**Calculating long-range two-photon visibility for entanglement-swapping-based quantum communication via sampling**

Pengqing Zhang
Charlottesville, VA

B.S., University of Illinois at Urbana Champaign, 2013

A Dissertation presented to the Graduate Faculty of the University of Virginia in Candidacy for the Degree of Master of Science

Department of Physics

University of Virginia
May 2015

**Abstract**

In this dissertation I develop a Monte-Carlo sampling approach to redress the enormous computational time required to calculate two-photon visibility for multiple-entanglement-swapping-based long-distance quantum communication. I employ our theory to study both the realistic setting involving dark counts, multi-photon events and loss, and I also study the semi-idealistic case of perfect synchronized single-photon sources; this semi-idealistic case is used to verify my sampling method. My new sampling method enables successful, reliable calculation of visibility for up to six consecutive entanglement-swapping stations. Although six entanglement-swapping stations lead to extremely low rates in the real-world setting, my sampling method for solving long-distance quantum communication rates and visibility serves as a valuable tool for modeling future viable quantum communication strategies incorporating promising technology such as optical quantum memory.

**Acknowledgements**

I am honor to finish this project with my collaborators Prof. Barry C. Sanders from University of Calgary in Canada and Prof. Aeysha Khalique from National University of Sciences and Technology in Pakistan. I gratefully acknowledge valuable discussions with my friend S. Qi, J. Wadden and Prof. H. de Riedmatten. I appreciate financial support from the 1000 Talent Program of China and AITF. I also appreciate the computing resources provided by University of Virginia, USA.

I gratelyfully thank the kindly help and support from Prof. Eugene Kolomeisky and instruction on EPR paradox from Prof. Olivier Pfister, which is the starting point of my love for quantum information and quantum computation. It is my great honor to have a chance to study in University of Virginia. I will always miss the past two years.

I want to express my love for my great parents, who love and support me for the past twenty-three years, and my dear friends, without whom my life can never be that wonderful. Finally, I want to thank her, who is the reason why I never give up on this project.

# Contents

# Chapter 1

# Introduction

Quantum communication, which is especially important for quantum-enhanced security such as quantum key distribution, suffers from a distance limit. Practical issues such as transmission loss results in exponential losses with respect to transmission distance, and secure quantum communication has an absolute distance limit when dark counts are factored in. Countervailing strategies can mitigate these problems. A quantum relay built as a concatenated sequence of entanglement swapping stations can extend the effective transmission distance [1–5], and quantum repeaters could overcome the exponential loss rate [6, 7] but relies on a much-vaunted optical quantum memory [8], which is beyond current technological reach. Thus, the quantum relay is currently the best approach to extending the reach of secure quantum communication until superior technology is viable.

The quantum relay concept is to create entangled photons shared between distant parties Alice and Bob via concatenated entanglement swapping, and we use the term quantum relay to refer to each entanglement swapping station. Our aim is to develop a tractable algorithm for simulating quantum-relay-based quantum communication for three reasons. The output of the algorithm is an approximation of the expected two-photon visibility observed by two distantly separate parties Alice and Bob; this two-photon visibility is the appropriate figure of merit to assess the expected bit rate and quantum bit error rate. The first reason is that we regard an accurate algorithm as a testable tool to that theoretical models for long-distance quantum communication are reliable and tested empirically. Our second reason is that the algorithmic tool will be needed as a component of fugue models that accommodate future technologies such as quantum repeaters. The third reason is more academic: an accurate, tractable algorithm for solving quantum communication employing several sequential quantum relay stations is a theoretical and computational challenge that warrants new thinking.

Here we report a numerical solution for six quantum relays in the realistic setting of PDC sources. We emphasize that our algorithm is only tractable for several sequential entanglement swapping stations and is not designed nor guaranteed to be scalable with respect to increasing the number $N$ of quantum relay station. Our algorithm is based on an established theory of practical quantum communication based on a sequence of $N$ quantum relays for $N$ any natural number [9–11]. By reaching $N = 6$ quantum relays, our sampling simulation far exceeds the current best of $N = 3$ quantum relays [11] obtained by numerically solving exact equations for a truncated Hilbert space. We refer to our approach here as the sampling method and to numerically solving exact equations for a truncated Hilbert space as direct computation. The reason for the $N = 3$ limit in previous work is that the algorithm has a computation-time overhead of $O(4^{8N+4})$.

We add another caution regarding the theory-experiment divide for quantum-relay quantum communication. Current experimental entanglement-swapping-based long-distance quantum communication has only been achieved for a single ($N = 1$) quantum relay [12–14]. Meanwhile, the theoretical prediction of visibility is limited up to $N = 3$ swaps due to excessive computational time of simulations of higher numbers of swaps.

Our approach to solving the transmission rate is markedly different than prior work, which employed a combination of mathematical physics special functions and high-performance computing to obtain exact answers [9–11]. In this work, our strategy is to get approximate answers to transmission rate via sampling the outcome using a Monte Carlo approach equipped with pseudo-random number sampling based on the binary-search method. as working even in a truncated Fock space for each mode is infeasible for simulation past three sequential quantum relays. As expected the transmission success rate is dismal, but the good news that our Monte Carlo algorithm is successful in that it agrees with known results for up to three quantum relay stations and furthermore yields correct results for the semi-idealistic case of perfect synchronized single photon sources.

As we developed our algorithm and tested for accuracy, we encountered a problem in earlier work that we correct here. Specifically a previous test of theoretical vs experimental two-photon visibility [9] for a single-swap experiment [12] revealed that the simulated visibility is within one standard deviation of the experimental visibility. We find that the simulation parameters [9] are incorrect, and we show the corrected result here. Our new result shows that the simulated two-photon visibility in fact lies within two standard deviations of the experimental two-photon visibility, not one standard deviation as thought before.

We organize our paper as follows. Requisite background is provided In Chapter. 2. In Chapter. 3 we correct the earlier simulation [9] by inserting correct parameters for the single-swap experiment [12]. Our sampling approach to calculating two-photon visibility

for $N$ swaps in a quantum relay network is described in detail in Chapter. 4. In Chapter. 5 we show how to establish the prior distribution for $N$ quantum relays based on successful sampling for the $N-1$ case. Our results of verification of sampling method are shown in Chapter. 6. Our results of simulated visibilities are provided in Chapter. 7 for $N \leq 6$, and we verify these results against other simulations for PDCn sources and for the semi-idealistic single-photon sources. We conclude in Chapter. 8 and provide detailed derivations in the appendices.

# Chapter 2

# Background

In this chapter we provide the requisite background that is needed for this dissertation. In Chapter. 2.1 we give the theoretical background of LDQC through any number of entanglement-swapping operations in a quantum-relay configuration. In Chapter. 2.2 we give the parameters based on current technologies that are entered for the simulations in this dissertation . In Chapter. 2.3 we show the intractability of direct computation of visibilities for simulations of $N \geq 4$ swaps using a single node on a desktop computer and truncations that are applied to reduce the computational time. In Chapter. 2.4 we review the salient background of Monte Carlo simulation. In Chapter. 2.5 we summarize the general background of pseudo-random number sampling based on the binary search method.

## 2.1 Theory of LDQC through any number of entanglement-swapping operations in a quantum-relay configuration

The theory of LDQC through any number-$N$ of entanglement-swapping operations in a quantum-relay configuration [9–11] is achieved by connecting $N$ single-swap elements through intermediate postselection-operation (PSO) stations, where each single-swap element is constructed with two PDC sources, one 50:50 beamsplitter, two polarizing beamsplitters and a set of four single-photon detectors, as shown in Fig. 2.1(a). The outermost two photons have to pass through the polarization rotators and polarizing beamsplitters before reaching Alice's and Bob's detectors. We provide $N = 2$ swaps as an example in Fig. 2.1(b). The two-photon visibility of any $N$ swaps can be predicted theoretically based on the theory.

### 2.1.1 Two-photon visibility

By setting both polarization angles to be $\pi/4$, we are able to simulate the two-photon visibility via the equation [11]

$$V = \frac{Q_{1010}^{\mathbf{1010}} + Q_{0101}^{\mathbf{1010}} - Q_{1001}^{\mathbf{1010}} - Q_{0110}^{\mathbf{1010}}}{Q_{1010}^{\mathbf{1010}} + Q_{0101}^{\mathbf{1010}} + Q_{1001}^{\mathbf{1010}} + Q_{0110}^{\mathbf{1010}}}, \tag{2.1}$$

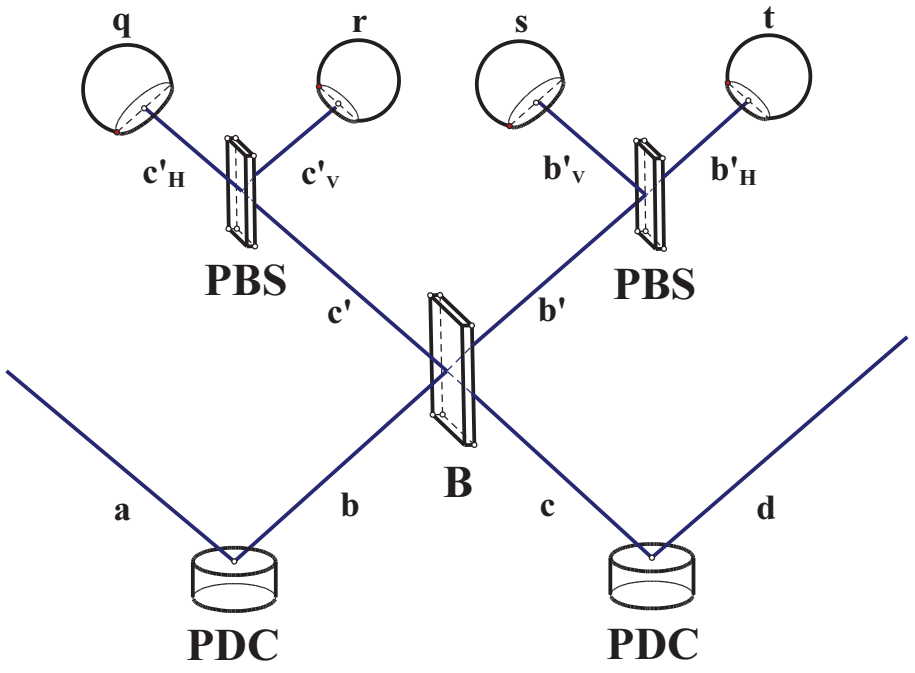
where $Q_{q'r's't'}^{\boldsymbol{qrst}}$ is the conditional probability for Alice to observe the two-tuple click event $(t's')$ and Bob to observe $(r'q')$, given that the four-tuple click events $(\boldsymbol{qrst})$ have been yielded from all the intermediate detectors. Here $(\boldsymbol{qrst})$ is the abbreviated form of $(q_1r_1s_1t_1)$, $(q_2r_2s_2t_2)$...$(q_{2N-1}r_{2N-1}s_{2N-1}t_{2N-1})$. As we assume all the detectors are single-photon detectors, $(\boldsymbol{qrst})$ and $(q'r's't')$ can only take values from $\{0, 1\}$, where 1 means "click" and 0 means "not click". The four-tuple click events $(\boldsymbol{qrst}) = (\mathbf{1010})$ and $(\mathbf{0101})$ on the intermediate detectors correspond to anticorrelated polarizations, thus giving maximum coincidences for anticorrelated four-tuple click event $(q'r's't') = (1010)$ or $(0101)$ and minimum for correlated four-tuple click event $(0110)$ or $(1001)$ at Alice's and Bob's detectors. We now show how to calculate the conditional probabilities $Q_{q'r's't'}^{\boldsymbol{qrst}}$ based on the theory [9].

### 2.1.2 Conditional probability

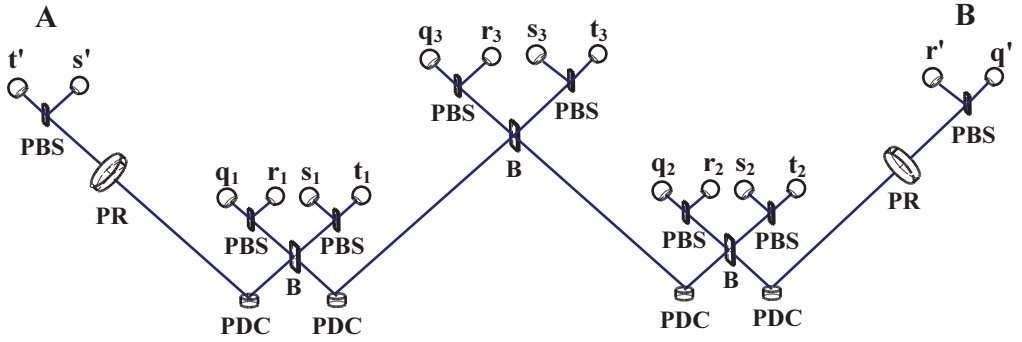
The conditional probability $Q_{q'r's't'}^{\boldsymbol{qrst}}$ can be calculated through the equation [9]

$$Q_{q'r's't'}^{\boldsymbol{qrst}} = \sum_{i'j'k'l'=0}^{\infty} \sum_{\boldsymbol{ijkl}=0}^{\infty} p\left(q'r's't'|i'j'k'l'\right) P_{\boldsymbol{ijkl}}^{\boldsymbol{qrst}} W_{i'j'k'l'}^{\boldsymbol{ijkl}}, \tag{2.2}$$

where $p\left(q'r's't'|i'j'k'l'\right)$ is the conditional probability for Alice to observe two-tuple click event $(t's')$ and Bob to observe $(r'q')$ by using imperfect single-photon detectors including losses, given the hypothesis that ideal photon-number discriminating detectors without any loss would have yielded two-tuple counting events $(l'k')$ for Alice and $(j'i')$ for Bob. $P_{\boldsymbol{ijkl}}^{\boldsymbol{qrst}}$ is the conditional probability for ideal photon-number discriminating detectors without any loss to yield four-tuple counting events $(\boldsymbol{ijkl})$, given that the single-photon detectors including losses have yielded four-tuple click events $(\boldsymbol{qrst})$, for all the intermediate PSO stations. $W_{i'j'k'l'}^{\boldsymbol{ijkl}}$ is the conditional probability for Alice to observe the two-tuple counting event $(l'k')$ and Bob to observe $(j'i')$, given that the intermediate PSO stations have yielded the four-tuple counting events $(\boldsymbol{ijkl})$, in an ideal-world scenario, i.e., using ideal photon-number discriminating detectors and no loss during transmission. Notice that each index of the four-tuple counting events $(\boldsymbol{ijkl})$ and




(a)




(b)

FIGURE 2.1: $N = 2$ swaps (b) achieved by combining two single-swap elements (a) with an intermediate PSO station. In each single-swap element, the two PDC sources will emit photons into four spatial modes, i.e., $a$, $b$, $c$ and $d$. The modes coming out of the beamsplitter are denoted as $c'$ and $b'$ and those coming out of the PBSs are denoted as $c'_{\rm H}$, $c'_{\rm V}$, $b'_{\rm V}$ and $b'_{\rm H}$. The four-tuple click events of detectors at the 1st, 2nd and 3rd PSO stations are denoted as $(q_1 r_1 s_1 t_1)$, $(q_2 r_2 s_2 t_2)$ and $(q_3 r_3 s_3 t_3)$, respectively. The four-tuple click events of Alice's and Bob's detectors are denoted as $(q' r' s' t')$.

$(i'j'k'l')$ of ideal photon-number discriminating detectors can take integer values from $[0, \infty)$. All the details of the formulas can be found in Appendix A.

## 2.2 Parameters based on current technologies

The conditional probability $Q^{\boldsymbol{qrst}}_{q'r's't'}$ depends on the nonlinearities of PDC sources ($\chi$), the efficiencies ($\eta$) and dark count probabilities ($\varrho$) of detectors, the transmission efficiency ($\eta_{\mathrm{t}}$) and the coupling efficiency ($\eta_{\mathrm{c}}$). The theory [9] includes the factors of transmission loss and coupling loss into the "effective efficiency" of the detector, which can be calculated through the equation

$$\eta_{\mathrm{e}} = \eta\eta_{\mathrm{c}}10^{-\alpha d/10}, \tag{2.3}$$

where $\eta$ is the efficiency of the detector, $1-\eta_{\mathrm{c}}$ is the fraction of coupling loss and the transmission efficiency $\eta_{\mathrm{t}} = 10^{-\alpha d/10}$ [9], where $\alpha$ is the loss coefficient of the transmission medium in dB/km; $d$ is the distance traveled in km. As a result, the parameters we need to enter for the simulation are the nonlinearities of all PDC sources $\{\chi\}$ and the "effective efficiencies" $\{\eta_{\mathrm{e}}\}$ and the dark count probabilities $\{\varrho\}$ of all detectors.

The most efficient single-photon detector available is the superconducting nanowire single-photon detector (SNSPD) reported in 2013 [15], with a system detection efficiency of 90% including coupling loss. The requisite temperature is 2 K. The lowest transmission loss reported in 2002 is 0.2 db/km [1] for photons with wavelength at 1550 nm. The dark count rate of SNSPD is around 1 c.p.s with timing jitter of ∼150 ps [15], which corresponds to dark count probability $\varrho \approx 1.5 \times 10^{-10}$. The brightness of the PDC source, which is proportional to $\chi^2$, can be adjusted. Therefore, we treat $\chi$ as a variable instead of parameter.

Then if we simulate the length of each outer arm ($a$, $d$) of each single-swap element to be 100 km and that of each inner arm ($b$, $c$) to be negligible in km, the "effective efficiency" of the detectors at outer arms are all equal to $90\% \times 10^{-0.2\times100/10} \approx 0.9\%$ and those at inner arms are all equal to 90% as transmission loss is negligible in the inner arms. Those are the parameters based on current technologies that we use for simulating long-range two-photon visibilities for various numbers of swaps in this paper.

## 2.3 Truncations and intractability of direct computation

As the simulation of $Q^{\boldsymbol{qrst}}_{q'r's't'}$ requires taking all possible values of four-tuple indices $(\boldsymbol{ijkl})$ and $(i'j'k'l')$ with each index ranging from 0 to infinity, which is infeasible, the upper bound of each index is set to be $n_{\max}$. For $n_{\max} = 3$, which is found to be a reliable truncation [11], the visibilities have been successfully computed for the cases of $N = 1$ swap and $N = 2$ swaps, but not for $N \geq 3$ swaps [11]. In order to break this limitation, truncations are put on the possible values of four-tuple indices $(\boldsymbol{ijkl})$ and $(i'j'k'l')$, i.e., each four-tuple indices $(ijkl)$ and $(i'j'k'l')$ only take values that satisfy the condition

$$\begin{aligned} 2 \leq i + j + k + l \leq 4, \\ 2 \leq i' + j' + k' + l' \leq 4. \end{aligned} \tag{2.4}$$

The truncations are reasonable as a $4N$-photon coincidence is not observed unless each $i + j + k + l \geq 2$ and $i' + j' + k' + l' \geq 2$. At the same time, the probability to observe $i + j + k + l > 4$ or $i' + j' + k' + l' > 4$ is small as it is a rare event for PDC source to generate high-number pairs of photon-pair. Therefore, the simulated visibilities with truncations on $(\boldsymbol{ijkl})$ and $(i'j'k'l')$ are approximations of those without truncations [11].

The computational time of simulation with truncations on $(\boldsymbol{ijkl})$ and $(i'j'k'l')$ is much less than that without them. The order of computational time with truncation is $O(61^{2N+1})$ whereas that without truncation is $O(256^{2N+1})$. For $N = 2$ simulation, the wall-clock time with truncations on $(\boldsymbol{ijkl})$ and $(i'j'k'l')$ is around 20 seconds whereas that without truncations is around 4 hours using a single node on an ASUS i7-4770 desktop computer with CPU @ 3.40 GHz and 16 GB RAM.

By truncating, visibilities are successfully computed up to $N = 3$ swaps but not for $N \geq 4$ swaps using a single node on the same desktop computer. Therefore, the intractability of $N \geq 4$ simulations needs to be solved.

## 2.4 Monte Carlo simulation

Monte Carlo simulation is a broad class of simulations that approach solutions of quantitative problems by repeated random sampling from a known probability distribution $P$. For each trial of the simulation, an input $X$ is generated by some pseudo-random number generator according to $P$. The deterministic algorithm then takes $X$ and generates an output. The solution of the quantitative problem is then obtained by aggregating all the outputs generated through large number of trials.

The probability distribution $P$ as a prior tells the probabilities of occurance of all possible values of $X$ over its domain $D$, which is usually generated from historical observations. In this paper, *cumulative distribution function* (CDF) is used to describe the probability distribution of $X$, which tells the probability of occurance of $X$ that is less than or equal to $x$, where $x$ is some particular value over $D$. The CDF is generated from the *probability density function* (PDF) of $X$. The details of transforming from PDF to CDP is shown in Chapter. 2.5.

According to the *law of large numbers*, as the number of trials increases, the simulated result will approach the expected result of the quantitative problem. By *central limit theorem*, we know that the deviation between the simulated value and the true expected value will approach zero as the number of trials approaches infinity. For the simulations in this paper, the maximum number of trials is limited to some finite number $n$. As a result, as the number of trials approaches $n$, the deviation approaches zero. Therefore, the number of trials for each simulation is determined by how small the deviation we want to achieve.

## 2.5 Pseudo-random number sampling based on binary-search method

Pseudo-random number sampling is a numerical practice of generating random variable $X$ from a probability distribution $P$. We define $f$ to be the discrete PDF of $X$ where $f_x$ corresponds to the probability of occurance of $X = x$. The basic algorithm of pseudo-random number sampling from $f$ is as following. Notice that step (1) shows the details of transforming discrete PDF to discrete CDP.

(1) Define a discrete CDF $F$ of $X$ based on $f$ as

$$F_i = \sum_{j=1}^{i} f_j; F_0 := 0. \tag{2.5}$$

(2) Divide the interval $[0, 1]$ into $n$ individual intervals: $[F_0, F_1)$, $[F_1, F_2)$, $[F_2, F_3)$... $[F_{n-1}, F_n]$.

(3) Generate a random number $R$ uniformly from the interval $[0, 1)$.

(4) Apply any type of search method to find the index $i$ such that

$$F_{i-1} \leq R < F_i. \tag{2.6}$$

(5) Use the index $i$ found in (4) for particular use of computation.

Note that in step (4) we use the binary-search method for searching technique, whose computational time is $O(\log(l))$ where $l$ is the length of the searching list. The detailed algorithm can be found in Appendix B.

Up to now, we have introduced all the background that are needed for this dissertation .

# Chapter 3

# Corrected parameters for single-swap-experiment

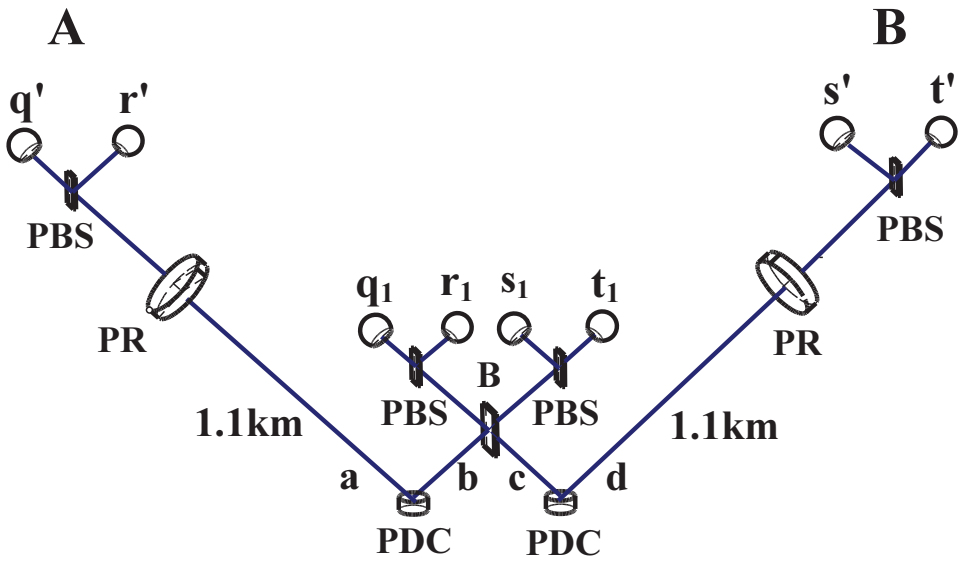



FIGURE 3.1: Simulated configuration for single-swap experiment. Two of the four intermediate PSO detectors are liquid-nitrogen-cooled GeAPD single-photon detectors and another two are $In_xGa_{1-x}As$ APDs single-photon detectors. Alice's and Bob's detectors are $In_xGa_{1-x}As$ APDs single-photon detectors. Each outer arm ($a$, $d$) has length equal to 1.1 km and each inner arm ($b$, $c$) has negligible length in km.

In this section we correct the parameters entered for the simulation of a single-swap experiment [9]. The simulated visibility has been compared to the experimental visibility

for a single-swap experiment [12]. The former lies within one standard error of the latter [9]. However, we find that the parameters entered for that simulation need to be corrected. We now provide the corrected parameters here.

We provide the simulated configuration of the single-swap experiment in Fig. 3.1. As given in the figure, two of the four intermediate PSO detectors are liquid-nitrogen-cooled GeAPD (NEC) single-photon detectors with efficiency around 10% for 40 kHz dark counts rate [12]. Another two detectors are $\mathrm{In_xGa_{1\text{-}x}As}$ APDs (id Quantique) single-photon detectors with efficiency around 30% for a dark count probability of around $10^{-4}$ per ns [12]. The time for which the detectors are active is around 300 ps [12]. Thus, the dark count probability of the former type of detector is approximately $10^{-5}$ and that of the latter type is approximately $3 \times 10^{-5}$.

The distances traveled from the two PDC sources to the PSO station (b and c) are negligible in km. Therefore, we assume that the transmission loss from the sources to the PSO station can be ignored. The coupling loss is around 30% in this experiment [12]. As a result, the "effective efficiencies" of the intermediate PSO detectors are

$$\eta_{\mathrm{e}}^{(1)} = \{7\%, 7\%, 21\%, 21\%\}, \tag{3.1}$$

respectively. The dark count probabilities of the intermediate PSO detectors are

$$\varrho^{(1)} = \{10^{-5}, 10^{-5}, 3 \times 10^{-5}, 3 \times 10^{-5}\}, \tag{3.2}$$

respectively.

The outer arms $a$ and $d$ both have length equal to 1.1 km. The loss coefficient is $\alpha = 0.25$ dB/km for photons at 1550 nm in this experiment [12]. According to the exponential rule, we know that

$$\eta_{\mathrm{t}} = 10^{-0.25 \times 1.1/10} \approx 94.9\%. \tag{3.3}$$

Alice's and Bob's detectors are $\mathrm{In}_x\mathrm{Ga}_{1-x}\mathrm{As}$ APDs (id Quantique) single-photon detectors, with efficiency of 30% and dark count probabilities around $3 \times 10^{-5}$. As a result, the "effective efficiencies" of Alice's and Bob's detectors are

$$\eta_{\mathrm{e}}^{(2)} = \{20\%, 20\%, 20\%, 20\%\}, \tag{3.4}$$

respectively. The dark count probabilities of Alice's and Bob's detectors are

$$\varrho^{(2)} = \{3 \times 10^{-5}, 3 \times 10^{-5}, 3 \times 10^{-5}, 3 \times 10^{-5}\}, \tag{3.5}$$

respectively.

The *photon-pair production rate* $\chi^2$ of the PDC source is around 6% here, which corresponds to the nonlinearity of the PDC source $\chi \approx 0.245$ [12]. These are the corrected simulated parameters based on situation of the single-swap experimental.

By entering the above parameters and setting both polarization angles to be $\pi/4$, we compute the maximum four-photon coincidence rate $Q_{1010}^{1010} + Q_{0101}^{1010}$ to be around 2.51% and the minimum four-photon coincidence rate $Q_{1001}^{1010} + Q_{0110}^{1010}$ to be around 0.38%. The former is 6.6 times the latter, while in the single-swap experiment, the maximum four-photon coincidence rate is nearly 8 times the minimum four-photon coincidence rate [12].

The simulated visibility is around 74% compared to 77.7% computed earlier [9]. The experimental result is 80%±4% [12]. Thus, we find that the theory does not make as good a prediction as appeared in the previous paper. Nevertheless, the simulated result of visibility lies within 2 standard errors of the experimental result and we consider the theory has generated good simulated results that can be useful to predict the experimental results.

Having corrected the parameters for the simulation of single-swap experiment, which provides a clearer vision of how well the prediction of visibility based on the theory is, we now show how to apply our sampling method to compute the visibilities of various swaps based on the theory and how to verify it by doing various simulations.

# Chapter 4

# Approach

In this Chapter we present the approach of how to apply our sampling method to compute visibilities for various numbers of swaps and how to verify our sampling method. In Chapter. 4.1 we introduce the basic concept of our sampling method based on Monte Carlo simulation. In Chapter. 4.2 we show the detailed procedure of how we apply our sampling method to compute the visibilities for various numbers of swaps. In Chapter. 4.3 we show how we verify our sampling method in various simulations.

## 4.1 Basic concept

The simulation of $Q^{\boldsymbol{qrst}}_{q'r's't'}$ is based on repeated computation through Eq. (2.2) over different combinations of the four-tuple indices $(\boldsymbol{ijkl})$ and $(i'j'k'l')$, which are the numbers of photons in spatial modes. If we treat $(\boldsymbol{ijkl})$ and $(i'j'k'l')$ as inputs, and Eq. (2.2) to be the formula of the algorithm, then Monte Carlo simulation can be applied here to compute $Q^{\boldsymbol{qrst}}_{q'r's't'}$.

As Eq. (2.2) requires us to take all the possible values of $(\boldsymbol{ijkl})$ and $(i'j'k'l')$ with each index ranging from 0 to infinity, which is infeasible, we set the upper bound of the number of photons in each mode to be $n_{\max} = 3$ [11]. As a result, the domain $D$ of each index of $(\boldsymbol{ijkl})$ and $(i'j'k'l')$ is $[0, 3]$. As the domain of each index of $(\boldsymbol{ijkl})$ and $(i'j'k'l')$ of $N \geq 4$ swaps is the same as that of $N = 2$ swaps and $N = 3$ swaps, the probability distribution $P$ of the inputs $(\boldsymbol{ijkl})$ of $N \geq 4$ simulation can be generated through one-time computation of $Q^{\boldsymbol{qrst}}_{q'r's't'}$ from achievable $N = 2$ and $N = 3$ simulations and recorded in the $N = 2$ and $N = 3$ prior lists, respectively.

For each trial of the new simulation, we apply pseudo-random number sampling technique to generate the input $(\boldsymbol{ijkl})$ from the prior lists, whereas we takes all the possible

values of $(i'j'k'l')$ with each index ranging from 0 to 3. The algorithm of Eq. (2.2) then takes the input and generates an output. The final results of $Q^{\boldsymbol{qrst}}_{q'r's't'}$ can then be gained by aggregating all the outputs generated by the algorithm for large number of trials. Finally, the visibility can be calculated through Eq. (2.1) based on those simulated results of $Q^{\boldsymbol{qrst}}_{q'r's't'}$. We now provide the detailed procedure.

## 4.2 Procedure

Our sampling method is accomplished via the following seven steps.

1. We generate two prior lists that select the most significant combinations of $(\boldsymbol{ijkl})$ to the computational results of conditional probabilities through Eq. (2.2), from $N = 2$ and $N = 3$ simulations respectively. Then we order each of the lists from the most significant combination to the least significant combination among them. For each row of the list we record a combination of $(\boldsymbol{ijkl})$ and its CDF value $F$.

2. For each new simulation of $N$ swaps, we determine which and how many prior lists we want to use. For example, for $N = 4$ swaps we need two $N = 2$ prior lists; for $N = 5$ swaps we need one $N = 2$ prior list and one $N = 3$ prior list, etc. The choice is flexible as long as the addition of the numbers of $N$ of the prior lists is equal to the number of swaps $N$ we are simulating for. Up to now we only have the $N = 2$ and $N = 3$ prior lists.

3. We pick the number of combinations we want to use for simulation from each prior list, i.e., $n_1, n_2 \ldots$.

4. For each trial:

a) We apply pseudo-random number sampling based on the binary-search method to generate an index of row $m$ from the first prior list. Then we set the inputs based on $m$ from all the prior lists we use (details in Chapter. 5), which we denote as $(\boldsymbol{ijkl}^{(m)})$. There are in total $n_2 n_3 \ldots n_{\mathrm{f}}$ possible combinations of $(\boldsymbol{ijkl}^{(m)})$ for each trial, where $n_{\mathrm{f}}$ is the number of samples we pick from the last prior list.

b) We compute the conditional probabilities $Q_{q'r's't'}^{\boldsymbol{qrst},\mathrm{block}(m)}$ for each $(\boldsymbol{ijkl}^{(m)})$ we gain in step 4(a), which is calculated through the equation

$$Q_{q'r's't'}^{\boldsymbol{qrst},\mathrm{block}(m)} = \sum_{i'j'k'l'=0}^{3} p\left(q'r's't'|i'j'k'l'\right) W_{i'j'k'l'}^{\boldsymbol{ijkl}^{(m)}} P_{\boldsymbol{ijkl}^{(m)}}^{\boldsymbol{qrst}}, \tag{4.1}$$

and record them in the memory of computer.

c) We delete the $m$th row from the first prior list, which has already been used for calculating $Q_{q'r's't'}^{\boldsymbol{qrst},\mathrm{block}(m)}$, to avoid duplicate computations.

5. We repeat step 4 for $n_1$ times.

6. We aggregate all the recorded $Q_{q'r's't'}^{\boldsymbol{qrst},\mathrm{block}(m)}$ together to get the simulated conditional probabilities $Q_{q'r's't'}^{\boldsymbol{qrst}}$, i.e.,

$$Q_{q'r's't'}^{\boldsymbol{qrst}} = \sum_{m} Q_{q'r's't'}^{\boldsymbol{qrst},\mathrm{block}(m)}. \tag{4.2}$$

7. We calculate the two-photon visibility based on the simulated conditional probabilities through Eq. (2.1).

The main algorithm of our sampling method can be found in Appendix B.2. We now show how we verify our sampling method in various simulations.

## 4.3 Verify sampling method

Having introduced the detailed procedure of our sampling method, we now show how we verify it in various simulations.

### 4.3.1 $N = 3$ simulation

The first verification we do is to verify our sampling method for $N = 3$ simulation. The direct computational visibilities of $N = 3$ swaps have been gained with parameters $\eta_e = 0.04$ and $\varrho = 10^{-5}$ for all single-photon detectors [11]. We verify our sampling method for $N = 3$ simulation by comparing the sampled visibilities based on $N = 2$ and

$N = 3$ prior lists to the direct computational visibilities of $N = 3$ swaps, respectively, and see how big the discrepancies are for various values of $\chi$.

### 4.3.2 $N = 4$ simulation

The second verification we do is to verify our sampling method for $N = 4$ simulation. As we discussed in Chapter. 2.3, the direct computational visibility of $N = 4$ swaps cannot be gained by using a single node on our desktop computer due to excessive computational time. However, we apply parallel computing technique on a supercomputer cluster using 256 cores with each CPU being Intel(R) Xeon(R) CPU E5530 @ 2.40GHz and successfully gain the visibility of $N = 4$ swaps with parameters $\chi = 0.1$, $\eta_e = 0.04$ and $\varrho = 10^{-5}$ for all single-photon detectors, which cost more than 7 days' wall-clock time. The visibility is found to be 0.403. We then gain the sampled visibility of $N = 4$ by entering the same parameters and compare it to the direct computational visibility to verify our sampling method for $N = 4$ simulation.

### 4.3.3 $N = 3, 4, 5, 6$ simulations in semi-ideal case of using single-photon sources

As we have only tested our sampling method for $N = 4$ simulation for $\chi = 0.1$, the verification of sampling method for $N \geq 4$ simulations is incomplete. The reason why we cannot finish the direct computation of visibilities for $N \geq 4$ in reasonalble time using a single node on a desktop computer is because of the hugeness of the Hibert space of numbers of photons, which is due to the multipair nature of PDC sources. Therefore, we can reduce the computational time by replacing PDC sources with single-photon sources. The single-photon source will generate exactly one entangled photon pair at a time and that will largely shrink the dimension of Hibert space. Although an ideal single-photon source does not exist yet, it does not prevent us from using it and verifying our sampling method in a theoretical way. As a result, the third verification we do is to verify our sampling method for $N = 3, 4, 5, 6$ simulations in the semi-ideal case when using single-photon sources.

As we only change the sources and leave everything else the same, the only modification we need to do is to derive the new $W^{\boldsymbol{ijkl}}_{i'j'k'l'}$ in Eq. (2.2), which can be calculated through [9],

$$W^{\boldsymbol{ijkl}}_{i'j'k'l'} = \left| A^{\boldsymbol{ijkl}}_{i'j'k'l'} \right|^2, \tag{4.3}$$

where the new $A^{\boldsymbol{ijkl}}_{i'j'k'l'}$ is found to be the one derived in Appendix A.

To check the veracity of the new formula, we simulate the conditional probabilities in the ideal-world scenario, i.e, ideal photon-number discriminating detectors, zero transmission loss and zero coupling loss. By setting both of the polarization angles to be $\pi/4$ (correspondingly $\tilde{\alpha} = \tilde{\delta} = \pi/2$) [11], we obtain $Q_{1010}^{\mathbf{1010}} = Q_{1010}^{\mathbf{0101}} = 0.5$ and $Q_{1010}^{\mathbf{1001}} = Q_{1010}^{\mathbf{0110}} = 0$, which perfectly satisfy our prediction. As in an ideal-world scenario, after all the intermediate PSO stations have been projected onto the state $|\phi^-\rangle = \frac{1}{\sqrt{2}}(|1010\rangle - |0101\rangle)$, the outermost two modes will 100% be projected onto the same state. Therefore the conditional probability for Alice and Bob to observe the four-tuple click event (1010) is 0.5 and that to observe (0101) is 0.5, while it is impossible for them to observe the four-tuple click event (1001) or (0110).

By changing PDC sources to single-photon sources, we are able to directly compute the visibilities up to $N = 6$ swaps in reasonable time, even without truncating $(\boldsymbol{ijkl})$ and $(i'j'k'l')$. We then apply our sampling method to compute the sampled visibilities up to $N = 6$ swaps. We compare the sampled visibilities to the corresponding direct computational visibilities to verify our sampling method in the semi-ideal case when using single-photon sources.

Those are the simulations that we do to verify our sampling method. The results of verification are shown in Chapter. 5. We now introduce how we set the inputs from the prior lists for each trial of simulations in the following Chapter.

# Chapter 5

# Method of setting the inputs

In this chapter we show how we set the inputs ($\boldsymbol{ijkl}^{(m)}$) based on $N = 2$ and $N = 3$ prior lists for each trial of the simulation for $N \leq 6$ swaps, which corresponds to step 4(a) in our procedure of sampling method that listed in Chapter. 4.2.

## 5.1 $N = 2$ simulation

By sampling $N = 2$ swaps we only need one $N = 2$ prior list. We directly set the ($\boldsymbol{ijkl}^{(m)}$) based on those combinations picked from $N = 2$ prior list as they represent

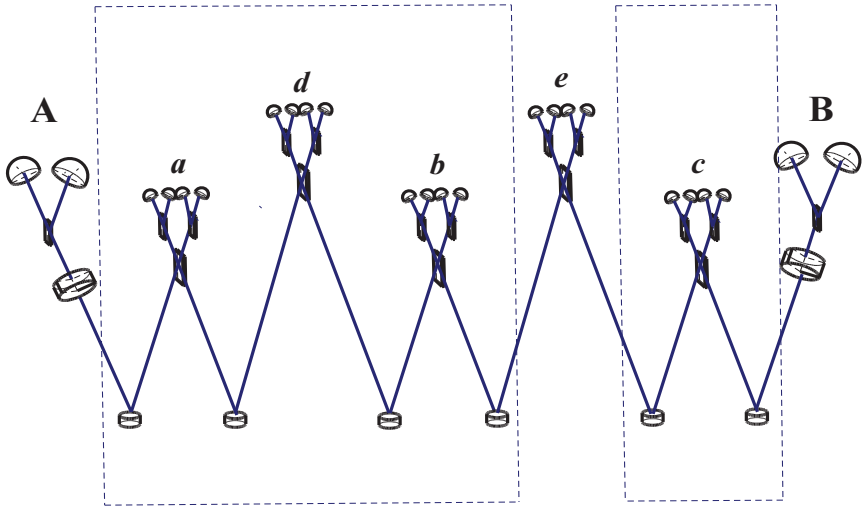



FIGURE 5.1: $N = 3$ swaps viewed as a combination of an imaginary $N = 2$ swaps and an imaginary $N = 1$ swap. $a$, $b$, $c$, $d$, $e$ correspond to the 1st, 2nd, 3rd, 4th and 5th PSO stations of $N = 3$ swaps, respectively. At the same time, $a$, $b$, $d$ correspond to the 1st, 2nd and 3rd PSO stations of the imaginary $N = 2$ swaps, respectively.

the numbers of photons in the same modes, i.e., for each trial, we set the $(\boldsymbol{ijkl}^{(m)})$ in a way like

$$\begin{aligned}(i_1j_1k_1l_1)^{(m)}_{N=2} &= (i_1j_1k_1l_1)^{(m)}_{N=2,\text{prior}}\,,\\ (i_2j_2k_2l_2)^{(m)}_{N=2} &= (i_2j_2k_2l_2)^{(m)}_{N=2,\text{prior}}\,,\\ (i_3j_3k_3l_3)^{(m)}_{N=2} &= (i_3j_3k_3l_3)^{(m)}_{N=2,\text{prior}}\,.\end{aligned}$$

This is how we set $(\boldsymbol{ijkl}^{(m)})$ for $N = 2$ simulation based on $N = 2$ prior list.

## 5.2 $N = 3$ simulation

Similarly, by sampling $N = 3$ swaps we only need one $N = 3$ prior list. We take the values of $(\boldsymbol{ijkl}^{(m)})$ to be the same as the corresponding ones in the $N = 3$ prior list. This is how we set $(\boldsymbol{ijkl}^{(m)})$ for $N = 3$ simulation based on $N = 3$ prior list.

Besides, we find that there is another way to put settings of $(\boldsymbol{ijkl}^{(m)})$ for $N = 3$ simulation, i,e., by using the $N = 2$ prior list. The reason is that we can view the $N = 3$ swaps as a combination of one $N = 2$ swaps and one $N = 1$ swap, with the $N = 2$ swaps on the left and the $N = 1$ swap on the right, joined by a PSO station in the middle, as shown in Fig. 5.1. As given in Fig. 5.1, the 1st, 2nd and 4th PSO stations of the $N = 3$ swaps correspond to the 1st, 2nd and 3rd PSO stations of the imaginary $N = 2$ swaps, respectively. Therefore, for each trial, we set the $(\boldsymbol{ijkl}^{(m)})$ in a way like

$$\begin{aligned}(i_1j_1k_1l_1)^{(m)}_{N=3} &= (i_1j_1k_1l_1)^{(m)}_{N=2,\text{prior}}\,,\\ (i_2j_2k_2l_2)^{(m)}_{N=3} &= (i_2j_2k_2l_2)^{(m)}_{N=2,\text{prior}}\,,\\ (i_4j_4k_4l_4)^{(m)}_{N=3} &= (i_3j_3k_3l_3)^{(m)}_{N=2,\text{prior}}\,,\end{aligned}$$

as they represent the numbers of photons in the same modes and take all the possible values of $(i_3j_3k_3l_3)^{(m)}_{N=3}$ and $(i_5j_5k_5l_5)^{(m)}_{N=3}$ with each index ranging from 0 to 3. This is how we set $(\boldsymbol{ijkl}^{(m)})$ for $N = 3$ simulation based on $N = 2$ prior list.

## 5.3 $N = 4$ and $N \geq 5$ simulations

For $N = 4$ simulation, there are seven sets of $(\boldsymbol{ijkl}^{(m)})$. As given in the Fig. 5.2, we can view the $N = 4$ swaps as a combination of two imaginary $N = 2$ swaps, joined by a PSO station in between. The 1st, 2nd and 3rd PSO stations of the first imaginary $N = 2$ swaps correspond to the 1st, 2nd and 5th PSO stations of the $N = 4$ swaps, respectively. The 1st, 2nd and 3rd PSO stations of the second imaginary $N = 2$ swaps correspond to

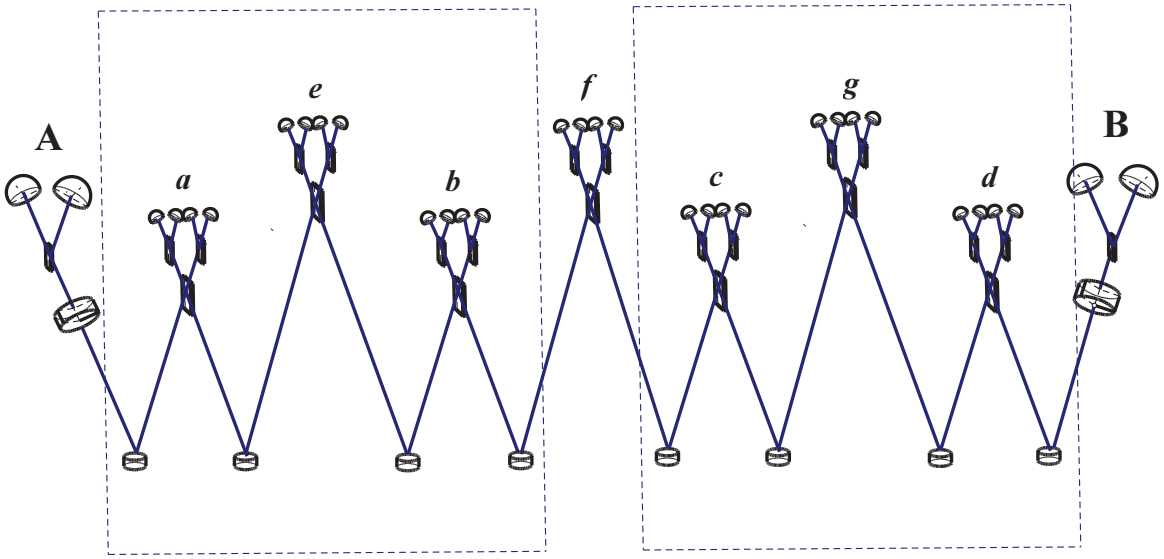



FIGURE 5.2: $N = 4$ swaps viewed as a combination of two $N = 2$ swaps. $a$, $b$, $c$, $d$, $e$, $f$, $g$ correspond to the 1st, 2nd, 3rd, 4th, 5th, 6th and 7th PSO stations of $N = 4$ swaps, respectively. At the same time, $a$, $b$, $e$ correspond to the 1st, 2nd and 3rd PSO stations of the first imaginary $N = 2$ swaps, respectively. $c$, $d$, $g$ correspond to the 1st, 2nd and 3rd PSO stations of the second imaginary $N = 2$ swaps, respectively.

the 3rd, 4th and 7th PSO stations of the $N = 4$ swaps, respectively. Therefore, for each trial, we set the first part of $(\boldsymbol{ijkl}^{(m)})$ according to the combinations we pick from the first $N = 2$ prior list, in a way like

$$
\begin{aligned}
(i_1 j_1 k_1 l_1)^{(m)}_{N=4} &= (i_1 j_1 k_1 l_1)^{(m)}_{N=2,\text{1st prior}}\,, \\
(i_2 j_2 k_2 l_2)^{(m)}_{N=4} &= (i_2 j_2 k_2 l_2)^{(m)}_{N=2,\text{1st prior}}\,, \\
(i_5 j_5 k_5 l_5)^{(m)}_{N=4} &= (i_3 j_3 k_3 l_3)^{(m)}_{N=2,\text{1st prior}}\,.
\end{aligned}
$$

For each of the setting we put above, we set the second part of $(\boldsymbol{ijkl}^{(m)})$ from the second $N = 2$ prior list, started from the 1st combination to the $n_2$th combination. If we denote the index of combination we pick from the second prior list to be $k$, then the way we set the second part of $(\boldsymbol{ijkl}^{(m)})$ in the $k$th run is

$$
\begin{aligned}
(i_3 j_3 k_3 l_3)^{(m)}_{N=4} &= (i_1 j_1 k_1 l_1)^{(k)}_{N=2,\text{2nd prior}}\,, \\
(i_4 j_4 k_4 l_4)^{(m)}_{N=4} &= (i_2 j_2 k_2 l_2)^{(k)}_{N=2,\text{2nd prior}}\,, \\
(i_7 j_7 k_7 l_7)^{(m)}_{N=4} &= (i_3 j_3 k_3 l_3)^{(k)}_{N=2,\text{2nd prior}}\,.
\end{aligned}
$$

After that we take all the possible values of $(i_6 j_6 k_6 l_6)^{(m)}_{N=4}$ with each index varying from 0 to 3. This is how we set $(\boldsymbol{ijkl}^{(m)})$ for $N = 4$ simulation based on two $N = 2$ prior lists.

Similarly, we can view the $N = 5$ swaps as a combination of one imaginary $N = 2$ swaps and one imaginary $N = 3$ swaps; $N = 6$ swaps as a combination of two imaginary $N = 3$ swaps, with a joined PSO station connecting them, respectively. Therefore, we can set the inputs $(\boldsymbol{ijkl})$ of $N = 5$ and $N = 6$ simulations in a similar way as we set those for $N = 4$ simulation.

Having introduced the details of how we apply our sampling method to compute visibilities of $N \leq 6$ swaps and set the inputs, we now show the results of verification in the following chapter.

# Chapter 6

# Results of verification

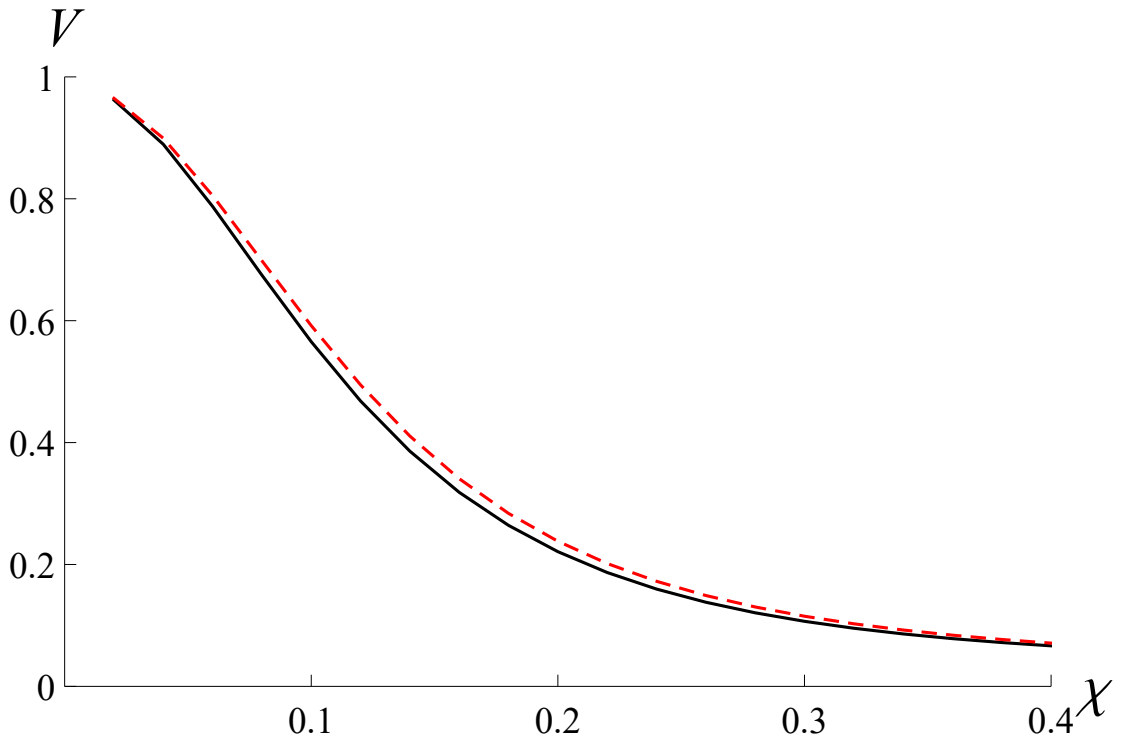
In this chapter we show the results of simulations that are done for verification of our sampling method as introduced in Chapter. 4.3. In Chapter. 6.1 we compare the sampled visibilities of $N = 3$ swaps based on $N = 2$ and $N = 3$ prior lists to the direct computational visibilities of $N = 3$ swaps, respectively. In Chapter. 6.2 we show the sampled visibilities of $N = 4$ swaps based on $N = 2$ prior list and compare them to the direct computational visibilities. In Chapter. 6.3 we show the sampled vs direct computational visibilities for $N \leq 6$ swaps in the semi-ideal case when using single-photon sources.

## 6.1 $N = 3$ simulation

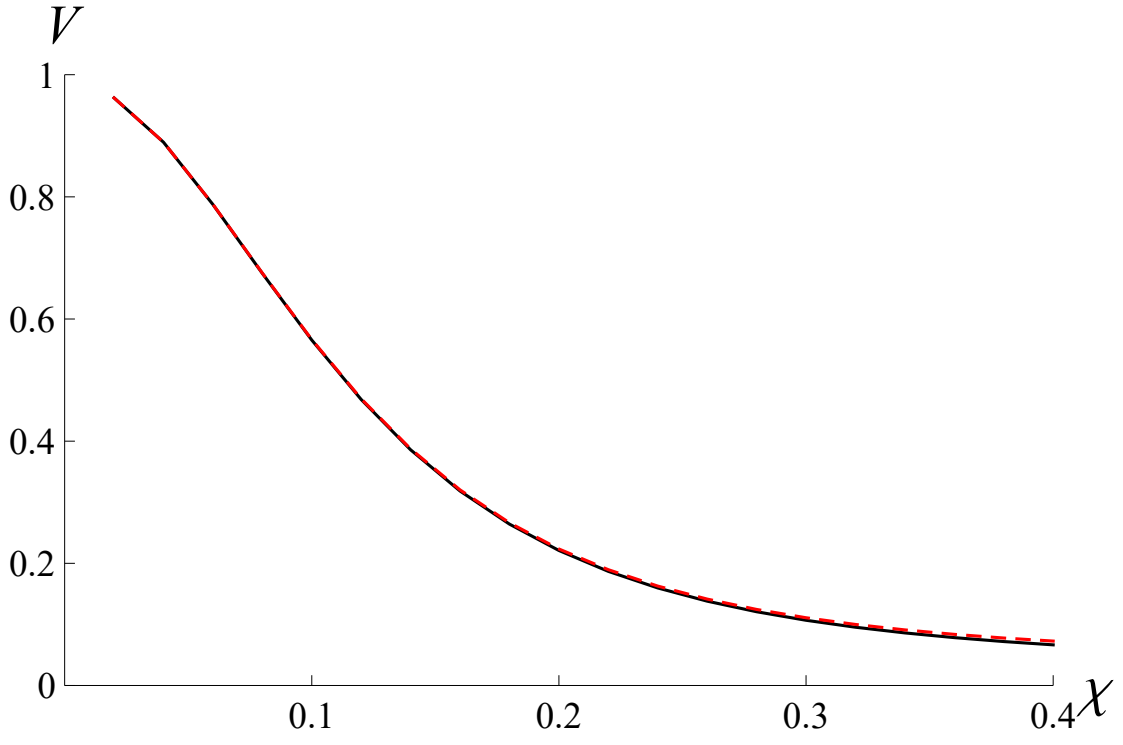
We obtain the sampled vs direct computational visibilities of $N = 3$ swaps by using all the combinations from $N = 2$ prior list (a) and $N = 3$ prior list (b) in Fig. 6.1. There is only a small gap between the two curves in each figure. The maximum difference between the sampled and direct computational visibility for (a) is 0.026449 and for (b) is 0.006192, which shows the success of applying our sampling method to compute visibilities for $N = 3$ swaps.

## 6.2 $N = 4$ simulation

The direct computational visibility of $N = 4$ swaps with parameters listed in Chapter. 4.3.2 is 0.403, whereas the sampled visibility is 0.466 by using 1000 combinations from each $N = 2$ prior list. There is a 0.063 difference between the sampled visibility and the direct computational visibility.




(a)




(b)

FIGURE 6.1: Sampling results of visibilities of $N = 3$ swaps versus $\chi$ compared to the direct computational results of visibilities versus $\chi$, using all the combinations from (a) $N = 2$ prior list and (b) $N = 3$ prior list, respectively. $\chi \in \{0.02, 0.40\}$, $\eta_e = 0.04$, $\varrho = 0.00001$ for all detectors. The red-dashed curve represents the sampling results, while the black-solid curve represents the direct computational results.

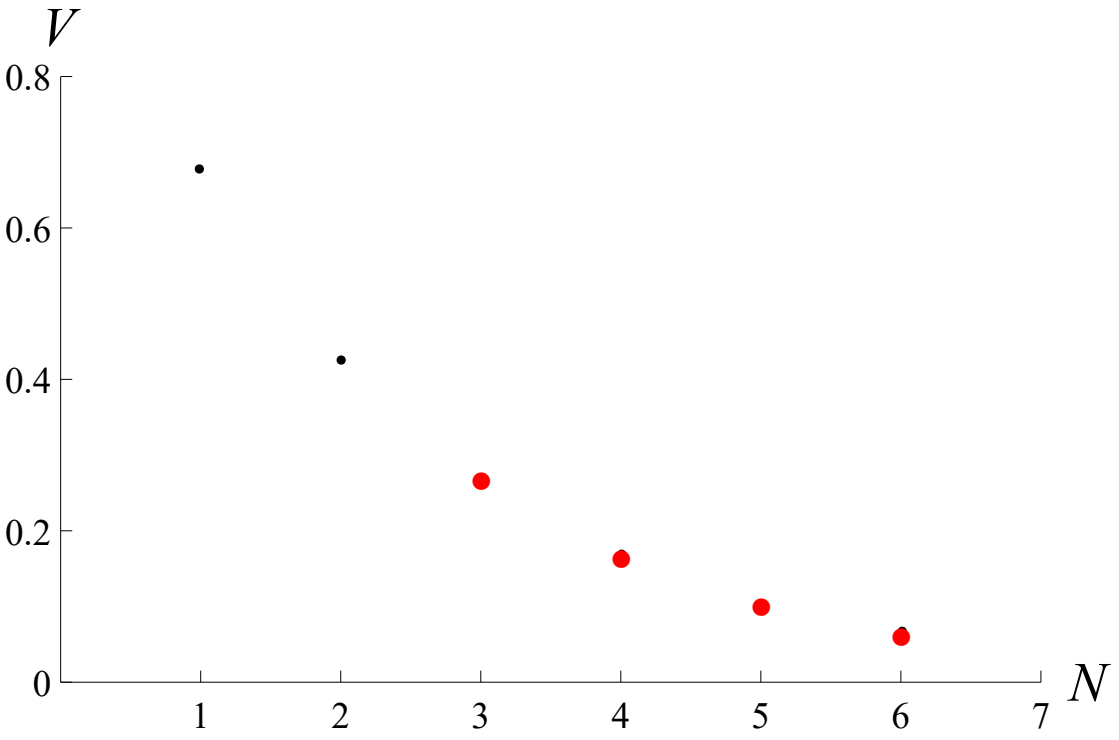



FIGURE 6.2: (Color online) Sampling results compared to direct computational visibilities for $N = 1, 2, 3, 4, 5, 6$ swaps using single-photon sources, by using 100 combinations from each $N = 2$ prior list and 1000 combinations from each $N = 3$ prior list. The parameters entered are $\eta_e = 0.2$ and $\varrho = 0.01$ for all the single-photon detectors. The (big-red) dots are sampled visibilities of $N = 3, 4, 5, 6$ swaps. The (small-black) dots are the direct computational visibilities of $N = 1, 2, 3, 4, 5, 6$ swaps. The big-red dots basically overlap with their corresponding small-black dots.

As shown in Fig. 2.1(a), the maximum difference between sampled and direct computational visibility lies within the interval $\chi \in [0.1, 0.2]$ for $N = 3$ simulation. Similar pattern is expected for $N = 4$ simulation. Therefore, the difference 0.063 observed for $\chi = 0.1$ is considered to be near the maximum difference between the sampled and direct computational visibilities of $N = 4$ swaps. As a result, our sampling method produces good upper bounds of true theoretical visibilities of $N = 4$ swaps.

## 6.3 $N \leq 6$ simulations using single-photon sources

The sampled visibilities vs the direct computational visibilities of $N \leq 6$ swaps using single-photon sources are shown in Fig. 6.2. As given in Fig. 6.2, the sampled visibilities are nearly the same as their corresponding direct computational visibilities, with maximum difference being 0.005665, which proves that our sampling method works well in the semi-ideal case of using ideal single-photon sources. This gives us confidence to apply it for the real-world case of using imperfect PDC sources.

The discrepancy between sampled and direct computational visibilities can be ignored for other sets of parameters as the most significant combinations of ($\boldsymbol{ijkl}$) recorded in the prior lists are always computed first, regardless of what parameters are entered for simulations. As a result, our sampling method is verified completely for $N = 3$ simulations and partially for $4 \leq N \leq 6$ simulations (only in semi-ideal case). Armed with that, we now show the results of simulated visibilities of $N \leq 6$ swaps using imperfect PDC sources.

# Chapter 7

# Results and discussion

In this chapter we provide the simulated visibilities of $N \leq 6$ swaps using imperfect PDC sources. By entering the parameters based on current technologies as introduced in Chapter. 2.2, we gain the simulated visibilities vs $\chi$ up to $N = 6$ swaps in Fig. 7.1. As shown in Fig. 7.1, all sampled visibilities lie within the predicted range. The expected

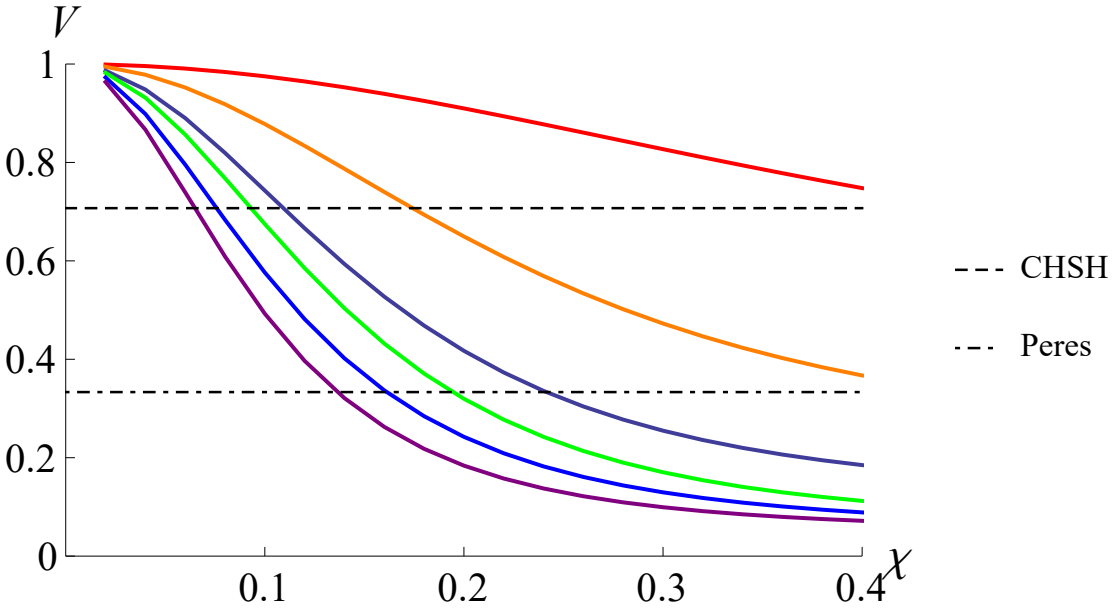



FIGURE 7.1: Simulated results of visibility of $N = 1$ swap (red), $N = 2$ swaps (orange), $N = 3$ swaps (grey), $N = 4$ swaps (green), $N = 5$ swaps (blue) and $N = 6$ swaps (purple), with topmost for $N = 1$ swap to bottommost for $N = 6$ swaps. The simulated results of $N = 1$ and $N = 2$ are gained from direct computation, whereas those of $N \geq 3$ are gained by applying sampling method. For $N = 3$ simulation we use 10802 combinations from the $N = 3$ prior list. For $N = 4, 5, 6$ simulations we use 200 combinations from each of the two prior lists (corresponds to 40000 different combinations totally).

ranges of $\chi$ to break CHSH inequality [16] (dashed line) and Peres critetia [17] (dot-dashed line) for different numbers of swaps can be clearly seen from the figure.

The simulated visibilities of various numbers of swaps in Fig. 7.1 provide us a clear vision of what are the upper bounds of experimental results of visibility in real-world experiments. As given in Fig. 7.1, the visibilities fall rapidy as $\chi$ increases for higher number of swaps. Therefore, in order to achieve high-enough visibility for the purpose of LDQC, the brightness of the PDC sources, which is proportional to $\chi^2$, should be controlled in a range of small values.

However, too-small $\chi$ will lead to too-low $4N$-photon-coincidence rates as considerable vacuum component will be generated in the mixed states coming out of the PDC sources, which will result in overly-long experimental run time. Additionally, the $4N$-photon-coincidence rates decrease as the number of swaps increases. Indeed, even in the ideal case of perfect detectors with unit efficiency and zero dark counts, the maximum secret key-generation rate (SKGR) of $N = 3$ swaps, which can achieve 850 km, is three million centuries per bit for optimal choice $\chi = 0.07$ [18]. This result shows the infeasibility of real-world long-distnce quantum key distribution (QKD) using this quantum-relay protocol.

When the same setup is used in QKD protocol [18], visibility is directly related to the error rate $Q$ as $Q = (1 - V)/2$, thus for large number of concatenations , very low $V$ would yield a high $Q$. One way to attain high $V$ is to keep $\chi$ very small as can be seen from Fig. 7.1, but this has adverse effect on the key bits lost in the sifting process for analysis done for concatenations up to $N = 3$ [18]. Our analysis suggests the continual decrease in SKGR for concatenations $N > 3$ as well. Thus increasing the concatenated swapping would not be feasible for practical QKD and quantum memories are vital to achieve a reasonable SKGR.

# Chapter 8

# Conclusion

We have corrected the parameters entered for the simulation of single-swap experiment that was done earlier [9]. The corrected simulated visibility lies within two standard errors of the experimental result, which provides a clearer vision of how well the theoretical prediction is.

We have developed a Monte-Carlo-based sampling method, equipped with pseudo-random number sampling based on the binary-search method to compute the visibilities for $N \geq 4$ swaps using PDC sources. We have shown the approach of applying our sampling method to compute visibilities for various numbers of swaps and corresponding algorithms. We have verified our sampling method by comparing sampling visibilities to direct computational visibilities in various simulations.

We have provided the simulated results of visibilities of $N \leq 6$ swaps using PDC sources by using our sampling method. The simulated visibilities are good upper bounds of the future experimental results and therefore, good guidance for experimentalists who want to perform a real-world experiments of LDQC through $N \geq 2$ entanglement-swapping operations in a quantum-relay configuration. Our results show that to achieve high-enough visibilities for the purpose of LDQC for $N \geq 3$ swaps based on current technologies, $\chi$ should be less than 0.1. However, this range of $\chi$ will lead to too-low $4N$-photon-coincidence rates and thus, excessive experimental run time.

We have addressed the feasibility of real-world QKD for $N \geq 3$ swaps using this quantum-relay configuration because key rates are atrociously low for $\chi$ that can generate high-enough visibility. As a result, new technologies such as optical quantum memories are needed to solve this problem [18].

There are some potential developments. The simulated visibilities of $N \geq 7$ swaps can be gained by applying sampling method with more than two prior lists. Besides, as long

as we generate the $N \geq 4$ prior lists, the simulations for higher number of swaps can be easily achieved. For example, we can apply our sampling method based on three $N = 4$ prior lists to compute the visibilities of $N = 12$ swaps.

# Appendix A

# Formulas

In this appendix we provide all the formulas that are needed in calculating conditional probabilities $Q^{\boldsymbol{qrst}}_{q'r's't'}$ through Eq. (2.2).

In each single-swap element, given the theoretical hypothesis that the four-ideal-photon-number-discriminating-detectors without any loss would have yielded the readouts $(ijkl)$, the conditional probability to observe the readouts $(qrst)$ from four-imperfect-single-photon-detectors including losses is [9]

$$p(qrst|ijkl) = p(q|i)p(r|j)p(s|k)p(t|l), \tag{A.1}$$

with

$$\begin{aligned} p(q=0|i) &= (1-\varrho)[1-\eta_e(1-\varrho)]^i, \\ p(q=1|i) &= 1-(1-\varrho)[1-\eta_e(1-\varrho)]^i, \end{aligned} \tag{A.2}$$

where $\eta_e$ is defined in Eq. (2.3).

Relatively, in each single-swap element, given the readouts $(qrst)$ of the four-imperfect-single-photon-detectors including losses, we infer the hypothetical readouts of four-ideal-photon-number-discriminating-detectors without any loss to be $(ijkl)$, with probability $P^{qrst}_{ijkl} \equiv p(ijkl|qrst)$. By applying Bayes' theorem, this probability is found to be [9]

$$P^{qrst}_{ijkl} = \frac{p(qrst|ijkl)p(ijkl)}{\sum\limits_{i'j'k'l'=0}^{\infty} p(qrst|i'j'k'l')p(i'j'k'l')}, \tag{A.3}$$

where $p(ijkl)$ is the prior probability for the resultant state of the outermost two modes to be projected onto $|\phi_{ijkl}\rangle$, i,e., $p(ijkl) \equiv \langle\phi_{ijkl}|\phi_{ijkl}\rangle$. The probability $P^{\boldsymbol{qrst}}_{\boldsymbol{ijkl}}$ for all

PSO stations can then be calculated through

$$P^{\boldsymbol{qrst}}_{\boldsymbol{ijkl}} = P^{q_1r_1s_1t_1}_{i_1j_1k_1l_1} P^{q_2r_2s_2t_2}_{i_2j_2k_2l_2} P^{q_3r_3s_3t_3}_{i_3j_3k_3l_3} \dots . \tag{A.4}$$

The transitional probability $W^{\boldsymbol{ijkl}}_{i'j'k'l'}$ is the norm of the complex transitional probability amplitude $A^{\boldsymbol{ijkl}}_{i'j'k'l'}$ as given in Eq. (4.3), where the explicit form of the formula of $A^{\boldsymbol{ijkl}}_{i'j'k'l'}$ in PDC source case is [11]

$$\begin{aligned}
A^{\boldsymbol{ijkl}}_{i'j'k'l'} = & \prod_{p=1}^{N} \frac{1}{\sqrt{2^{i_p+j_p+k_p+l_p} i_p! j_p! k_p! l_p!}} \frac{(\tanh\chi)^{i_p+j_p+k_p+l_p}}{\cosh^{4N}\chi} \sum_{\mu_p=0}^{i_p} \sum_{\nu_p=0}^{j_p} \sum_{\kappa_p=0}^{k_p} \sum_{\lambda_p=0}^{l_p} \\
& \times (-1)^{\mu_p+\nu_p} \binom{i_p}{\mu_p} \binom{j_p}{\nu_p} \binom{k_p}{\kappa_p} \binom{l_p}{\lambda_p} \\
& \times \prod_{n=1}^{N-1} \Omega(\mu_n, \lambda_n, i_{N+n}, l_{N+n}) \Omega(\nu_n, \kappa_n, j_{N+n}, k_{N+n}) \frac{\sqrt{i_{N+n}! j_{N+n}! k_{N+n}! l_{N+n}!}}{(\sqrt{2})^{i_{N+n}+j_{N+n}+k_{N+n}+l_{N+n}}} \\
& \times \delta_{i_{N+n}+l_{N+n},\mu_n+\lambda_n+i_{n+1}+l_{n+1}-\mu_{n+1}-\lambda_{n+1}} \delta_{j_{N+n}+k_{N+n},\nu_n+\kappa_n+j_{n+1}+k_{n+1}-\nu_{n+1}-\kappa_{n+1}} \\
& \times (\nu_N+\kappa_N)!(j_1+k_1-\nu_1-\kappa_1)! \sqrt{\frac{j'!k'!}{i'!l'!}} \sum_{n_a=0}^{\mathrm{Min}[j',\nu_N+\kappa_N]} \sum_{n_d=0}^{\mathrm{Min}[k',j_1+k_1-\nu_1-\kappa_1]} \\
& \times \left(\mathrm{i}\tan\frac{\tilde{\alpha}}{2}\right)^{\nu_N+\kappa_N+j'-2n_a} \times \left(\cos\frac{\tilde{\alpha}}{2}\right)^{i'+j'-2n_a} \left(i\tan\frac{\tilde{\delta}}{2}\right)^{k'+j_1+k_1-\nu_1-\kappa_1-2n_d} \\
& \times \left(\cos\frac{\tilde{\delta}}{2}\right)^{l'+k'-2n_d} \frac{(i'+j'-n_a)!(l'+k'-nd)!}{n_a! n_d! (j'-n_a)! (k'-n_d)! (\nu_N+\kappa_N-n_a)! (j_1+k_1-\nu_1-\kappa_1-n_d)!} \\
& \times \delta_{i'+j',\mu_N+\nu_N+\kappa_N+\lambda_N} \delta_{k'+l',i_1+j_1+k_1+l_1-\mu_1-\nu_1-\kappa_1-\lambda_1} .
\end{aligned} \tag{A.5}$$

Up to now we have given all the formulas that are needed for Eq. (2.2).

# Appendix B

# Algorithm

In this appendix we provide the details of our algorithms that correspond to various steps in Chapter. 4. In Appendix B.1 we introduce our algorithm of pseudo-random number sampling. In Appendix B.2 we inroduce the main algorithm of using our sampling method to calculate visibility.

## B.1 Algorithm of pseudo-random number sampling

As the number of samples we pick from each prior list is limited, we prefer to pick those most significant combinations for calculating $Q_{q'r's't'}^{\boldsymbol{qrst},\text{block}(m)}$ through Eq. (4.1). At the same time, we give some chance for the less significant ones to be picked to remain the randomness. To achive this goal, we design our prior lists to have the property that the interval between the cumulative function values $F_{k-1}$ and $F_k$ becomes smaller and smaller as $k$ increases, where $k$ is the index of row. As the random number $R$ for pseudo-random number sampling is uniformly generated from $[0, 1)$, the combination recorded at the row with smaller index will always have greater chance to be picked, which satisfies our goal. We design our own version of pseudo-random number sampling based on the general procedure of that, which is listed in Chapter. 2.5. We introduce the inputs, outputs and pseudo-codes of our own version of pseudo-random number sampling in Algorithm 1.

**Algorithm 1** Pseudo-random number sampling

**Input:**

$\{F\}$: a monotonically increased $l \times 1$ array of CDF value $F$

$i_{\mathrm{l}}$: lowest inclusive index of the subarray that are searched, whose minimum value is 0

$i_{\mathrm{u}}$: highest inclusive index of the subarray that are searched, whose maximum value is $l$

$R$: a random number uniformly generated from $[0, 1)$

**Output:**

$i$: index of row which satisfies the condition $F_{\mathrm{i\text{-}1}} \leq R < F_{\mathrm{i}}$

**procedure** PSEUDOF($\{F\}, i_{\mathrm{l}}, i_{\mathrm{u}}, R$)
  **if** $i_{\mathrm{l}} > i_{\mathrm{u}}$ **then**
    $i \leftarrow -1$
  **else**
    $i_{\mathrm{mid}} \leftarrow i_{\mathrm{l}} + i_{\mathrm{u}}$ ▷ find the middle index
    **if** $i_{\mathrm{mid}} = 0$ **then**
      preProb $\leftarrow 0$ ▷ record the previous probability
    **else**
      preProb $\leftarrow F_{i_{\mathrm{mid}}-1}$
      **if** preProb $\leq R < F_{i_{\mathrm{mid}}}$ **then**
        $i \leftarrow i_{\mathrm{mid}}$
      **else** ▷ recursive call of the function itself to find the index
        **if** $R < F_{i_{\mathrm{mid}}-1}$ **then**
          $i \leftarrow$ pseudoF($\{F\}, i_{\mathrm{l}}, i_{\mathrm{mid}} - 1, R$)
        **else**
          $i \leftarrow$ pseudoF($\{F\}, i_{\mathrm{mid}} + 1, i_{\mathrm{u}}, R$)
        **end if**
      **end if**
    **end if**
  **end if**
  **return** $i$.
**end procedure**

## B.2 Main algorithm of sampling method

We now introduce the detailed algorithm of applying our sampling method to calculate visibilities for $N \leq 6$ swaps. Notice that for simulations of $N \leq 6$ swaps we only need

two prior lists, as introduced in Chapter. 5. We now provide the inputs, outputs and pseudo-codes of our sampling method in Algorithm 2.

**Algorithm 2** Main algorithm of sampling method

**Input:**

$N$: the number of swaps we are simulating

$\{\chi\}$: the nonlinearities of all the PDC sources

$\{\eta_{\mathrm{e}}\}$: the "effective efficiencies" of all the detectors

$\alpha$: the polarization angle of Alice's polarization rotators

$\delta$: the polarization angle of Bob's polarization rotators

$n_{\max}$: the photon-number truncation in every mode

$P_1$: first prior list

$P_2$: second prior list

$L_1$: length of the first prior list

$L_2$: length of the second prior list

$n_1$: the total number of combinations picked from the first prior list, with its maximum value to be $L_1$

$n_2$: the total number of combinations picked from the second prior list, with its maximum value to be $L_2$

pseudoF$(\{F\}, i_{\mathrm{l}}, i_{\mathrm{u}}, R)$: algorithm of pseudo-random number sampling

**Output:**

$V$: simulated visibility of $N$ swaps based on the parameters we enter

**procedure** MAIN($N$, $\{\chi\}$, $\{\eta_{\mathrm{e}}\}$, $\alpha$, $\delta$, $n_{\max}$, $P_1$, $P_2$, $L_1$, $L_2$, $n_1$, $n_2$, pseudoF)
  **for** $i \leftarrow 1, n_1$ **do**
    $R_1 \leftarrow [0, 1)$ ▷ generate a random number
    $m \leftarrow \mathrm{pseudoF}(P_1, 0, L_1 - 1, R_1)$ ▷ apply pseudo-random number sampling to find the index of row from the first prior list
    $(\boldsymbol{ijkl}^{(m)}) \leftarrow (P_1)_m$ ▷ use the combination located at the $m$th row of the first prior list to set the first part of $(\boldsymbol{ijkl}^{(m)})$
    **for** $j \leftarrow 1, n_2$ **do**
      $(\boldsymbol{ijkl}^{(m)}) \leftarrow (P_2)_j$ ▷ use the combination located at the $j$th row of the second prior list to set the second part of $(\boldsymbol{ijkl}^{(m)})$
      $Q_{1010}^{\mathbf{1010}} \mathrel{+}= Q_{1010}^{\mathbf{1010},\mathrm{block}(m)}(\{\chi\},\{\eta_{\mathrm{e}}\},\alpha,\delta,n_{\max},(\boldsymbol{ijkl}^{(m)}))$
      $Q_{0101}^{\mathbf{1010}} \mathrel{+}= Q_{0101}^{\mathbf{1010},\mathrm{block}(m)}(\{\chi\},\{\eta_{\mathrm{e}}\},\alpha,\delta,n_{\max},(\boldsymbol{ijkl}^{(m)}))$
      $Q_{1001}^{\mathbf{1010}} \mathrel{+}= Q_{1001}^{\mathbf{1010},\mathrm{block}(m)}(\{\chi\},\{\eta_{\mathrm{e}}\},\alpha,\delta,n_{\max},(\boldsymbol{ijkl}^{(m)}))$
      $Q_{0110}^{\mathbf{1010}} \mathrel{+}= Q_{0110}^{\mathbf{1010},\mathrm{block}(m)}(\{\chi\},\{\eta_{\mathrm{e}}\},\alpha,\delta,n_{\max},(\boldsymbol{ijkl}^{(m)}))$
    **end for**
  **end for**
  $V \leftarrow$ Eq. (2.1) ▷ calculate the visibility
  **return** $V$
**end procedure**

Up to now we have introduced all the significant algorithms of our sampling method.

# Appendix C

# Theory of LDQC through any number of entanglement-swapping operations in a quantum-relay configuration using single-photon sources

In this appendix we show the details of how we develop the theory of LDQC through any number of entanglement-swapping operations in a quantum-relay configuration using single-photon sources.

We know the unnormalized joined state coming out of the two single-photon sources is the tensor product of each individual state, i.e.,

$$\begin{aligned} |\psi\rangle = |\psi_{\mathrm{ab}}\rangle \otimes |\psi_{\mathrm{cd}}\rangle &= \frac{1}{2}\left(\hat{a}_{\mathrm{H}}^{\dagger}\hat{b}_{\mathrm{V}}^{\dagger} - \hat{a}_{\mathrm{V}}^{\dagger}\hat{b}_{\mathrm{H}}^{\dagger}\right)\left(\hat{c}_{\mathrm{H}}^{\dagger}\hat{d}_{\mathrm{V}}^{\dagger} - \hat{c}_{\mathrm{V}}^{\dagger}\hat{d}_{\mathrm{H}}^{\dagger}\right)|\mathrm{vac}\rangle \\ &= \frac{1}{2}\left(\hat{a}_{\mathrm{H}}^{\dagger}\hat{b}_{\mathrm{V}}^{\dagger}\hat{c}_{\mathrm{H}}^{\dagger}\hat{d}_{\mathrm{V}}^{\dagger} - \hat{a}_{\mathrm{H}}^{\dagger}\hat{b}_{\mathrm{V}}^{\dagger}\hat{c}_{\mathrm{V}}^{\dagger}\hat{d}_{\mathrm{H}}^{\dagger} - \hat{a}_{\mathrm{V}}^{\dagger}\hat{b}_{\mathrm{H}}^{\dagger}\hat{c}_{\mathrm{H}}^{\dagger}\hat{d}_{\mathrm{V}}^{\dagger} + \hat{a}_{\mathrm{V}}^{\dagger}\hat{b}_{\mathrm{H}}^{\dagger}\hat{c}_{\mathrm{V}}^{\dagger}\hat{d}_{\mathrm{H}}^{\dagger}\right)|\mathrm{vac}\rangle\,. \end{aligned} \tag{C.1}$$

After passing through the beamsplitter, the unnormalized state becomes

$$\begin{aligned}\hat{U}_{\mathrm{B}}\left|\psi\right\rangle =&\frac{1}{4}\Big[\hat{a}_{\mathrm{H}}^{\dagger}\hat{b}_{\mathrm{V}}^{\dagger\prime}\hat{b}_{\mathrm{H}}^{\dagger\prime}\hat{d}_{\mathrm{V}}^{\dagger}+\hat{a}_{\mathrm{H}}^{\dagger}\hat{b}_{\mathrm{V}}^{\dagger\prime}\hat{c}_{\mathrm{H}}^{\dagger\prime}\hat{d}_{\mathrm{V}}^{\dagger}-\hat{a}_{\mathrm{H}}^{\dagger}\hat{c}_{\mathrm{V}}^{\dagger\prime}\hat{b}_{\mathrm{H}}^{\dagger\prime}\hat{d}_{\mathrm{V}}^{\dagger}-\hat{a}_{\mathrm{H}}^{\dagger}\hat{c}_{\mathrm{V}}^{\dagger\prime}\hat{c}_{\mathrm{H}}^{\dagger\prime}\hat{d}_{\mathrm{V}}^{\dagger}\\&-\hat{a}_{\mathrm{H}}^{\dagger}\hat{b}_{\mathrm{V}}^{\dagger\prime}\hat{b}_{\mathrm{V}}^{\dagger\prime}\hat{d}_{\mathrm{H}}^{\dagger}-\hat{a}_{\mathrm{H}}^{\dagger}\hat{b}_{\mathrm{V}}^{\dagger\prime}\hat{c}_{\mathrm{V}}^{\dagger\prime}\hat{d}_{\mathrm{H}}^{\dagger}+\hat{a}_{\mathrm{H}}^{\dagger}\hat{c}_{\mathrm{V}}^{\dagger\prime}\hat{b}_{\mathrm{V}}^{\dagger\prime}\hat{d}_{\mathrm{H}}^{\dagger}+\hat{a}_{\mathrm{H}}^{\dagger}\hat{c}_{\mathrm{V}}^{\dagger\prime}\hat{c}_{\mathrm{V}}^{\dagger\prime}\hat{d}_{\mathrm{H}}^{\dagger}\\&-\hat{a}_{\mathrm{V}}^{\dagger}\hat{b}_{\mathrm{H}}^{\dagger\prime}\hat{b}_{\mathrm{H}}^{\dagger\prime}\hat{d}_{\mathrm{V}}^{\dagger}-\hat{a}_{\mathrm{V}}^{\dagger}\hat{b}_{\mathrm{H}}^{\dagger\prime}\hat{c}_{\mathrm{H}}^{\dagger\prime}\hat{d}_{\mathrm{V}}^{\dagger}+\hat{a}_{\mathrm{V}}^{\dagger}\hat{c}_{\mathrm{H}}^{\dagger\prime}\hat{b}_{\mathrm{H}}^{\dagger\prime}\hat{d}_{\mathrm{V}}^{\dagger}+\hat{a}_{\mathrm{V}}^{\dagger}\hat{c}_{\mathrm{H}}^{\dagger\prime}\hat{c}_{\mathrm{H}}^{\dagger\prime}\hat{d}_{\mathrm{V}}^{\dagger}\\&+\hat{a}_{\mathrm{V}}^{\dagger}\hat{b}_{\mathrm{H}}^{\dagger\prime}\hat{b}_{\mathrm{V}}^{\dagger\prime}\hat{d}_{\mathrm{H}}^{\dagger}+\hat{a}_{\mathrm{V}}^{\dagger}\hat{b}_{\mathrm{H}}^{\dagger\prime}\hat{c}_{\mathrm{V}}^{\dagger\prime}\hat{d}_{\mathrm{H}}^{\dagger}-\hat{a}_{\mathrm{V}}^{\dagger}\hat{c}_{\mathrm{H}}^{\dagger\prime}\hat{b}_{\mathrm{V}}^{\dagger\prime}\hat{d}_{\mathrm{H}}^{\dagger}-\hat{a}_{\mathrm{V}}^{\dagger}\hat{c}_{\mathrm{H}}^{\dagger\prime}\hat{c}_{\mathrm{V}}^{\dagger\prime}\hat{d}_{\mathrm{H}}^{\dagger}\Big]\left|\mathrm{vac}\right\rangle .\end{aligned} \tag{C.2}$$

The two PBSs will then reflect the vertical polarization and transit the horizontal polarization. After that the detectors will perform measurements. The post-measurement unnormalized state will then be

$$\begin{aligned}\hat{\Pi}\hat{U}_{\mathrm{B}}\left|\psi\right\rangle =&\frac{1}{4}\Big(\hat{a}_{\mathrm{H}}^{\dagger}\hat{d}_{\mathrm{V}}^{\dagger}\delta_{i0}\delta_{j0}\delta_{k1}\delta_{l1}+\hat{a}_{\mathrm{H}}^{\dagger}\hat{d}_{\mathrm{V}}^{\dagger}\delta_{i1}\delta_{j0}\delta_{k1}\delta_{l0}-\hat{a}_{\mathrm{H}}^{\dagger}\hat{d}_{\mathrm{V}}^{\dagger}\delta_{i0}\delta_{j1}\delta_{k0}\delta_{l1}-\hat{a}_{\mathrm{H}}^{\dagger}\hat{d}_{\mathrm{V}}^{\dagger}\delta_{i1}\delta_{j1}\delta_{k0}\delta_{l0}\\&-\hat{a}_{\mathrm{H}}^{\dagger}\hat{d}_{\mathrm{H}}^{\dagger}\delta_{i0}\delta_{j0}\delta_{k2}\delta_{l0}-\hat{a}_{\mathrm{H}}^{\dagger}\hat{d}_{\mathrm{H}}^{\dagger}\delta_{i0}\delta_{j1}\delta_{k1}\delta_{l0}+\hat{a}_{\mathrm{H}}^{\dagger}\hat{d}_{\mathrm{H}}^{\dagger}\delta_{i0}\delta_{j1}\delta_{k1}\delta_{l0}+\hat{a}_{\mathrm{H}}^{\dagger}\hat{d}_{\mathrm{H}}^{\dagger}\delta_{i0}\delta_{j2}\delta_{k0}\delta_{l0}\\&-\hat{a}_{\mathrm{V}}^{\dagger}\hat{d}_{\mathrm{V}}^{\dagger}\delta_{i0}\delta_{j0}\delta_{k0}\delta_{l2}-\hat{a}_{\mathrm{V}}^{\dagger}\hat{d}_{\mathrm{V}}^{\dagger}\delta_{i1}\delta_{j0}\delta_{k0}\delta_{l1}+\hat{a}_{\mathrm{V}}^{\dagger}\hat{d}_{\mathrm{V}}^{\dagger}\delta_{i1}\delta_{j0}\delta_{k0}\delta_{l1}+\hat{a}_{\mathrm{V}}^{\dagger}\hat{d}_{\mathrm{V}}^{\dagger}\delta_{i2}\delta_{j0}\delta_{k0}\delta_{l0}\\&+\hat{a}_{\mathrm{V}}^{\dagger}\hat{d}_{\mathrm{H}}^{\dagger}\delta_{i0}\delta_{j0}\delta_{k1}\delta_{l1}+\hat{a}_{\mathrm{V}}^{\dagger}\hat{d}_{\mathrm{H}}^{\dagger}\delta_{i0}\delta_{j1}\delta_{k0}\delta_{l1}-\hat{a}_{\mathrm{V}}^{\dagger}\hat{d}_{\mathrm{H}}^{\dagger}\delta_{i1}\delta_{j0}\delta_{k1}\delta_{l0}-\hat{a}_{\mathrm{V}}^{\dagger}\hat{d}_{\mathrm{H}}^{\dagger}\delta_{i1}\delta_{j1}\delta_{k0}\delta_{l0}\Big)\\&\otimes\left|\mathrm{vac}\right\rangle .\end{aligned} \tag{C.3}$$

We normalize the state in Eq. (C.3) and simplify it to be

$$\left|\Phi\right\rangle =\frac{1}{\sqrt{2}}\left[C_1\hat{a}_{\mathrm{H}}^{\dagger}\hat{d}_{\mathrm{V}}^{\dagger}+C_2\hat{a}_{\mathrm{H}}^{\dagger}\hat{d}_{\mathrm{H}}^{\dagger}+C_3\hat{a}_{\mathrm{V}}^{\dagger}\hat{d}_{\mathrm{V}}^{\dagger}+C_4\hat{a}_{\mathrm{V}}^{\dagger}\hat{d}_{\mathrm{H}}^{\dagger}\right]\left|\mathrm{vac}\right\rangle , \tag{C.4}$$

where the coefficients are defined as

$$\begin{aligned}C_1&=\delta_{i0}\delta_{j0}\delta_{k1}\delta_{l1}+\delta_{i1}\delta_{j0}\delta_{k1}\delta_{l0}-\delta_{i0}\delta_{j1}\delta_{k0}\delta_{l1}-\delta_{i1}\delta_{j1}\delta_{k0}\delta_{l0},\\C_2&=\delta_{i0}\delta_{j2}\delta_{k0}\delta_{l0}-\delta_{i0}\delta_{j0}\delta_{k2}\delta_{l0},\\C_3&=\delta_{i2}\delta_{j0}\delta_{k0}\delta_{l0}-\delta_{i0}\delta_{j0}\delta_{k0}\delta_{l2},\\C_4&=\delta_{i0}\delta_{j0}\delta_{k1}\delta_{l1}+\delta_{i0}\delta_{j1}\delta_{k0}\delta_{l1}-\delta_{i1}\delta_{j0}\delta_{k1}\delta_{l0}-\delta_{i1}\delta_{j1}\delta_{k0}\delta_{l0}.\end{aligned} \tag{C.5}$$

Here $\delta_{ab}$ means that if $a=b$ then it is 1, otherwise it is 0.

Eq. (C.4) is the normalized state for each single-swap element after PSO. The resultant state of $N$ swaps after all the intermediate PSO measurements is obtained by applying intermediate measurements projectors on the tensor product of $N$ individual states of single-swap elements. We find it to be

$$\left|\Phi\right\rangle_N =\frac{1}{\sqrt{2}}\left[C_{\mathrm{swap}N,1}\hat{a}_{1\mathrm{H}}^{\dagger}\hat{d}_{N\mathrm{V}}^{\dagger}+C_{\mathrm{swap}N,2}\hat{a}_{1\mathrm{H}}^{\dagger}\hat{d}_{N\mathrm{H}}^{\dagger}+C_{\mathrm{swap}N,3}\hat{a}_{1\mathrm{V}}^{\dagger}\hat{d}_{N\mathrm{V}}^{\dagger}+C_{\mathrm{swap}N,4}\hat{a}_{1\mathrm{V}}^{\dagger}\hat{d}_{N\mathrm{H}}^{\dagger}\right]\left|\mathrm{vac}\right\rangle , \tag{C.6}$$

where $\hat{a}^{\dagger}_{1\mathrm{H}}$ and $\hat{a}^{\dagger}_{1\mathrm{V}}$ are the creation operators on the horizontal and vertical components of spatial mode in the arm towards Alice. $\hat{d}^{\dagger}_{N\mathrm{H}}$ and $\hat{d}^{\dagger}_{N\mathrm{V}}$ are the creation operators on the horizontal and vertical components of spatial mode in the arm towards Bob. The coefficients $C_{\mathrm{swap}N,1}$ $C_{\mathrm{swap}N,2}$ $C_{\mathrm{swap}N,3}$ $C_{\mathrm{swap}N,4}$ can be calculated through the recursive algorithm, started from $M = 2$ to $M = N$:

$$\begin{aligned}
C_{\mathrm{swap}M,1} &= C_{\mathrm{swap}(M-1),1}C_{M1}C_{(M+(M-1))1} - C_{\mathrm{swap}(M-1),1}C_{M3}C_{(M+(M-1))2} \\
&\quad - C_{\mathrm{swap}(M-1),2}C_{M1}C_{(M+(M-1))3} + C_{\mathrm{swap}(M-1),2}C_{M3}C_{(M+(M-1))4}, \\
C_{\mathrm{swap}M,2} &= C_{\mathrm{swap}(M-1),1}C_{M2}C_{(M+(M-1))1} - C_{\mathrm{swap}(M-1),1}C_{M4}C_{(M+(M-1))2} \\
&\quad - C_{\mathrm{swap}(M-1),2}C_{M2}C_{(M+(M-1))3} + C_{\mathrm{swap}(M-1),2}C_{M4}C_{(M+(M-1))4}, \\
C_{\mathrm{swap}M,3} &= C_{\mathrm{swap}(M-1),3}C_{M1}C_{(M+(M-1))1} - C_{\mathrm{swap}(M-1),3}C_{M3}C_{(M+(M-1))2} \\
&\quad - C_{\mathrm{swap}(M-1),4}C_{M1}C_{(M+(M-1))3} + C_{\mathrm{swap}(M-1),4}C_{M3}C_{(M+(M-1))4}, \\
C_{\mathrm{swap}M,4} &= C_{\mathrm{swap}(M-1),3}C_{M2}C_{(M+(M-1))1} - C_{\mathrm{swap}(M-1),3}C_{M4}C_{(M+(M-1))2} \\
&\quad - C_{\mathrm{swap}(M-1),4}C_{M2}C_{(M+(M-1))3} + C_{\mathrm{swap}(M-1),4}C_{M4}C_{(M+(M-1))4}.
\end{aligned} \tag{C.7}$$

Here the coefficients $C_{M1}$, $C_{M2}$, $C_{M3}$, $C_{M4}$ are defined as

$$\begin{aligned}
C_{M1} &= \delta_{i_M0}\delta_{j_M0}\delta_{k_M1}\delta_{l_M1} + \delta_{i_M1}\delta_{j_M0}\delta_{k_M1}\delta_{l_M0} - \delta_{i_M0}\delta_{j_M1}\delta_{k_M0}\delta_{l_M1} - \delta_{i_M1}\delta_{j_M1}\delta_{k_M0}\delta_{l_M0}, \\
C_{M2} &= \delta_{i_M0}\delta_{j_M2}\delta_{k_M0}\delta_{l_M0} - \delta_{i_M0}\delta_{j_M0}\delta_{k_M2}\delta_{l_M0}, \\
C_{M3} &= \delta_{i_M2}\delta_{j_M0}\delta_{k_M0}\delta_{l_M0} - \delta_{i_M0}\delta_{j_M0}\delta_{k_M0}\delta_{l_M2}, \\
C_{M4} &= \delta_{i_M0}\delta_{j_M0}\delta_{k_M1}\delta_{l_M1} + \delta_{i_M0}\delta_{j_M1}\delta_{k_M0}\delta_{l_M1} - \delta_{i_M1}\delta_{j_M0}\delta_{k_M1}\delta_{l_M0} - \delta_{i_M1}\delta_{j_M1}\delta_{k_M0}\delta_{l_M0}
\end{aligned} \tag{C.8}$$

and $C_{\mathrm{swap}2,1}$, $C_{\mathrm{swap}2,2}$, $C_{\mathrm{swap}2,3}$, $C_{\mathrm{swap}2,4}$ are defined as

$$\begin{aligned}
C_{\mathrm{swap}2,1} &= C_{11}C_{21}C_{31} - C_{11}C_{23}C_{32} - C_{12}C_{21}C_{33} + C_{12}C_{23}C_{34}, \\
C_{\mathrm{swap}2,2} &= C_{11}C_{22}C_{31} - C_{11}C_{24}C_{32} - C_{12}C_{22}C_{33} + C_{12}C_{24}C_{34}, \\
C_{\mathrm{swap}2,3} &= C_{13}C_{21}C_{31} - C_{13}C_{23}C_{32} - C_{14}C_{21}C_{33} + C_{14}C_{23}C_{34}, \\
C_{\mathrm{swap}2,4} &= C_{13}C_{22}C_{31} - C_{13}C_{24}C_{32} - C_{14}C_{22}C_{33} + C_{14}C_{24}C_{34}.
\end{aligned} \tag{C.9}$$

Now we apply unit operations of the rotators to the state in Eq. (C.6). The unit operations of the rotators can be mathematically written as [9]

$$\begin{aligned}
\hat{U}_{\hat{a}}(\tilde{\alpha}) = \sum_{n_1=0}^{\infty}\sum_{n_2=0}^{\infty} &\frac{i^{n_1}\left[\tan\left(\frac{\tilde{\alpha}}{2}\right)\right]^{n_1}\left(\hat{a}^{\dagger}_{1\mathrm{V}}\right)^{n_1}(\hat{a}_{1\mathrm{H}})^{n_1}}{n_1!} \\
&\times\left[\cos\left(\frac{\tilde{\alpha}}{2}\right)\right]^{\hat{a}^{\dagger}_{1\mathrm{H}}\hat{a}_{1\mathrm{H}}-\hat{a}^{\dagger}_{1\mathrm{V}}\hat{a}_{1\mathrm{V}}}\frac{i^{n_2}\left[\tan\left(\frac{\tilde{\alpha}}{2}\right)\right]^{n_2}(\hat{a}_{1\mathrm{V}})^{n_2}\left(\hat{a}^{\dagger}_{1\mathrm{H}}\right)^{n_2}}{n_2!}.
\end{aligned} \tag{C.10}$$

$$\hat{U}_{\hat{d}}(\tilde{\delta}) = \sum_{n_3=0}^{\infty}\sum_{n_4=0}^{\infty} \frac{i^{n_3}\left[\tan\left(\frac{\tilde{\delta}}{2}\right)\right]^{n_3}\left(\hat{d}^{\dagger}_{N\mathrm{V}}\right)^{n_3}\left(\hat{d}_{N\mathrm{H}}\right)^{n_3}}{n_3!} \times \left[\cos\left(\frac{\tilde{\delta}}{2}\right)\right]^{\hat{d}^{\dagger}_{N\mathrm{H}}\hat{d}_{N\mathrm{H}}-\hat{d}^{\dagger}_{N\mathrm{V}}\hat{d}_{N\mathrm{V}}} \frac{i^{n_4}\left[\tan\left(\frac{\tilde{\delta}}{2}\right)\right]^{n_4}\left(\hat{d}_{N\mathrm{V}}\right)^{n_4}\left(\hat{d}^{\dagger}_{N\mathrm{H}}\right)^{n_4}}{n_4!}. \tag{C.11}$$

The state of the $N$ swaps after passing through the rotators is then found to be

$$\begin{aligned}
\hat{U}_{\hat{a}}(\tilde{\alpha})\otimes\hat{U}_{\hat{d}}(\tilde{\delta})\left|\Phi\right\rangle_N = &\sum_{n_1=0}^{1}\sum_{n_2=0}^{1}\sum_{n_3=0}^{1}\sum_{n_4=0}^{1}\frac{1}{\sqrt{2}}\frac{i^{n_1+n_2+n_3+n_4}\left[\tan\left(\frac{\tilde{\alpha}}{2}\right)\right]^{n_1+n_2}\left[\tan\left(\frac{\tilde{\delta}}{2}\right)\right]^{n_3+n_4}}{n_1!n_2!n_3!n_4!}\\
\times\Bigg[&C_{\mathrm{swap}N,1}\left[\cos\left(\frac{\tilde{\alpha}}{2}\right)\right]\left[\cos\left(\frac{\tilde{\delta}}{2}\right)\right]^{2n_4-1}\delta_{n_3\le n_4}\delta_{n_2=0}\left|1-n_1,n_1,1+n_3-n_4,n_4-n_3\right\rangle\\
&+C_{\mathrm{swap}N,2}\left[\cos\left(\frac{\tilde{\alpha}}{2}\right)\right]\left[\cos\left(\frac{\tilde{\delta}}{2}\right)\right]\delta_{n_4=0}\delta_{n_2=0}\left|1-n_1,n_1,n_3,1-n_3\right\rangle\\
&+C_{\mathrm{swap}N,3}\left[\cos\left(\frac{\tilde{\alpha}}{2}\right)\right]^{2n_2-1}\left[\cos\left(\frac{\tilde{\delta}}{2}\right)\right]^{2n_4-1}\delta_{n_3\le n_4}\delta_{n_1\le n_2}\left|n_2-n_1,1+n_1-n_2,1+n_3-n_4,n_4-n_3\right\rangle\\
&+C_{\mathrm{swap}N,4}\left[\cos\left(\frac{\tilde{\alpha}}{2}\right)\right]^{2n_2-1}\left[\cos\left(\frac{\tilde{\delta}}{2}\right)\right]\delta_{n_4=0}\delta_{n_1\le n_2}\left|n_2-n_1,1+n_1-n_2,n_3,1-n_3\right\rangle\Bigg],
\end{aligned} \tag{C.12}$$

where $\delta_{a\le b}$ means that if $a \le b$ then it is 1, otherwise it is 0. Here we remain our convention of notation of Fock state $|a_{\mathrm{H}}, a_{\mathrm{V}}, d_{\mathrm{V}}, d_{\mathrm{H}}\rangle$.

The new $A^{ijkl}_{i'j'k'l'}$ is obtained by appling measurements projectors on the above state, which is found to be

$$
\begin{aligned}
&A^{ijkl}_{i'j'k'l'} = \left\langle i'j'k'l' \right| \hat{U}_{\hat{a}}(\tilde{\alpha}) \otimes \hat{U}_{\hat{d}}(\tilde{\delta}) \left| \Phi \right\rangle_N \\
&= \sum_{n_1=0}^{1}\sum_{n_2=0}^{1}\sum_{n_3=0}^{1}\sum_{n_4=0}^{1} \frac{1}{\sqrt{2}} \frac{i^{n_1+n_2+n_3+n_4}\left[\tan\left(\frac{\tilde{\alpha}}{2}\right)\right]^{n_1+n_2}\left[\tan\left(\frac{\tilde{\delta}}{2}\right)\right]^{n_3+n_4}}{n_1!n_2!n_3!n_4!} \\
&\times \Bigg[ C_{\mathrm{swap}N,1}\left[\cos\left(\frac{\tilde{\alpha}}{2}\right)\right]\left[\cos\left(\frac{\tilde{\delta}}{2}\right)\right]^{2n_4-1} \delta_{n_3\le n_4}\delta_{n_2=0}\delta_{i'=1-n_1}\delta_{j'=n_1}\delta_{k'=1+n_3-n_4}\delta_{l'=n_4-n_3} \\
&+ C_{\mathrm{swap}N,2}\left[\cos\left(\frac{\tilde{\alpha}}{2}\right)\right]\left[\cos\left(\frac{\tilde{\delta}}{2}\right)\right] \delta_{n_4=0}\delta_{n_2=0}\delta_{i'=1-n_1}\delta_{j'=n_1}\delta_{k'=n_3}\delta_{l'=1-n_3} \\
&+ C_{\mathrm{swap}N,3}\left[\cos\left(\frac{\tilde{\alpha}}{2}\right)\right]^{2n_2-1}\left[\cos\left(\frac{\tilde{\delta}}{2}\right)\right]^{2n_4-1} \delta_{n_3\le n_4}\delta_{n_1\le n_2}\delta_{i'=n_2-n_1}\delta_{j'=1+n_1-n_2}\delta_{k'=1+n_3-n_4}\delta_{l'=n_4-n_3} \\
&+ C_{\mathrm{swap}N,4}\left[\cos\left(\frac{\tilde{\alpha}}{2}\right)\right]^{2n_2-1}\left[\cos\left(\frac{\tilde{\delta}}{2}\right)\right] \delta_{n_4=0}\delta_{n_1\le n_2}\delta_{i'=n_2-n_1}\delta_{j'=1+n_1-n_2}\delta_{k'=n_3}\delta_{l'=1-n_3} \Bigg].
\end{aligned}
\tag{C.13}
$$

Here $\delta_{a=b}$ means that if $a = b$ then it is 1, otherwise it is 0. $\delta_{a\le b}$ means that if $a \le b$ then it is 1, otherwise it is 0.

The $p(q'r's't'|i'j'k'l')$ and $P^{\boldsymbol{qrst}}_{\boldsymbol{ijkl}}$ functions are the same as those in PDC source case [11] as we do not change the detectors. Finally, we calculate the conditional probabilities $Q^{\boldsymbol{qrst}}_{q'r's't'}$ through Eq. (2.2) and corresponding visibility based on them through Eq. (2.1).

# Bibliography


[1] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74:145–195, Mar 2002. doi: 10.1103/RevModPhys.74.145. URL http://link.aps.org/doi/10.1103/RevModPhys.74.145.

[2] Edo Waks, Assaf Zeevi, and Yoshihisa Yamamoto. Security of quantum key distribution with entangled photons against individual attacks. *Phys. Rev. A*, 65:052310, Apr 2002. doi: 10.1103/PhysRevA.65.052310. URL http://link.aps.org/doi/10.1103/PhysRevA.65.052310.

[3] B. C. Jacobs, T. B. Pittman, and J. D. Franson. Quantum relays and noise suppression using linear optics. *Phys. Rev. A*, 66:052307, Nov 2002. doi: 10.1103/PhysRevA.66.052307. URL http://link.aps.org/doi/10.1103/PhysRevA.66.052307.

[4] H. de Riedmatten, I. Marcikic, W. Tittel, H. Zbinden, D. Collins, and N. Gisin. Long distance quantum teleportation in a quantum relay configuration. *Phys. Rev. Lett.*, 92:047904, Jan 2004. doi: 10.1103/PhysRevLett.92.047904. URL http://link.aps.org/doi/10.1103/PhysRevLett.92.047904.

[5] Daniel Collins, Nicolas Gisin, and Hugues De Riedmatten. Quantum relays for long distance quantum cryptography. *J. Mod. Opt.*, 52(5):735–753, 2005. doi: 10.1080/09500340412331283633. URL http://dx.doi.org/10.1080/09500340412331283633.

[6] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.*, 81:5932–5935, Dec 1998. doi: 10.1103/PhysRevLett.81.5932. URL http://link.aps.org/doi/10.1103/PhysRevLett.81.5932.

[7] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller. Long-distance quantum communication with atomic ensembles and linear optics. *Nature*, 414:413–418, Nov 2001. doi: 10.1038/35106500. URL http://dx.doi.org/10.1038/35106500.

[8] Alexander I. Lvovsky, Barry C. Sanders, and Wolfgang Tittel. Optical quantum memory. *Nature Photon.*, 3:706–714, Dec 2009. doi: 10.1038/nphoton.2009.231. URL http://dx.doi.org/10.1038/nphoton.2009.231.

[9] Artur Scherer, Regina B. Howard, Barry C. Sanders, and Wolfgang Tittel. Quantum states prepared by realistic entanglement swapping. *Phys. Rev. A*, 80:062310, Dec 2009. doi: 10.1103/PhysRevA.80.062310. URL http://link.aps.org/doi/10.1103/PhysRevA.80.062310.

[10] Aeysha Khalique, Wolfgang Tittel, and Barry C. Sanders. Practical long-distance quantum communication using concatenated entanglement swapping. *Phys. Rev. A*, 88:022336, Aug 2013. doi: 10.1103/PhysRevA.88.022336. URL http://link.aps.org/doi/10.1103/PhysRevA.88.022336.

[11] Aeysha Khalique and Barry C. Sanders. Long-distance quantum communication through any number of entanglement-swapping operations. *Phys. Rev. A*, 90: 032304, Sep 2014. doi: 10.1103/PhysRevA.90.032304. URL http://link.aps.org/doi/10.1103/PhysRevA.90.032304.

[12] H. de Riedmatten, I. Marcikic, J. A. W. van Houwelingen, W. Tittel, H. Zbinden, and N. Gisin. Long-distance entanglement swapping with photons from separated sources. *Phys. Rev. A*, 71:050302, May 2005. doi: 10.1103/PhysRevA.71.050302. URL http://link.aps.org/doi/10.1103/PhysRevA.71.050302.

[13] Jian-Wei Pan, Dik Bouwmeester, Harald Weinfurter, and Anton Zeilinger. Experimental entanglement swapping: Entangling photons that never interacted. *Phys. Rev. Lett.*, 80:3891–3894, May 1998. doi: 10.1103/PhysRevLett.80.3891. URL http://link.aps.org/doi/10.1103/PhysRevLett.80.3891.

[14] Thomas Jennewein, Gregor Weihs, Jian-Wei Pan, and Anton Zeilinger. Experimental nonlocality proof of quantum teleportation and entanglement swapping. *Phys. Rev. Lett.*, 88:017903, Dec 2001. doi: 10.1103/PhysRevLett.88.017903. URL http://link.aps.org/doi/10.1103/PhysRevLett.88.017903.

[15] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T.Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam. Detecting single infrared photons with 93 *Nature Photon.*, 7:210–214, Mar 2013. doi: 10.1038/nphoton.2013.13. URL http://dx.doi.org/10.1038/nphoton.2013.13.

[16] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, Oct 1969. doi: 10.1103/PhysRevLett.23.880. URL http://link.aps.org/doi/10.1103/PhysRevLett.23.880.

[17] Asher Peres. Separability criterion for density matrices. *Phys. Rev. Lett.*, 77:1413–1415, Aug 1996. doi: 10.1103/PhysRevLett.77.1413. URL http://link.aps.org/doi/10.1103/PhysRevLett.77.1413.

[18] Aeysha Khalique and Barry C. Sanders. Practical long-distance quantum key distribution through concatenated entanglement swapping with parametric down-conversion sources. Jan 2015. URL http://arxiv.org/abs/1501.03317.