Round-robin differential phase-shift quantum key distribution protocol with threshold detectors

Toshihiko Sasaki[1] and Masato Koashi[1]

[1] *Photon Science Center, Graduate School of Engineering, The University of Tokyo, Bunkyo-ku, Tokyo 113-8656, Japan*

The round-robin differential phase-shift (RRDPS) quantum key distribution (QKD) protocol is a QKD protocol which does not require monitoring of disturbance unlike conventional QKD protocols. In the original proposal, security was proved provided that the receiver can use number-resolving photon detectors. It ensures that the sifted key is generated from the events where a single photon is received by the receiver. Here we consider a passive configuration of RRDPS protocol with threshold detectors and prove its security without estimating the frequency of multiphoton received events.

I. INTRODUCTION

Quantum cryptography [1–11] is one of the most promising applications of quantum information technology. The reason why quantum cryptography can be secure is usually understood in terms of the uncertainty principle [12]. If an eavesdropper Eve tries to measure the signal from a sender Alice, it must cause disturbance on a physical quantity which is complementary to the one carrying the transmitted information. It means that Alice and a receiver Bob can bound the information leaked to Eve from the estimated amount of disturbance. Once they bound it, they can use the privacy amplification to obtain a secure final key.

Recently, round-robin differential phase-shift (RRDPS) quantum key distribution (QKD) protocol was proposed [13]. The most interesting feature of this protocol is that it does not need monitoring of disturbance to guarantee the security. In other words, we can guarantee the security without any knowledge about the intervention during the transmission of the signal. In its security proof, one of the main building block is the statistical property of a pair of indices announced by Bob. Since this property is based on the condition that Bob receives one photon in an L-pulse train, he needs to use the photon-number-resolving detector to select valid events.

In actual implementation of QKD protocols, it is preferable to use threshold detectors which cannot discriminate the arrival of a single photon from that of two or more photons. One way to adapt the RRDPS protocol to the use of threshold detectors is to add a procedure for estimating how often multiphotons have arrived at the receiver. Since this added procedure can be regarded as a monitoring of the change in the optical signal, it may amount to forfeiting the main feature of the RRDPS protocol. We are thus led to a question of whether the protocol can be made secure without an added procedure of monitoring the disturbance. In this paper, we analyze an implementation of RRDPS with a passive delay change and show that the security is achieved without monitoring disturbance, even with the use of threshold detectors.

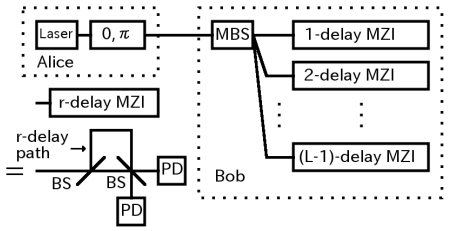

FIG. 1. An implementation of a protocol using Mach Zender interferometer (MZI) array. Alice's laser emits pulses with an interval $\Delta\tau$. A phase shift $\{0, \pi\}$ is applied to each pulse randomly. Bob uses a multiway beamsplitter (MBS) which splits pulses evenly and make them superposed by $L-1$ MZIs made from two half beamsplitters (BS) and two photon detector (PD). The r-delay MZI superposes two pulses whose time interval is $r\Delta\tau$.

II. PROTOCOL

We consider a setup illustrated in Fig. 1. Alice uses a laser which repeatedly emits pulses at the same interval of time, $\Delta\tau$, and a phase shifter which applies phase shift 0 or π to each pulse. Bob splits incoming pulses evenly into $L-1$ paths by a multiway beamsplitter (MBS). These paths are connected to r-delay Mach-Zender interferometers (MZI), where r varies from 1 to $L-1$. The r-delay MZI superposes two pulses whose time interval is $r\Delta\tau$ and two photon detectors (PDs) measure whether the relative phase between these two pulses is 0 or π. We suppose that the photon detectors are threshold detectors which discriminate whether the number of photons in a pulse is 0 or not. If we use an optical switch instead of MBS and PDs can discriminate the number of photons, this setup is identical to the original one. This change is irrelevant if the number of photons received at Bob's side is one.

With this setup, Alice and Bob share their key as follows. We regard the pulses emitted from Alice as a repetition of L-pulse trains. Bob records the timings when each detector detects photons. He only records a detection from superposition of two pulses in the same L-pulse train. We use indices $i \in \{1, \cdots, L\}$ to label the L pulses in a train. When we focus on an interference of a pair

$\{i,j\}$, there are four types of output: no detection, detection at one detector (0 or π), detection at both detectors. We call three types other than "no detection" as a detection of a pair $\{i,j\}$. When there are multiple detections of pairs in one L-pulse train, Bob randomly chooses a detected pair. If an output of a chosen pair is a detection at one detector, Bob sets his bit depending on which of the detectors has reported the detection. His bit becomes 0 and 1 if the relative phase of a pair is 0 and π, respectively. If both detectors are activated, he chooses 0 or 1 randomly. He announces the indices $\{i,j\}$ of the chosen pair in a L-pulse train over a public channel. Since Alice knows the phase of each pulse, she can calculate the relative phase between the ith and jth pulses. If the experimental setups are ideal and the quantum channel does not disturb relative phases, this scheme allows Alice and Bob to share the same random bits.

We assume that the efficiency does not depend on the paths and PDs. This allows us to assume that Bob's apparatus has unit efficiency and an appropriate attenuator is placed in front of Bob's apparatus. We consider this attenuator as a part of the quantum channel. We also assume that dead time and dark count rate of PDs are negligible for simplicity.

III. SECURITY

The security analysis is almost the same as that in [13]. First, we focus on Alice's side. Instead of using the laser, she could in principle prepare L qubits and L pulses in an entangled state $2^{-L/2}\bigotimes_{k=1}^{L}\sum_{s_k=0,1}|s_k\rangle_k(-1)^{s_k\hat{n}_k}|\Psi\rangle$, where $\{|0\rangle_k,|1\rangle_k\}$ is the Z-basis states of the kth qubit and $\hat{n}_k$ is the number operator of the kth pulse. If she measures each qubit on Z-basis, we obtain the same state as in the actual setting. We denote the results of Z-basis measurements as $s_1,\cdots,s_L$. Alice's sifted key bit is obtained by performing exclusive OR operation on s_i and s_j where $\{i,j\}$ are the indices announced by Bob. This bit is also obtained if she measures the target bit on Z-basis after performing controlled-NOT (CNOT) operations on the qubit pair $\{i,j\}$. We call $\{|0^X\rangle_k,|1^X\rangle_k\}$ as X-basis of the kth qubit, where $|t^X\rangle=(|0\rangle+(-1)^t|1\rangle)/\sqrt{2}$, $t=0,1$. We can rewrite the Alice's state as $2^{-L}\bigotimes_{k=1}^{L}\sum_{t_k=0,1}|t_k^X\rangle_k\left(1+(-1)^{t_k}(-1)^{\hat{n}_k}\right)|\Psi\rangle$. The operators $(1+(-1)^{\hat{n}_k})/2$ and $(1-(-1)^{\hat{n}_k})/2$ are projections onto states whose number of photons at the kth pulse is even and odd, respectively. A pulse with an odd number of photons includes at least one photon. Using the technique in [14], we have only to consider the case where the number of photons in L-pulse train is no larger than a threshold value $\nu_{\rm th}$. Under this condition, the number of qubits found in $|1^X\rangle$ states is no larger than $\nu_{\rm th}$ if Alice measures her qubits with X-basis.

Before analyzing the setup in Fig. 1, we review the crux of the security proof in [13]. It is based on the existence of an equivalent protocol where Bob can tell Alice additional information about which index of the pair $\{i,j\}$ is the first one. In other words, Bob can tell Alice an ordered pair (i,j). We denote the probability of obtaining an unordered pair $\{i,j\}$ and an ordered pair (i,j) as $p_{\{i,j\}}$ and $p_{(i,j)}$, respectively. In order to keep Eve's knowledge on the Alice's sifted key bit exactly the same as in the actual protocol, we require $p_{\{i,j\}}=p_{(i,j)}+p_{(j,i)}$. From explicit construction of the equivalent protocol, the proof shows that $p_{(i,j)}$ satisfies

$$p(j|i)=\frac{p_{(i,j)}}{\sum_{j'}p_{(i,j')}}\leq\tilde{p}=\frac{1}{L-1} \tag{1}$$

for all i,j. This inequality stems from the condition that only one photon reaches Bob's side. Alice's bit is obtained from Z-basis measurement on the target qubit j after the CNOT operation on the pair (i,j). According to [15], we can prove the security if we know how we can predict the result of X-basis measurement on the target qubit. Note that X-basis measurement on a target qubit commutes with the CNOT operation. Among $L-1$ qubits except the control qubit, the number of those in state $|1^X\rangle$ is no larger than $\nu_{\rm th}$. Thus, the probability of obtaining the $|1^X\rangle$ state at the target qubit is no larger than $\tilde{p}\nu_{\rm th}$. The asymptotic secure key rate G from this result is $G=Q\left(1-h(e_{\rm bit})-\frac{e_{\rm src}}{Q}-\left(1-\frac{e_{\rm src}}{Q}\right)h\left(\tilde{p}\nu_{\rm th}\right)\right)$, where Q is sifted key rate, $e_{\rm bit}$ is bit error rate, and $e_{\rm src}$ is probability that the number of photons emitted in a L-pulse train is larger than $\nu_{\rm th}$.

Since use of the threshold detectors is assumed in this paper, we cannot use the same equivalent protocol as in [13] and Eq. (1). Instead, we will show the following proposition.

Probosition 1 *For Bob's apparatus in the actual setup in Fig. 1, there exists an alternative procedure of producing an unordered pair $\{i,j\}$ through the production of ordered pair (i,j), satisfying the following properties (a) and (b) regardless of the state received by Bob. Let $p_{(i,j)}$ is the probability of the ordered pair produced in the alternative protocol. (a) $p_{\{i,j\}}=p_{(i,j)}+p_{(j,i)}$, where $p_{\{i,j\}}$ is the probability of unordered pair in the actual protocol. (b) $p(j|i)=\frac{p_{(i,j)}}{\sum_{j'}p_{(i,j')}}\leq\tilde{p}=\frac{2}{L}$, for all $i,j\in\{1,\cdots,L\},i\neq j$.*

From this result and the above argument, we obtain an asymptotic secure key rate G with $\tilde{p}=2/L$, namely

$$G=Q\left(1-h(e_{\rm bit})-\frac{e_{\rm src}}{Q}-\left(1-\frac{e_{\rm src}}{Q}\right)h\left(\frac{2\nu_{\rm th}}{L}\right)\right). \tag{2}$$

IV. PROPOSITION 1

Although the proof of Proposition 1 is the main body of this work, it is rather technical and is found in the supplementary material. Instead, we show what properties are essential in proving it.

In the actual experiment, Bob announces an unordered pair $\{i,j\}$ by using the interferometers in Fig. 1. Interferences occur only at the second beamsplitters of the interferometers and these interferences have nothing to do with which pair $\{i,j\}$ is eventually announced by Bob. Even if we remove the second beam splitters, $p_{\{i,j\}}$ does not change. In other words, $p_{\{i,j\}}$ depends only on how each photon chooses its path probabilistically through the array of beamsplitters, just like a classical particle.

When an unordered pair $\{i,j\}$ is detected and chosen over other detected pairs, there are three cases. (i) The photons responsible for this detection comes only from ith pulse. (ii) The photons responsible for this detection comes only from jth pulse. (iii) The photons responsible for this detection comes from both ith pulse and jth pulse. For the case (i), this detection is counted as (i,j). For the case (ii), it is counted as (j,i). For the case (iii), we randomly choose (i,j) or (j,i). From these rules, Bob can determine a pair (i,j) such that the distribution of $\{i,j\}$ is identical to the actual protocol.

If there is one photon in an L-pulse train at Bob's side, it is shown in the original proposal that $p(j|i)$ is bounded by $1/(L-1)$. The bound in Proposition 1 is almost twice as large as the original one. This factor can be understood from the following example. We assume that Eve sends a pulse train where the first pulse ($i=1$) contains no photon, the second pulse ($i=2$) contains one photon and the other pulses contain a large number of photons. Consider the case where L is large. For $(2,1)$ to be chosen, the photon in the second pulse must choose the delayed arm of the 1-bit delay interferometer, which occurs with probabiltiy $\sim 1/(2L)$. It must further beats the other detected pairs. Since almost all the $L(L-1)/2$ pairs are detected, this probability is $\sim 2/L^2$. Since the first pulse has no photon, the case (iii) does not happen. Hence we have $p_{(2,1)} \sim 1/L^3$. For $(2,j)(j \neq 1,2)$, the argument is almost the same except that case (iii) surely occurs. Hence we have $p_{(2,j)} \sim 1/(2L^3)$. Since it means $p(1|2) \sim \frac{2}{L}$, it is an almost optimal attack for Eve.

V. CONCLUSION

We have proven the security of the RRDPS protocol with the measurement setup in Fig. 1 with threshold detectors. The only difference between analysis in this paper and that in the original one [13] is how to construct a equivalent protocol to produce an ordered pair (i,j). In [13], the unbiased distribution is derived from the condition that there is one photon in an L-pulse train. Although we remove this condition in this paper, we make use of the fact that each photon is distributed to each MZI with an equal probability in order to guarantee almost unbiased distribution of a pair. In return for the omission of checking the number of photons in an L-pulse train, the argument of the binary entropy function for the privacy amplification is nearly doubled. Roughly speaking, this amounts to an additional loss of 3dB in the channel.

Our results show that the main feature of the RRDPS is maintained even if the exact number of photons incident on Bob' s apparatus is unknown. The absence of statistical estimation also has a practical advantage when the communication time is short and the finite-key effect is dominant. It is also interesting to consider whether a similar argument is applicable to the originally proposed implementation of the RRDPS protocol with an active variable delay.

ACKNOWLEDGMENTS

This work was funded in part by ImPACT Program of Council for Science, Technology and Innovation (Cabinet Office, Government of Japan) and Photon Frontier Network Program (MEXT)

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India (IEEE Press, New York, 1984) p. 175.
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[4] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
[5] D. Mayers and A. Yao, in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society, Washington, DC, USA, 1998) p. 503.
[6] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[7] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. A **68**, 022317 (2003).
[8] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).
[9] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, Applied Physics Letters **87**, 194108 (2005).
[10] L. Sheridan and V. Scarani, Phys. Rev. A **82**, 030301 (2010).
[11] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[12] W. Heisenberg, Z. Phys. **43**, 172 (1927).
[13] T. Sasaki, Y. Yamamoto, and M. Koashi, Nature **509**, 475 (2014).
[14] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quant. Inf. Comp. **4**, 325 (2004).
[15] M. Koashi, New Journal of Physics **11**, 045018 (2009).

Proof of proposition 1 in "Round-robin differential phase-shift quantum key distribution protocol with threshold detectors"

Toshihiko Sasaki[1] and Masato Koashi[1]

[1] *Photon Science Center, Graduate School of Engineering, The University of Tokyo, Bunkyo-ku, Tokyo 113-8656, Japan*

I. PROOF OF PROPOSITION 1

In this supplementary material, we will prove Proposition 1 in "Round-robin differential phase-shift quantum key distribution protocol with threshold detectors".

Probosition 1 *For Bob's apparatus in the actual setup in Fig. 1, there exists an alternative procedure of producing an unordered pair $\{i,j\}$ through the production of ordered pair (i,j), satisfying the following properties (a) and (b) regardless of the state received by Bob. Let $p_{(i,j)}$ be the probability of the ordered pair produced in the alternative protocol. (a) $p_{\{i,j\}} = p_{(i,j)} + p_{(j,i)}$, where $p_{\{i,j\}}$ is the probability of unordered pair in the actual protocol. (b) $p(j|i) = \frac{p_{(i,j)}}{\sum_{j'} p_{(i,j')}} \leq \tilde{p} = \frac{2}{L}$, for all $i,j \in \{1,\cdots,L\}, i \neq j$.*

In order to prove Proposition 1, we consider an equivalent protocol for Bob producing an ordered pair (i,j). Before considering the probability distribution of an ordered pair (i,j), we focus on that of an unordered pair $\{i,j\}$. In the actual protocol, it is determined by the measurement in Fig. 1. The multiway beamsplitter (MBS) splits each pulse into $L-1$ paths evenly. The first beamsplitters (BSs) of the interferometers further split these pulses into 2 paths evenly. A pulse brought to r-delay MZI will be superposed with rth pulse after it or rth pulse before it. Let $\hat{c}^\dagger_{i,i\pm r}$ be the creation operator of the mode which comes from ith pulse and will be superposed with $i \pm r$-th pulse at the 2nd BS of the r-delay MZI. When $i \pm r$ is smaller than 1 or greater than L, it should be understood as representing a pulse in the previous or subsequent L-pulse train. Although the actual measurement involving the relative phase corresponds to the operator $(\hat{c}^\dagger_{(i,j)} \pm \hat{c}^\dagger_{(j,i)})(\hat{c}_{(i,j)} \pm \hat{c}_{(j,i)})/2$, we are only interested in the probability distribution of a pair $\{i,j\}$. Since a pair $\{i,j\}$ is detected if and only if there are photons in either or both of the two modes, it can be determined only through the total photon number $\hat{c}^\dagger_{(i,j)}\hat{c}_{(i,j)} + \hat{c}^\dagger_{(j,i)}\hat{c}_{(j,i)}$. In the alternative protocol, we use the measurement corresponding to $\hat{c}^\dagger_{(i,j)}\hat{c}_{(i,j)}$ and $\hat{c}^\dagger_{(j,i)}\hat{c}_{(j,i)}$ instead of the actual measurement, and assume that the pair $\{i,j\}$ is detected whenever the total photon number is nonzero. We denote $P_{\mathbf{n}}$ as the probability that the measurement result of $\hat{c}^\dagger_{(i,j)}\hat{c}_{(i,j)}$ is $n_{(i,j)}$, where $\mathbf{n}$ is a set of $2L(L-1)$ variables $n_{(i,j)}$ for $i \in \{1,\cdots,L\}, j \in \{i-L+1,\cdots,i+L-1\}\backslash\{i\}$. The number $N_{\mathbf{n}}$ of the detected pairs in a single L-pulse train is related to $\mathbf{n}$ as

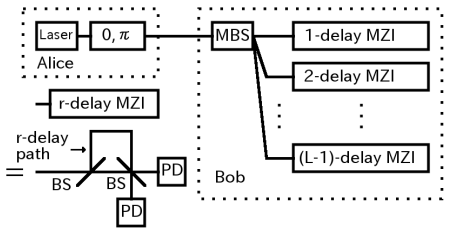

FIG. 1. An implementation of a protocol using Mach Zender interferometer (MZI) array. Alice's laser emits pulses with an interval $\Delta\tau$. A phase shift $\{0,\pi\}$ is applied to each pulse randomly. Bob uses a multiway beamsplitter (MBS) which splits pulses evenly and make them superposed by $L-1$ MZIs made from two half beamsplitters (BS) and two photon detector (PD). The r-delay MZI superposes two pulses whose time interval is $r\Delta\tau$.

$$N_{\mathbf{n}} = \#\left\{\{i,j\} \mid i,j \in \{1,\cdots,L\},\ i \neq j,\ n_{(i,j)} + n_{(j,i)} > 0\right\}. \tag{1}$$

Using these values, we can write the probability $p_{\{i',j'\}}$ that a pair $\{i',j'\}(i,j \in \{1,...L\}, i \neq j)$ is announced as

$$p_{\{i',j'\}} = \sum_{\{\mathbf{n} | n_{(i',j')} + n_{(j',i')} > 0\}} P_{\mathbf{n}} \frac{1}{N_{\mathbf{n}}}. \tag{2}$$

Suppose that a pair $\{i,j\}$ is chosen. It means $n_{(i,j)} + n_{(j,i)} > 0$. The alternative protocol chooses an ordered pair through the following rule.

(i) If $n_{(j,i)}$ is zero, we choose (i,j).

(ii) If $n_{(i,j)}$ is zero, we choose (j,i).

(iii) If neither is zero, we choose (i,j) or (j,i) randomly.

This rule defines the probability $p_{(i,j)}$ of choosing an ordered pair (i,j) as

$$p_{(i',j')} = \sum_{\mathbf{n}} P_{\mathbf{n}} \frac{1}{N_{\mathbf{n}}} E^{(i',j')}_{\mathbf{n}} \left(\frac{1}{2}\right)^{E^{(j',i')}_{\mathbf{n}}}, \tag{3}$$

where $E^{(i,j)}_{\mathbf{n}}$ is defined as

$$E^{(i,j)}_{\mathbf{n}} = \begin{cases} 0 & n_{(i,j)} = 0 \\ 1 & n_{(i,j)} > 0 \end{cases}. \tag{4}$$

From this definition, it automatically satisfies

$$p_{\{i,j\}} = p_{(i,j)} + p_{(j,i)}. \tag{5}$$

We will show there is a constant Λ satisfying

$$p_{(i,j)} \geq \Lambda p_{(i,j')} \tag{6}$$

for all $i, j, j' \in \{1, \cdots, L\}, i \neq j, i \neq j'$. If this inequality holds, we can derive the following inequality.

$$\begin{aligned} p(j|i) &:= \frac{p_{(i,j)}}{\sum_{j' \in \{\, k | k \in \{1,\cdots,L\}, k \neq i \,\}} p_{(i,j')}} \\ &\leq \frac{p_{(i,j)}}{p_{(i,j)} + (L-2)\Lambda p_{(i,j)}} \\ &= \frac{1}{1 + (L-2)\Lambda} \end{aligned}. \tag{7}$$

Now we will determine the constant Λ. We consider a permutation operation σ which permutates the values of $n_{(i',j')}$ and $n_{(i',j'')}$ in the number distribution $\mathbf{n}$. Note that this permutation does not change (j', i') and (j'', i'). Since MBS and first BSs split each pulse evenly, the probability distribution $P_{\mathbf{n}}$ is symmetric under this permutation.

$$P_{\sigma\mathbf{n}} = P_{\mathbf{n}}. \tag{8}$$

For any function $f(\mathbf{n})$ of $\mathbf{n}$, the order of a summation is irrelevant in taking the sum over all possible values of $\mathbf{n}$, namely,

$$\sum_{\sigma\mathbf{n}} f(\mathbf{n}) = \sum_{\mathbf{n}} f(\mathbf{n}). \tag{9}$$

This leads to

$$\begin{aligned} & p_{(i',j'')} \\ =& \sum_{\mathbf{n}} P_{\mathbf{n}} \frac{1}{N_{\mathbf{n}}} E_{\mathbf{n}}^{(i',j'')} \left(\frac{1}{2}\right)^{E_{\mathbf{n}}^{(j'',i')}} \\ =& \sum_{\sigma\mathbf{n}} P_{\sigma\mathbf{n}} \frac{1}{N_{\sigma\mathbf{n}}} E_{\sigma\mathbf{n}}^{(i',j'')} \left(\frac{1}{2}\right)^{E_{\sigma\mathbf{n}}^{(j'',i')}} \\ =& \sum_{\sigma\mathbf{n}} P_{\mathbf{n}} \frac{1}{N_{\sigma\mathbf{n}}} E_{\mathbf{n}}^{(i',j')} \left(\frac{1}{2}\right)^{E_{\mathbf{n}}^{(j'',i')}} \\ =& \sum_{\mathbf{n}} P_{\mathbf{n}} \frac{1}{N_{\sigma\mathbf{n}}} E_{\mathbf{n}}^{(i',j')} \left(\frac{1}{2}\right)^{E_{\mathbf{n}}^{(j'',i')}} \end{aligned}. \tag{10}$$

We consider a ratio X defined as

$$X = \frac{N_{\mathbf{n}} 2^{E_{\mathbf{n}}^{(j',i')}}}{N_{\sigma\mathbf{n}} 2^{E_{\mathbf{n}}^{(j'',i')}}}. \tag{11}$$

When $E_{\mathbf{n}}^{(i',j')}$ equals to 1, this value can be calculated as

$$X = \begin{cases} 1 & \begin{matrix}(E_{\mathbf{n}}^{(i',j'')}, E_{\mathbf{n}}^{(j',i')}, E_{\mathbf{n}}^{(j'',i')}) \\ =(0,0,0),(1,0,0),(0,1,1),(1,11)\end{matrix} \\ \frac{2N_{\mathbf{n}}}{N_{\mathbf{n}}+1} & \begin{matrix}(E_{\mathbf{n}}^{(i',j'')}, E_{\mathbf{n}}^{(j',i')}, E_{\mathbf{n}}^{(j'',i')}) \\ =(0,1,0)\end{matrix} \\ \frac{N_{\mathbf{n}}}{2(N_{\mathbf{n}}-1)} & \begin{matrix}(E_{\mathbf{n}}^{(i',j'')}, E_{\mathbf{n}}^{(j',i')}, E_{\mathbf{n}}^{(j'',i')}) \\ =(0,0,1)\end{matrix} \\ 2 & \begin{matrix}(E_{\mathbf{n}}^{(i',j'')}, E_{\mathbf{n}}^{(j',i')}, E_{\mathbf{n}}^{(j'',i')}) \\ =(1,1,0)\end{matrix} \\ \frac{1}{2} & \begin{matrix}(E_{\mathbf{n}}^{(i',j'')}, E_{\mathbf{n}}^{(j',i')}, E_{\mathbf{n}}^{(j'',i')}) \\ =(1,0,1)\end{matrix} \end{cases}. \tag{12}$$

Since we assumed $E_{\mathbf{n}}^{(i',j')} = 1$, $N_{\mathbf{n}}$ is no less than 1. If the condition $E_{\mathbf{n}}^{(j'',i')} = 1$ also holds, $N_{\mathbf{n}}$ is no less than 2. Hence $X \geq \frac{1}{2}$ always holds, leading to

$$\begin{aligned} & p_{(i',j'')} \\ =& \sum_{\mathbf{n}} P_{\mathbf{n}} \frac{1}{N_{\sigma\mathbf{n}}} E_{\mathbf{n}}^{(i',j')} \left(\frac{1}{2}\right)^{E_{\mathbf{n}}^{(j'',i')}} \\ =& \sum_{\mathbf{n}} P_{\mathbf{n}} X \frac{1}{N_{\mathbf{n}}} E_{\mathbf{n}}^{(i',j')} \left(\frac{1}{2}\right)^{E_{\mathbf{n}}^{(j',i')}} \\ \geq& \frac{1}{2} \sum_{\mathbf{n}} P_{\mathbf{n}} \frac{1}{N_{\mathbf{n}}} E_{\mathbf{n}}^{(i',j')} \left(\frac{1}{2}\right)^{E_{\mathbf{n}}^{(j',i')}} \\ =& \frac{1}{2} p_{(i',j')}. \end{aligned} \tag{13}$$

Thus we can set Λ to be $\frac{1}{2}$ and obtain

$$p(j|i) \leq \frac{2}{L}. \tag{14}$$