Security Analysis of Biased Basis for Efficient BB84

Hiroki Yamamuro[a], Shohei Beppu[b], Kazuhide Fukushima[c] and Shinsaku Kiyomoto[d]
KDDI Research, Inc., 2-1-15 Ohara, Fujimino, Saitama, 356-8502, Japan
{*hi-yamamuro, sh-beppu, ka-fukushima, sh-kiyomoto*}*@kddi.com*

Keywords: Quantum Key Distribution, Efficient BB84, Intercept-Resend Attack.

Abstract: Quantum key distribution (QKD) is a secure protocol for exchanging a secret key that is based on the principles of quantum physics and fulfills information-theoretical security requirements. The first QKD protocol, BB84, was proposed in 1984. Bit information is sent via four types of quantum states, combining two types of the bits and bases in BB84. However, half of the bits are discarded after the basis information is exchanged since a sender and receiver select a basis equally likely. Lo et al. (J. Cryptol.'05) proposed Efficient BB84, in which basis selection is biased to improve the efficiency. The biased basis selection increases the probability that the selected bases match, which results in fewer bits being discarded. This letter describes an attack method against Efficient BB84 that exploits the bias in basis selection and analyzes the security of the method. An eavesdropper intercepts the first part of the quantum states, performs measurements in the basis with high selection probability, and obtains bit information without being detected. We then evaluate the extent to which the obtained bit information compromises the security of the secret key.

1 INTRODUCTION

1.1 Background

Encryption algorithms are essential to ensure the confidentiality of messages for secure communication. A sender and receiver need to exchange a secret key to encrypt messages. Key exchange protocols based on public-key cryptography, such as RSA and Diffie–Hellman, are widely used. These protocols are based on computationally secure mathematical problems, whereas in the field of quantum computing, a quantum algorithm called Shor's algorithm (Shor, 1994) was proposed. Shor's algorithm overcomes these mathematical problems, which means that with the development of quantum computers, there is a risk that the currently used protocols for secret key exchange will be compromised.

Several solutions have been proposed to address this risk. One promising solution is quantum key distribution (QKD). QKD is a secure protocol for exchanging a secret key that is based on the principles of quantum physics and provides information-theoretic security, not computational security. The best-known QKD protocol is BB84, which was proposed by Bennett and Brassard (Bennett and Brassard, 1984) in 1984. Four types of quantum states are used, combining two types of the transmission bits and transmission bases in BB84. A sender (Alice) firstly sends the quantum states calculated from one randomly selected bit and basis to a receiver (Bob). Bob randomly selects one of two measurement bases and measures the received quantum states. Alice and Bob publicly exchange information about the selected bases and discard bits for which the selected bases do not match. Alice and Bob compare a subset of the remaining bits and calculate the quantum bit error rate (QBER), which is used to detect an eavesdropper (Eve). If the QBER exceeds the threshold, the protocol is initiated. Otherwise, Alice and Bob perform the key distillation process to correct bit errors and remove leaked information and share a secret key.

The basis selection method provides the same probability of being selected for both bases and the probability that the bases match is $1/2$. The method is inefficient due to half of the bits being discarded. An efficient version of BB84 (Efficient BB84) was proposed by Lo, Chau, and Ardehali (Lo et al., 2005). Alice and Bob do not select each basis equally, which biases the selection probability in Efficient BB84. In other words, there are a basis with low selection probability (minority basis) and a basis with high selection

[a] https://orcid.org/0009-0004-5559-291X
[b] https://orcid.org/0000-0002-8220-9515
[c] https://orcid.org/0000-0003-2571-0116
[d] https://orcid.org/0000-0003-0268-0532

Yamamuro, H., Beppu, S., Fukushima, K. and Kiyomoto, S.
Security Analysis of Biased Basis for Efficient BB84.
DOI: 10.5220/0013245800003899

In *Proceedings of the 11th International Conference on Information Systems Security and Privacy (ICISSP 2025) - Volume 2*, pages 571-574
ISBN: 978-989-758-735-1; ISSN: 2184-4356

probability (majority basis). Fewer bits are discarded by increasing the probability that the bases match, which results in higher efficiency. Lo et al. also introduced a refined calculation method for the QBER in line with the basis selection bias. Alice and Bob calculate the QBER for each basis, not for both bases together. The calculation method for the QBER prevents an intercept-and-resend (I-R) attack, in which Eve intercepts quantum states from Alice, measures them, and resends the same quantum states to Bob as the measurement results. The interception of all quantum states that is measured only in the majority basis is detected by increasing the QBER on the minority basis. However, the above mentioned method is applicable to the case of intercepting all quantum states and the case of intercepting only a portion of the quantum states is not considered. The greater the bias in basis selection, the smaller the probability that both Alice and Bob select the minority basis. Eve is therefore able to intercept quantum states without being detected if she attacks only a part of them.

1.2 Contribution

This letter considers a variant of the I-R attack using only the majority basis, in which Eve intercepts only a part of the quantum states, particularly the initial part. We firstly calculate the probability that the attack is detected, (i.e., the probability of increasing the QBER on the minority basis). We estimate the number of bits until the first detection on the basis of the calculated probability and the properties of the geometric distribution. The estimated value is the number of bits to intercept. We then calculate the proportion of the successful attack among the intercepted bits and estimate the number of correctly intercepted bits. The attack succeeds if Eve guesses the correct basis and receives the same bits as Alice and Bob. We finally evaluate the impact on the security of the secret key via the acquired bits corresponding to the value of the bias. Since the bits, including the bits we did not obtain in our attack, are randomized in the key distillation process, we do not obtain the bit sequence of the secret key itself. Instead, we discuss the extent to which the obtained bits affect the security of the secret key, particularly its entropy.

1.3 Related Works

We review some basic attacks against BB84.

A simple attack is I-R attack (Bennett and Brassard, 1984) mentioned above. Fake-State (F-S) attack (Makarov and Hjelme, 2005) is a variant of I-R attack, which exploits the weakness of Bob's detector.

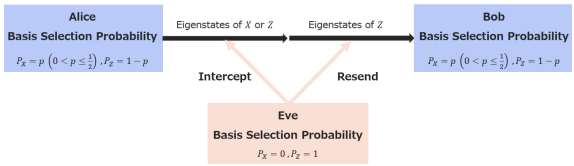

Figure 1: Our Attack Model.

F-S attack utilizes quantum states that are detected by the Bob in a manner controlled by Eve, instead of the quantum states that were intercepted and measured.

Photon number splitting (PNS) attack (Huttner et al., 1995; Brassard et al., 2000; Lütkenhaus, 2000) uses the existence of the quantum states with multi-photon such as weak coherent states, not single-photon. Eve firstly intercepts the quantum states from Alice, blocks them in the case of single photons, and in the case of multiple photons, splits off one photon and sends the rest to Bob. Eve then acquires the bit information by obtaining the basis information exchanged between Alice and Bob and measuring in the same basis.

2 ATTACK MODEL

We denote the minority basis as X, the majority basis as Z, the selection probability of the X basis as P_X, and the selection probability of the Z basis as P_Z. Owing to the bias in basis selection, we set $P_X = p\ (0 < p \leq 1/2)$ and $P_Z = 1 - p$.

An overview of our attack model is shown in Figure 1. Intuitively, we take advantage of the fact that the Z basis is chosen more often because of the basis selection bias. Eve intercepts quantum states from Alice, measures them in the Z basis selected with probability 1, and resends the same quantum states to Bob as the measurement results. The quantum states sent by Alice are the eigenstates of the X basis or Z basis depending on the probabilities P_X and P_Z, whereas the quantum states received by Bob are the eigenstates of the Z basis resent by Eve. If our attack fails (i.e., the QBER calculated by Alice and Bob exceeds the threshold), the information for the key distillation process is not exchanged over classical communication and the protocol is restarted from the beginning. Eve is therefore able to confirm whether the attack has been successful or failed. If the attack fails, it is repeated on the protocol that is restarted.

3 SECURITY ANALYSIS

This section evaluates the entropy loss of the secret key due to our proposed attack. We firstly calculate the probability that our attack is detected for our attack model. The detection of our attack occurs in the case in which both Alice and Bob select the X basis, whose measured bits differ. Since the probability that both Alice and Bob select the X basis is p^2 and the probability that their measured bits differ is $1/2$, the detection probability is $p^2/2$. The average number of eavesdropping bits until our attack is first detected is $2/p^2-1$ bits when Eve implements our attack from the first quantum state by utilizing the expected value of the geometric distribution. Eve thus obtains the first $2/p^2-1$ bits without being detected.

We then calculate the proportion of the successful attack among $2/p^2-1$ bits. The successful attack occurs in the case in which under the condition that our attack is not detected, the basis chosen by both Alice and Bob is either the X basis or Z basis and the measured bits of Alice, Bob, and Eve are all the same. The probability that both Alice and Bob select the X basis is p^2, and in this case, the probability that the measured bits of Alice, Bob, and Eve are all the same is $1/4$. The probability that both Alice and Bob select the Z basis is $(1-p)^2$, and in this case, the probability that the measured bits of Alice, Bob, and Eve are all the same is 1. Since the probability of not being detected is $1-p^2/2$, the proportion of the successful attack is

$$\frac{p^2\times\frac{1}{4}+(1-p)^2\times 1}{1-\frac{p^2}{2}}=\frac{5p^2-8p+4}{-2p^2+4}.$$

Thus, the number of bits that are successfully attacked among $2/p^2-1$ bits is

$$\left(\frac{2}{p^2}-1\right)\times\frac{5p^2-8p+4}{-2p^2+4}$$
$$=\frac{5p^4-8p^3-6p^2+16p-8}{2p^4-4p^2}.$$

The above mentioned value is the number of bits after exchanging the information of the selected basis. Although the randomization of bits in the key distillation process does not allow for obtaining the bit sequence of the secret key, it is possible to evaluate the entropy loss of the secret key. Some bits are discarded in the QBER calculation process and key distillation process to obtain a secret key. We assume that half of the bits are consumed in the QBER calculation process and $2H_2(\mathrm{QBER})$ proportion of bits in the key distillation process for the sake of simplicity. H_2 represents the binary entropy function, where $H_2(x)=-x\log_2(x)-(1-x)\log_2(1-x)$. Our attack

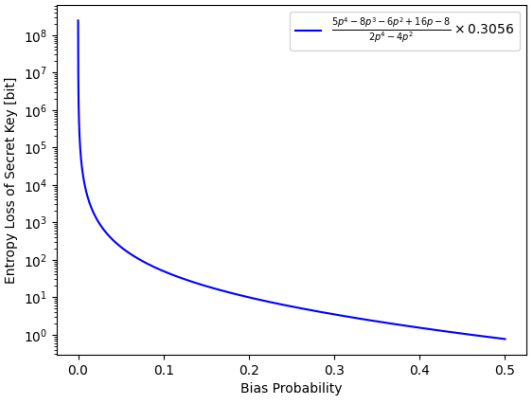

Figure 2: Entropy Loss of Secret Key.

increases the QBER only in the case in which both Alice and Bob choose the minority basis and their measured bits differ. We consider the influence of channel noise and assume that QBER $=0.03$ holds. Therefore, the number of secret key bits whose entropy decreases due to our attack is

$$\frac{5p^4-8p^3-6p^2+16p-8}{2p^4-4p^2}\times 0.5\times(1-2H_2(0.03))$$
$$=\frac{5p^4-8p^3-6p^2+16p-8}{2p^4-4p^2}\times 0.3056.$$

The entropy loss of the secret key corresponding to the biased probability p is shown in Figure 2.

The entropy loss of the secret key increases when the value of p is reduced to improve the efficiency from Figure 2. This result means that the bias in basis selection affects the security of the secret key.

4 DISCUSSION

We discuss the validity of the number of intercepted bits from the beginning. If our attack is successful, we obtain the number of intercepted bits. Otherwise, we do not obtain any bits. Let the number of intercepted bits be n. Since the attack success probability is $(1-p^2/2)^n$, the expected value of the obtained bits is $n(1-p^2/2)^n$. The expected value is maximized by $n_{max}=-1/\ln(1-p^2/2)$. Because we compare the relationship between the values of $(2/p^2-1)$ and n_{max}, we show that the following inequality holds

$$-\frac{1}{\ln(1-\frac{p^2}{2})}-1<\frac{2}{p^2}-1<-\frac{1}{\ln(1-\frac{p^2}{2})}.$$

Since $\ln(1-p^2/2)<0$ and $2/p^2>0$ hold for $0<p\leq 1/2$, the left side of the above inequality is transformed to

$$p^2<-2\ln\left(1-\frac{p^2}{2}\right)$$

and the right side is transformed to

$$-(2-p^2)\ln\left(1-\frac{p^2}{2}\right) < p^2.$$

We firstly show $p^2 < -2\ln(1-p^2/2)$ and set

$$f(p) = -2\ln\left(1-\frac{p^2}{2}\right) - p^2.$$

We have $f(p) > f(0) = 0$ i.e. $p^2 < -2\ln(1-p^2/2)$ holds since

$$f'(p) = \frac{2p^3}{2-p^2} > 0$$

holds.

We next show $-(2-p^2)\ln(1-p^2/2) < p^2$ and set

$$g(p) = p^2 + (2-p^2)\ln\left(1-\frac{p^2}{2}\right).$$

We have $g(p) > g(0) = 0$ i.e. $-(2-p^2)\ln(1-p^2/2) < p^2$ holds since

$$g'(p) = -2p\ln\left(1-\frac{p^2}{2}\right) > 0$$

holds.

Therefore, the number of intercepted bits $(2/p^2 - 1)$ is suppressed from above and below n_{max} and $n_{max} - 1$. The equation shows that our attack is almost optimal in terms of the number of the intercepted bits.

We then present two countermeasures against our attack. The first countermeasure is to reduce the bias in basis selection. The entropy loss of the secret key is reduced by reducing the basis selection bias as shown in Figure 2. The second countermeasure is to store the shared bits over a long period of time and combine these bits that are shared at different times to generate the secret key. Adding one-way functions to key generation increases its effectiveness.

5 CONCLUSIONS

This letter proposed an attack method that exploits the bias in basis selection against Efficient BB84 and performed a security evaluation of the entropy loss of the secret key. We firstly calculated the probability of detection and estimated the number of bits to attack from the beginning for the I-R attack that intercepts quantum states and measures only in the majority basis. We then calculated the number of bits for which we correctly obtained bit information within the estimated bits. We finally evaluated the contribution of the obtained bit information to the entropy loss of the secret key.

Decoy states (Hwang, 2003) were proposed to protect against PNS attack. Decoy states prevent the PNS attack by detecting changes in the photon number distribution caused by eavesdropping. Since our attack involves the partial interception of quantum states, the effect of introducing decoy states needs to be discussed in detail, which we will consider in future work.

REFERENCES

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

Brassard, G., Lütkenhaus, N., Mor, T., and Sanders, B. C. (2000). Limitations on practical quantum cryptography. *Phys. Rev. Lett.*, 85:1330–1333.

Huttner, B., Imoto, N., Gisin, N., and Mor, T. (1995). Quantum cryptography with coherent states. *Phys. Rev. A*, 51:1863–1869.

Hwang, W.-Y. (2003). Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.*, 91:057901.

Lo, H., Chau, H. F., and Ardehali, M. (2005). Efficient quantum key distribution scheme and a proof of its unconditional security. *J. Cryptol.*, 18(2):133–165.

Lütkenhaus, N. (2000). Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A*, 61:052304.

Makarov, V. and Hjelme, D. R. (2005). Faked states attack on quantum cryptosystems. *Journal of Modern Optics*, 52(5):691–705.

Shor, P. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134.