10^{-5}$. Loss at photon detector L_B and error due to imperfect detector $QBER_{opt}$ are ignored because their values are small. The average number of photons per pulse is $\mu = 0.1$ and 10^7 pulses were used in the simulation. 10% of raw key were compared in the error estimation. We have used a 10*10 matrix for error correction and repeated error correction process until no error found. We repeated the simulation 100 times and deduced the results according them, so we think that results are reliable.

Three different values were chosen for efficiency comparison: $(0.50,\ 0.15,\ 0.02)$. As mentioned before, the probability of Alice and Bob's basis compatibility is $P_\alpha = \alpha^2 + (1-\alpha)^2$ so:

$$\alpha = 0.50 \Rightarrow P_{0.50} = 0.50^2 + 0.50^2 = 0.50$$

$$\alpha = 0.15 \Rightarrow P_{0.15} = 0.15^2 + 0.85^2 = 0.745$$

$$\alpha = 0.02 \Rightarrow P_{0.02} = 0.02^2 + 0.98^2 = 0.9608$$

$$P_{0.15}/P_{0.50} = 1.49$$

$$P_{0.02}/P_{0.50} = 1.936$$

Simulation results shown in Figure 1 validate the same conclusion: *the ratio of bit rate with* $\alpha = 0.15$ *to the bit rate with* $\alpha = 0.50$ *(original BB84) is almost 1.5, and also the bit rate with* $\alpha = 0.15$ *to the bit rate with* $\alpha = 0.50$ *(original BB84) is almost 1.9.*

For security comparison, the raw key error rate vs. eavesdropping rate was computed, as shown in Figure 2. The curves for different values of α are similar. This means that any detectable eavesdropping in BB84 protocol is detectable in the improved protocol. We assume Eve could determine pulses that have more than a photon, measure a photon of the pulse and send remaining photons of the pulse to Bob, so her eavesdropping is not detectable. However 5% of non-empty pulses have more than a photon and Eve couldn't devise successful attack. Also we assumed Eve choose two bases with the same probability.

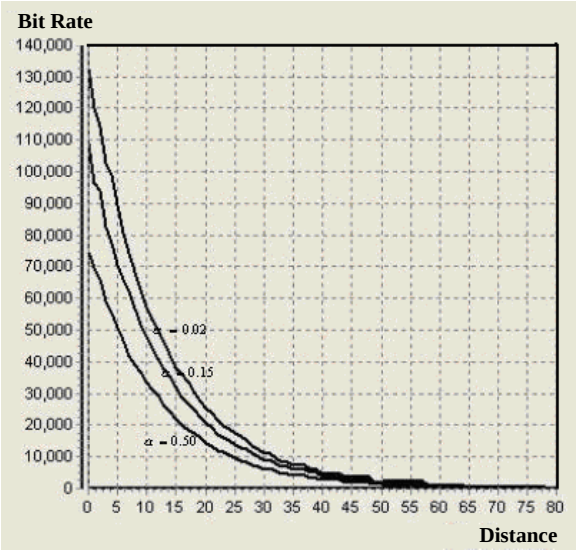

Figure 1: Efficiency vs. transmission length of BB84 and its improved protocols

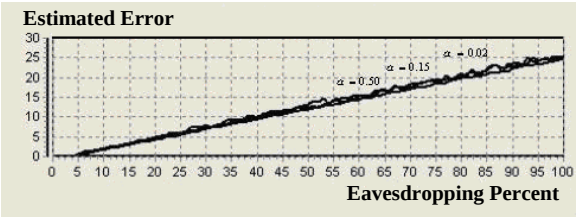

Figure 2: Error rate vs. eavesdropping rate of BB84 and its improved protocols

Eve could choose the bases with different probabilities; the simulation results of this

behavior are shown in Figure 3. We chose three values for eavesdropping (10%, 50%, and 100%) and for each value, the raw key error rate vs. eavesdropping rate were computed. Choosing two bases with the same probability, results in a detectable minimum error rate.

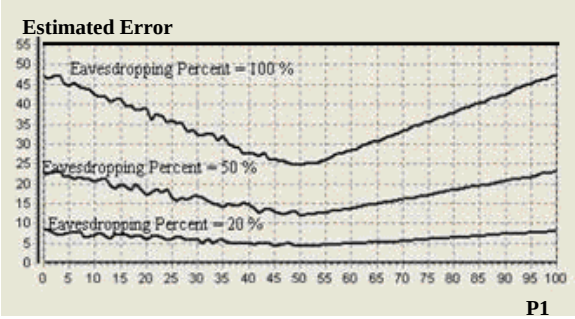

Figure 3: Error rate vs. diagonal bases percent of BB84 and its improved protocols

5. CONCLUSION

Quantum cryptography offers a new solution to the key distribution problem. Its security is based on principles of quantum mechanics. BB84 is a protocol for key distribution using these principles, but with the deficiency of losing half of the photons when different bases are used. We have reviewed an available refinement to BB84 protocol that could logically increase its efficiency. The refinement involves using rectilinear and diagonal bases with different probabilities. We have simulated the BB84 and its refined version and have shown facts and figures that in comparison with the BB84, the efficiency of the refined protocol could be almost doubled without affecting the security of BB84.

6. REFERENCES

[1] P. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", SIAM Journal of Computing, 26, 1997.

[2] S. J. Lomonaco, "A Talk on Quantum Cryptography or How Alice Outwits Eve", Preprint at Los Alamos Physics Preprint Archive, 2001 http://xxx.lanl.gov/abs/quant-ph/0102016

[3] V. Volovich, and Y. I. Volovich, "On Classical and Quantum Cryptography", Preprint at Los Alamos Physics Preprint Archive, 2001 http://xxx.lanl.gov/abs/quant-ph/0108133

[4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum Cryptography", Group of Applied Physics, University of Geneva, 2001.

[5] H. Bennet, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental Quantum Cryptography", Journal of Cryptography, Vol. 5, 1992, pp. 3-28.

[6] D. Mayers, "Unconditional Security in Quantum Cryptography", Preprint at Los Alamos Physics Preprint Archive, 1998 http://xxx.lanl.gov/abs/quant-ph/9802025

[7] H. Zbinden, H. Bechmann-Pasquinucci, N. Gisin, and G. Ribordy, "Quantum Cryptography", Applied Physics B 67, 1998, pp. 743-748.

[8] D. Stucki, N. Gisin, O. Guinnard, G. Riordy, and H. Zbinden, "Quantum Key Distribution over 67 km with a Plug & Play System", New Journal of Physics 4, 2002.

[9] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, "Practical Free-Space Quantum Key Distribution over 10 km in Daylight and at Night", Preprint at Los Alamos Physics Preprint Archive, 2002 http://xxx.lanl.gov/abs/quant-ph/0206092

[10] H. K. Lo, "Will Quantum Cryptography Ever Become a Successful Technology in the Marketplace?", MagiQ Technologies Inc., 2001.

[11] M. Ardehali, H. F. Chau, and H. K. Lo, "Efficient Quantum Key Distribution", Preprint at Los Alamos Physics Preprint Archive, 1999 http://xxx.lanl.gov/abs/quant-ph/9803007

Received: Nov. 2005. Accepted: Jul. 2007.