Randomness Extraction from Detection Loophole-Free Bell Violation with Continuous Parametric Down-Conversion

Shen Lijiong

Department of Physics & Centre for Quantum Technologies
National University of Singapore

This dissertation is submitted for the degree of
Doctor of Philosophy

Supervisor:
Professor Christian Kurtsiefer

Examiners:
Professor Lai Choy Heng
Dr Mukherjee, Manas
Dr Benson Oliver, Humboldt University Berlin

April 2019

Declaration

I hereby declare that the thesis is my original work and it has been written by me in its entirety. I have duly acknowledged all the sources of information which have been used in the thesis.

The thesis has also not been submitted for any degree in any university previously.

Shen Lijiong

Shen Lijiong
April 2019

Acknowledgements

First and foremost, I would like to thank my supervisor, Prof. Christian Kurtsiefer, who guides me for the entire journey of Ph.D. He is always patient and helpful when I feel difficult to move on.

Next, I would like to thank my lab partner Jianwei Lee. He is like a big brother to me. Four years ago, when I open the door of the lab, I almost knew nothing about quantum optics. He always earnestly answer my question no matter how stupid and how basic it is. We encouraged each other when we encountered problems and shared all the happiness with good results.

Special thanks to Dr. Alessandro Cerè who is the Postdoc oversee the project and the mentor to me. He has been of great help, not only in the experiment but in proofreading my writing, code, and presentation.

Adrian Nugraha Utama, office mate and the smartest friend ever, is always ready to help for others. Chi Huan Nguyen proofread this thesis for almost every chapter. Brenda Chng perpetually organizes the lab and advices both the experiment and life. Janet Lim was the one who made the offices of quantum optics full of laughter.

Thanks also to all the other group members or former group members for their suggestions to this projects including: Tan Peng Kian, Shi YiCheng, Mathias Seidler, Yeo Xi Jie, Wilson Chin Yue Sum, Matthias Steiner, Victor Leong, Antia Lamas-Linares, Gurpreet Kaur Gulati, Nick Lewty, Ng Boon Long, Chow Chang Hoong, Hou Shun Poh, Siddarth Joshi.

Thanks also go to Prof. Valerio Scarani and Asst Prof. José Carlos VIANA-GOMES. They consist the thesis advisory committee for my Ph.D. Prof. Valerio, Dr. LE Phuc Thinh, and Dr. Jean-Daniel BANCAL also made huge contribution to the theoretic part of this work.

Abstract

Quantum entanglement provides sources of randomness that can be certified as being uncorrelated with any outside process or variable. Certified private randomness can be extracted by a system that shows a violation of a Bell inequality. The randomness extraction rate depends on the observed violation and on the repetition rate of the Bell test. Photonic systems generally show a small violation, but thanks to their high repetition rate it is possible to obtain a high randomness generation rate.

In this thesis, polarization-entangled photon pairs generated by spontaneous parametric down conversion (SPDC), together with near-unit detection efficiency transition-edge sensors are used to demonstrate a detection loophole-free Bell violation. The setups presented in this thesis reach more than 82% detection efficiency for each measurement party of the Bell test.

We use a continuous wave source and organize detection events in uniform time bins to define a measurement round for the Bell test. A relatively high violation for a Bell test using photon pairs without detection loophole is observed with our system. The measurement outcome also shows that the observed violation and randomness generation rates depend on the time bin length. Using an extractor secure against a quantum adversary with quantum side information, we calculate an asymptotic rate of $\approx$ 1300 random bits/s. With an experimental run of 43 minutes, the extractor generated 617 920 random bits, corresponding to $\approx$ 240 random bits/s

List of Publications

Some of the results of this thesis have been reported in the following publications

1. **Lijiong Shen**, Jianwei Lee, Le Phuc Thinh, Jean-Daniel Bancal, Alessandro Cerè, Antia Lamas-Linares, Adriana Lita, Thomas Gerrits, Sae Woo Nam, Valerio Scarani, and Christian Kurtsiefer. **Randomness Extraction from Bell Violation with Continuous Parametric Down-Conversion.** *Physical Review Letters*, **121** (2018).

2. Jianwei Lee, **Lijiong Shen**, Alessandro Cerè, Adriana Lita, Thomas Gerrits, Sae Woo Nam, and Christian Kurtsiefer. **Multi-pulse fitting of Transition Edge Sensor signals from a near-infrared continuous-wave source.** *Review of Scientific Instruments*, **89**,8332 (2018).

3. Jianwei Lee, **Lijiong Shen**, Alessandro Cerè, James Troupe, Antia Lamas-Linares, and Christian Kurtsiefer. **Symmetrical clock synchronization with time-correlated photon pairs.** *Applied Physics Letters*, **114, 101102** (2019).

Some of the other results in this thesis have been presented in conferences.

1. **[Oral] Randomness extraction from Bell violation with continuous parametric down conversion**. In 8th International Conference on Quantum Cryptography, Shanghai, China, 27–31 August 2018

2. **[Poster] Randomness extraction from Bell violation with continuous parametric down conversion**. In Summer School on Experimental Quantum Computation 2018, Bensaque, Spain, 10-21 June 2018

3. **[Poster] Photon number and timing resolution of a near-infrared continuous-wave source with a transition-edge sensor**. In Single Photon Workshop 2017, Boulder, USA, July 31 - 4 August 2018

Table of contents

List of figures

Introduction

Randomness is an essential resource for many applications in modern science and technologies [1–5]. For example, Monte Carlo simulations require uniformly distributed random numbers as an input [5]. Some applications, such as quantum cryptography, require random numbers to be not only uniformly distributed, but also unpredictable [1, 2].

Most applications today rely on pseudo-random number generators, which are deterministic algorithms that generate sequences of statically random numbers from initial seeds [3, 6–9]. This type of random number generator is cheap and fast, but its output is completely determined by the input seed, making it not suitable for cryptography applications [1, 2].

Alternatively, a sequence of random numbers can be derived from a physical process (physical random number generator). Many existing physical random number generators are based on measuring properties of chaotic physical systems, such as fluctuation in atmospheric parameters, which are well described by classical mechanics [10]. These systems are deterministic, but the precision and computation resources necessary to measure the initial states and predict the measurement outcomes is outside of our current capacity. However, there is no way to ensure the quality and independence of the randomness generated.

Quantum random number generators belong to a special class of physical random number generators. They are based on one of the fundamental ideas of quantum mechanics: the outcome of a measurement on a quantum system is probabilistic. It is possible then to build a random number generator adopting a convenient choice of state and measurement. A simple example of quantum random number generator is the detection of single photons impinging on a 50-50 beam splitter. A binary random sequence is obtained by labeling the outcome of the photon transmitted or reflected as 1 and 0 [11]. The problem with this type of quantum random number generator is that it relies on the unverifiable assumption that the system is indeed governed by

a non-classical process. For example, how can we be sure that we are considering a single photon state [12]?

In 1964, John Bell proposed a test to check if the experimental system can be described by classical physics [13]. The Bell test takes the form of an inequality, and a violation of the Bell inequality means that the outcome from the measurement device can not be can not predetermined by local variables. Therefore, it is possible to use the violation of a Bell inequality to certify the generation of randomness [14, 12]. To date, several experimental realizations of Bell test have already been demonstrated [15–22].

In 2010, Pironio et al. first reported a randomness extraction experiment based on a Bell test using an atomic system (Yb+ ions) [14]. However, limited by the low repetition rate, the random number generation rate is only $\approx 10^{-5}$ s^{-1}, making it impractical for most applications. Photonic systems can have a much higher repetition rates compared with atomic systems, but photons are easily lost during transmission, and single photon detectors typically have low detection efficiencies. Most Bell tests using photons assume that the detected photons represent the whole system (fair sampling assumption). Conventionally, if a Bell violation is under this assumption, one attributes a detection loophole to this Bell test.

Advances in high-efficiency infrared single photon-detectors [23, 24], combined with high coupling-efficiency photon pair sources, allowed the demonstration of detection-loophole free Bell tests with entangled photons [17, 18, 20, 25]. The random bit generation rates for these setups are on the order of tens per second [26], where the main limitation is the fixed repetition rate of the experimental setup, combined with the small violation observed.

This thesis presents a polarization-entangled photon pair source based on continuous type-II spontaneous parametric down-conversion (SPDC) in Sagnac configuration [27, 28]. The source is designed and optimized to achieve high photon pair collection efficiency. However, an efficient source is not enough to close the detection loophole. Thus, it is necessary to couple the source to highly efficient superconducting detectors, transition-edge sensors (TESs) [29, 30]. Sae Woo Nam's research group from NIST manufactured the TESs for this work, and my lab partner Lee Jianwei installed and operated these detectors.

Most reported detection loophole-free Bell tests using photon pairs were performed with pulsed pumped SPDC sources, in which one measurement round of a Bell test can be naturally defined as one pump pulse [18, 20, 25, 26, 31]. For the continuous wave source presented in this thesis, the measurement rounds are defined by organizing the detection events into uniform time bins. For a fixed overall detection efficiency and

photon pair generation rate, the observed violation and random bit generation rate are functions of the time bin width.

0.1 Thesis outline

The goal of this thesis is to extract certified randomness from a detection loophole-free Bell violation with a continuous wave source. Chapter 1 discusses the concept of randomness and introduces different types of random number generators. It then explains the basic idea behind the Bell test, together with the concept of the detection loophole and remaining loopholes not addressed in this work. Chapter 1 also reports on state-of-the-art experiments generating certified randomness based on the Bell test.

Chapter 2 describes the process of designing and setting up the polarization-entangled photon pair source. This chapter also explains the method of optimizing the coupling efficiency and improving the signal-to-noise ratio. To close the detection loophole, the source is coupled to a pair of transition-edge sensors, which exhibits high quantum efficiency for single-photon [29, 30]. We show that the measured overall system efficiency is more than 82%, which is sufficient to close the detection loophole.

Chapter 3 explains the time binning method used to define measurement rounds of a Bell test with a continuous wave source. Based on the binning method, this chapter introduces a model used to estimate the maximal violation and optimal entanglement state. The procedures to experimentally prepare the optimal state is also described. This chapter closes with the experimental results of Bell violations for different time bin widths.

Chapter 4 briefly describes the randomness extraction protocol and random number extractor used in this work. The extractor extracted 617 920 certified random bits from the data used to demonstrate the violation.

Chapter 1

Theory and background

1.1 Randomness

1.1.1 The concept of randomness

This section answears two questions: "what is randomness?" and "is there intrinsic randomness in our nature?"

For the first question, let us look at this example [32]: there are two strings of numbers (a) and (b)

$$11111111111111111111111111111111 \quad \text{(a)}$$
$$10101100101000101101010101011110 \quad \text{(b)}$$

If one ask which string is random, perhaps most of the people will choose (b). This is because there is no obvious pattern in the string (b). But now if one say that these two strings are generated from the same process (for example consecutively toss a coin) and ask this question again, what is the answer?

Indeed, there are two types of randomness definition: process randomness and product randomness. Product randomness refers to a series of events which lack a pattern and process randomness refers to a process generating unpredictable series of events [33].

Although product randomness and process randomness are not the same, an unpredictable process will most likely produce a sequence that lacks a pattern. Yao's theorem also proved that process randomness will almost always imply product randomness [34].

This thesis studies the process randomness. In addition, this thesis also demonstrates a product randomness generation from our system.

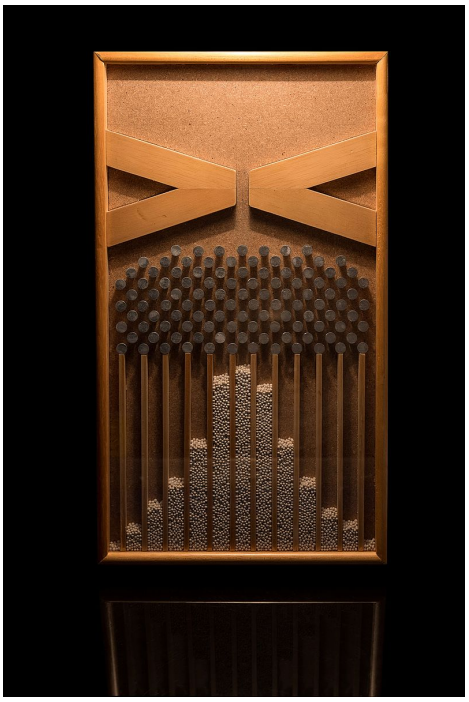


Fig. 1.1 The bean machine, also known as the Galton Board, invented by Sir Francis Galton [35]. The copyright of the image belong to [36]. Beans are dropped from the top. For an individual bean, when it hits the pegs, it either bounces left or right. Finally it will end at one bin at the bottom.

Now, it is time to answer the second question. By the definition of process randomness, generating randomness from scratch is impossible [12]. The hypothesis of super-deterministic model claims that everything, including the entire history of our universe, was predetermined in advance and known by an external observer. To the external observer, there is no random process in this universe. Therefore, any random generation protocol is based on some assumptions, and fundamentally a better random number generator is the one which has fewer assumptions. Since nothing is random to the external observer, one may ask the question: random for whom [33]? In an extreme case, if a random number generator is predictable to its user but not for any of adversaries (the external observers who may destroy the user's application seeded with the randomness input from the random number generator), it is still considered as a good random number generator.

1.1.2 Classical random number generator

There are few types of random number generators. A pseudo-random number generator is a deterministic algorithm that generates sequences of statically random numbers.

It will not be detailed in this thesis, since it belongs to the field of computer science, and the output of a pseudo-random number generator is completely determined by a seed. Another type of widely used random number generator is a physical random number generator, which generates random numbers from physical processes. For a physical system that can be described by classical mechanics, the randomness arises from the difficulty of predicting the classical system, making it practically unpredictable. However, classical mechanics is deterministic. In other words, in the classical theory, one can deterministically compute the measurement outcome of a classical system with all the initial conditions and infinite computation power. To clarify more on the classical mechanics' deterministic property, one can refer to the statement in the famous L. D. Landau and E. M. Lifshitz classical mechanics textbook [37]: "if all the coordinates and velocities are simultaneously specified, it is known from experience that the state of the system is completely determined and that its subsequent motion can, in principle, be calculated. Mathematically, this means that, if all the coordinates q and velocities $\dot{q}$ are given at some instant, the accelerations $\ddot{q}$ at that instant are uniquely defined". Thus, randomness from classical physics is based on the complexity of the system. If a system is chaotic, it is difficult to have the full detail of initial conditions and there is not enough computing power to predict where the system will end up.

Figure 1.1 exhibits a bean machine, which is used to demonstrate the central limit theorem [35, 36]. Nevertheless, it can also work as a classical random number generator. If I drop a bean from the top, it will hit the pegs and bounce to the left or right. Finally, the bean will end in one bin at the bottom. It is difficult to predict the destination of each beam. But in principle, it is possible to calculate the destination with all the initial conditions.

1.1.3 Quantum random number generator

Unlike classical mechanics, quantum mechanics is a probabilistic theory. For a general measurement, one cannot predict the outcome even if the state of the system is pure and well known. Figure 1.2 displays a simple example of a quantum random number generator by using single photons [11, 38, 39]. The user of the random number generator directs a photon to a 50-50 beam splitter. According to quantum theory, the photon has 50% chance to transmit through or be reflected by the beam splitter. If the detector at the transmission port (reflection port) of the beam splitter fire, the user labels the events with 1 (0). The interaction process between the single photon and the beam splitter is intrinsic random only if quantum mechanics can completely describe the

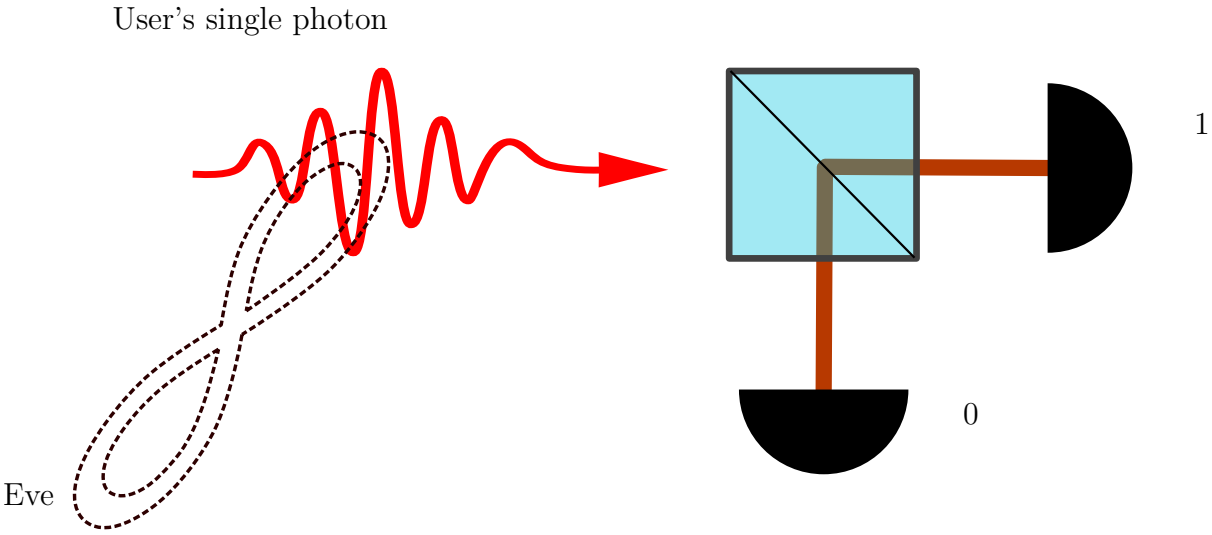


Fig. 1.2 A quantum random number generator using single photon. A photon is directed to a 50-50 beam splitter. Two single-photon detectors are placed at two out-ports of the beam splitter. If the detector at the transmission port (reflection port) of the beam splitter fires, the user labels it with 1 (0). Although this quantum random number generator is intrinsic random according to quantum theory, one can not rule out that the system is coupled with an adversary (Eve).

process. Moreover, the imperfection of the devices may bias the random outcome in an uncontrolled way. It is also impossible to prove that the single photons uncouples with an adversary's system. Therefore, the output may be random to the user, but not to an adversary.

Statistical tests are the only way to certify the outcome from a quantum random number generator using single photons. But as discussed in the previous section, product randomness does not necessitate process randomness. In an extreme case, one can copy the random numbers, passed all the statistical tests, to many memory-sticks. Each copy of the random numbers will pass the tests again, but they may be predictable to the adversary.

Consequently, it is important to build a random number generator producing device-independent certified private randomness. The random number generator should not rely on any modeling of the device. Fortunately, the Bell test offers a solution to it.

1.2 The Bell test

1.2.1 Background of the Bell test

In 1935, Einstein, Podolsky, and Rosen questioned in their famous paper [40]: is quantum mechanics a complete theory? In quantum mechanics, the measurement result on one particle of an entangled quantum system can be correlated to that of the other particles, regardless of the distance of the particles. However, this phenomenon is at odds with our everyday experience of the world, which happens to be local-realistic. Locality means that the information transfer speed is limited by the speed of light in vacuum. Realism is the assumption that a measurement outcome is predetermined before measurement. Thus, either the quantum mechanics theory is incomplete or nature itself is non-local-realistic.

In 1964, John Bell published the famous Bell theorem [13]. In that paper, he proposed an experimental method to check if the world is local-realistic. Even though he believed nature to be local-realistic, different experimental results of Bell tests have indicated that nature behaves differently. These experiments are implemented with different physical systems: ions [21], solid-state qubits [22], electron spins [19], and photons [15, 41, 17, 18, 20, 42–45].

1.2.2 The CHSH type Bell test

Today, there are a few different versions of the Bell test. Most of them take the form of an inequality. If one violates the inequality, the system under test is non-local-realistic. In this thesis, I focus on the CHSH-type Bell test, which was proposed by John Clauser, Michael Horne, Abner Shimony and Richard Holt in 1969 [46].

The CHSH scheme is a system with two parties conventionally named as Alice and Bob, who are space-like separated (shown in Fig. 1.3). Alice and Bob each have a measurement device with two measurement settings labeled with $x, y \in \{0, 1\}$, respectively. Alice and Bob perform the Bell test in successive rounds. In each round, each party independently chooses a measurement setting and records the measurement outcome. They label the outcomes with $a, b \in \{+1, -1\}$. The Clauser-Horne-Shimony-Holt expression can be defined as follows

$$S = E_{00} + E_{01} + E_{10} - E_{11}\,, \tag{1.1}$$

Fig. 1.3 A simplified CHSH Scheme. Alice and Bob each have a measurement device with two settings $x, y \in \{0, 1\}$ and two outputs $a, b \in \{-1, 1\}$. Bell tests are carried out in successions of rounds. Each party chooses a measurement setting and records the measurement outcome in every round.

where the correlators are defined by conditional probabilities $\Pr(A|B)$:

$$E_{xy} := \Pr(a = b|x, y) - \Pr(a \neq b|x, y)\,. \tag{1.2}$$

Using the labeling $a, b \in \{+1, -1\}$, one can rewrite the E_{xy} as

$$\begin{aligned} E_{xy} &= \Pr(ab = 1|x, y) - \Pr(ab = -1|x, y) && (1.3)\\ &= \langle (ab)_{xy} \rangle && (1.4)\\ &= \langle a_x b_y \rangle && (1.5) \end{aligned}$$

The last step of the derivation assumes the independence between the measurement setting of Bob (y) and the measurement outcomes at Alice (a), and also between Alice's setting (x) and Bob's outcomes (b). Thus, Eq.1.1 becomes:

$$S = \langle a_0 b_0 \rangle + \langle a_0 b_1 \rangle + \langle a_1 b_0 \rangle - \langle a_1 b_1 \rangle \tag{1.6}$$

If nature is local-realistic, the measurement outcome of Alice and Bob should be independent; $\langle a_x b_y \rangle = \langle a_x \rangle \times \langle b_y \rangle$. Therefore the absolute value of S can be written as:

$$\begin{aligned} |S| &= |\langle a_0 \rangle \langle b_0 \rangle + \langle a_0 \rangle \langle b_1 \rangle + \langle a_1 \rangle \langle b_0 \rangle - \langle a_1 \rangle \langle b_1 \rangle| && (1.7)\\ &= |\langle a_0 \rangle (\langle b_0 \rangle + \langle b_1 \rangle) + \langle a_1 \rangle (\langle b_0 \rangle - \langle b_1 \rangle)| && (1.8)\\ &\leq |\langle a_0 \rangle||\langle b_0 \rangle + \langle b_1 \rangle| + |\langle a_1 \rangle||\langle b_0 \rangle - \langle b_1 \rangle| && (1.9)\\ &\leq \max\{|\langle a_0 \rangle|, |\langle a_1 \rangle|\}(|\langle b_0 \rangle + \langle b_1 \rangle| + |\langle b_0 \rangle - \langle b_1 \rangle|) && (1.10) \end{aligned}$$

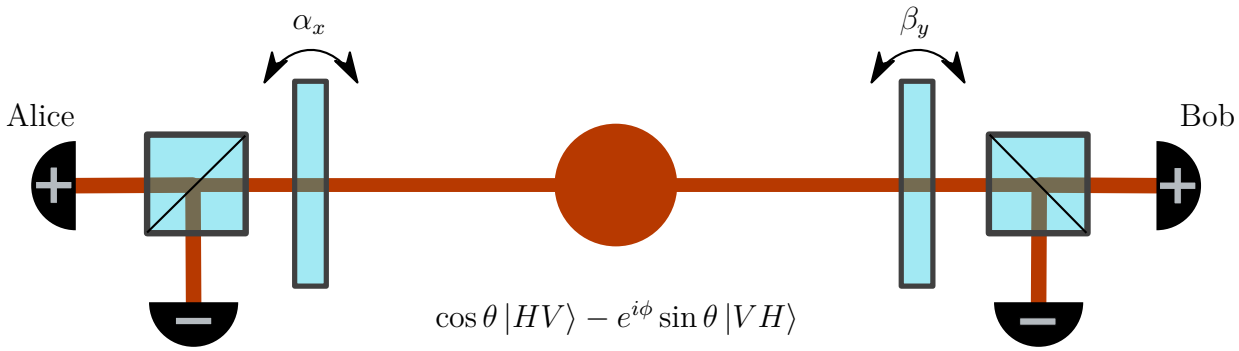


Fig. 1.4 A CHSH-type Bell test with photon pairs. A photon pair source distributes polarization-entangled photons to Alice and Bob. A half-wave plate (HWP) plate and a polarization beam splitter (PBS) define the measurement basis for Alice and Bob. Alice (Bob) has two measurement bases α_0,α_1 (β_0,β_1) corresponding to different HWP angles. In every measurement round, each party independently chooses a measurement basis. If the "+" ("−") detector fires, the output labeled as $+1$ (-1).

If $(\langle b_0\rangle+\langle b_1\rangle)(\langle b_0\rangle-\langle b_1\rangle) \geq 0$, then $|S| \leq \max\{|\langle a_0\rangle|, |\langle a_1\rangle|\}|2\langle b_0\rangle|$. Since $\max\{|\langle a_0\rangle|, |\langle a_1\rangle|\} \leq 1$, and $|2\langle b_0\rangle| \leq 2$, it is not difficult to see $|S| \leq 2$. Else $|S| \leq \max\{|\langle a_0\rangle|, |\langle a_1\rangle|\}|2\langle b_1\rangle|$, similarly, $|S| \leq 2$.

The above derivation proves that the $|S| \leq 2$ assuming local-realistic and one can write the CHSH inequality as

$$|E_{00} + E_{01} + E_{10} - E_{11}| \leq 2\,, \tag{1.11}$$

However, in quantum theory, if one performs a measurement on an entangled state with a smart choice of measurement basis, one can obtain a value of S more than 2. In other words, one can violate Bell inequality with an entangled state.

Here we take the polarization-entangled photon system as an example. In Fig. 1.4, a photon pair source distributes photons to Alice and Bob. The photon pair are in one of the maximally entangled

$$|\psi\rangle = \frac{1}{\sqrt{2}}\,|HV\rangle - \frac{1}{\sqrt{2}}\,|VH\rangle\ , \tag{1.12}$$

where H represents horizontal polarization, and V represents vertical polarization. A half-wave plate (HWP) plate and a polarization beam splitter (PBS) define the measurement basis for Alice and Bob. They can choose their measurement bases independently by rotating the HWPs. To be consistent with the CHSH inequality

introduced before, the "+" ("−") detectors correspond to the output values +1 (−1). If the four measurement bases are set as $\alpha_0 = 45°$, $\alpha_1 = 0°$, $\beta_0 = 22.5°$, and $\beta_1 = 67.5°$, quantum mechanics predicts

$$E_{00} = -\frac{1}{\sqrt{2}}, \qquad E_{01} = -\frac{1}{\sqrt{2}},$$
$$E_{10} = -\frac{1}{\sqrt{2}}, \qquad E_{11} = \frac{1}{\sqrt{2}}.$$

Via Eq.1.1, it is not difficult to find that $|S|$ value is equal to $2\sqrt{2}$, which violates the Bell inequality.

1.3 Loopholes in Bell test

Although the first experimental Bell test was done in 1972 [47], experimental violating the Bell inequality still draw a lot of interest. This is because the reported experimental Bell tests are under certain assumptions [48], which leave the experimental result open to local-realistic interpretations. This class of interpretations is called Local Hidden Variable (LHV) theories. If a Bell violation is observed under assumptions, this experimental Bell test so-called has loopholes. There are three main loopholes: locality, detection, and freedom of choice loopholes. In 2015, three independent groups reported that they completed a loophole-free Bell test [18–20], which closes the three main loopholes at the same time.

1.3.1 Detection loophole

In a real experimental system, not all the photon are registered due to the finite transmission and detection efficiency. The detection loophole can be explained as follows: the result of the Bell test can be explained as that the LHV selectively induces losses in the experiment in such a way that artificially violate the Bell inequality [50, 51]. Thus, the fraction of detected particles should be sufficiently large to represent the system.

Fortunately, closing the detection loophole does not require 100% detection efficiency (the probability that a generated particle pair is detected as a pair). While the minimum efficiency required for closing the loophole with a maximally entangled state is around 83% [52, 53], Eberhard showed that this threshold can be reduced to 66.7% by using non-maximally entangled state [49]. In his paper, he considered a photon pair system

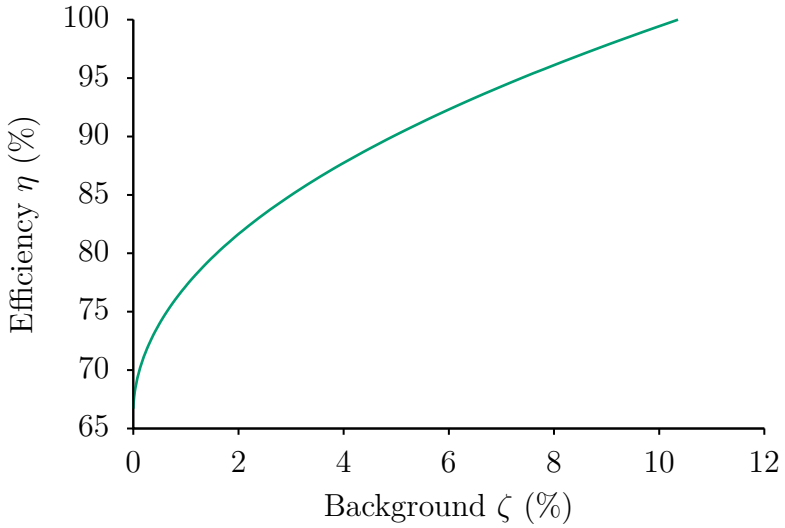


Fig. 1.5 Minimum-efficiency η required to close the detection loophole with different background counts level ζ according to Eberhard's model [49]. Here, Nζ is the number of the background counts, for N pairs generated.

similar to the Fig. 1.4 and derived an inequality

$$\begin{aligned} J^{ideal} &= n_{+-}(\alpha_1, \beta_2) + n_{+u}(\alpha_1, \beta_2) + n_{-+}(\alpha_2, \beta_1) \\ &\quad + n_{u+}(\alpha_2, \beta_1) + n_{++}(\alpha_2, \beta_2) - n_{++}(\alpha_1, \beta_1) \geq 0\,, \end{aligned} \tag{1.13}$$

where n is the coincidence counts with the subscripts $+$, $-$, u in which $+$ labels for the "$+$" detector fire, $-$ labels for the "$-$" detector fire, and u labels for undetected measurement outcomes. He constructed the quantum operator B for the value J^{ideal} and

$$J^{ideal} = \langle\psi|\, B\, |\psi\rangle\,, \tag{1.14}$$

where

$$|\psi\rangle = \frac{1}{\sqrt{1+r^2}}(|HV\rangle - r\,|VH\rangle)\,. \tag{1.15}$$

The value J^{ideal} is negative only if the operator B has a negative eigenvalue. By computing the corresponding eigenvector for the negative eigenvalue, he derived the r value of $|\psi\rangle$.

However, every real detector has dark counts even without any incident particles. Moreover, background particles from the environment may leak into the detection system and trigger the detector. All these contribute as background noise to the Bell test. The 66.7 % efficiency is only sufficient to close the detection loophole if there is zero background noise. Otherwise, a Bell test requires higher efficiency to become detection loophole-free.

Therefore, in Eberhard paper, he rewrote the J value as $J^{ideal} + 2\mathrm{N}\zeta$, where $\mathrm{N}\zeta$ is the number of the background counts. By reconstructing the B operator and applying the same procedures discussed above, he calculated the minimal required efficiency for closing the detection loophole as a function of background counts (shown in Fig. 1.5).

One can rewrite the Eberhard inequality [17] in Eq. 1.13 as

$$\begin{aligned} J^{ideal} = {} & S_{+}^{\mathrm{Alice}}(\alpha_1, \beta_2) - n_{++}(\alpha_1, \beta_2) + S_{+}^{\mathrm{Bob}}(\alpha_2, \beta_1) \\ & - n_{++}(\alpha_2, \beta_1) + n_{++}(\alpha_2, \beta_2) - n_{++}(\alpha_1, \beta_1) \geq 0\,, \end{aligned} \tag{1.16}$$

where $S_{+}^{\mathrm{Alice\ (Bob)}}(\alpha_x, \beta_y)$ are events registered at Alice's(Bob's) "+" detector with measurement settings α_x, β_y. Equation 1.16 also shows that two detectors sufficient to perform a detection loophole-free Bell test [17]. The equivalence of the Eberhard inequality with the CHSH inequality was shown several times [54–56].

In 2001, Rowe et al. [21] first performed a detection loophole-free Bell test using $^{9}\mathrm{Be}^{+}$ ions. They were able to detect ions with more than 90% efficiency. However, their two ions were only 3 μm separated from each other, and thus closing the locality loopholes (introduced in next section) was difficult. This work was also the first time a violation the Bell inequality has been observed without photons. In 2009, Ansmann et al. demonstrate a detection loophole-free Bell test with superconducting Josephson phase qubits [22]. This was the first experimental Bell test with solid-state qubits, but the distance between the two qubits was only a few mm. In 2013, two different groups closed the detection loophole with photon pairs [17, 25]. In this thesis, I will also demonstrate a detection loophole-free Bell test with a photon pair source. The method to define a measurement round in this work is different from others, and I will introduce that in Chapter 4.

1.3.2 Locality and freedom of choice loophole

In a Bell test, Alice and Bob are assumed to choose their measurement basis independently. To ensure that, there are can be no communication (no signaling) between the

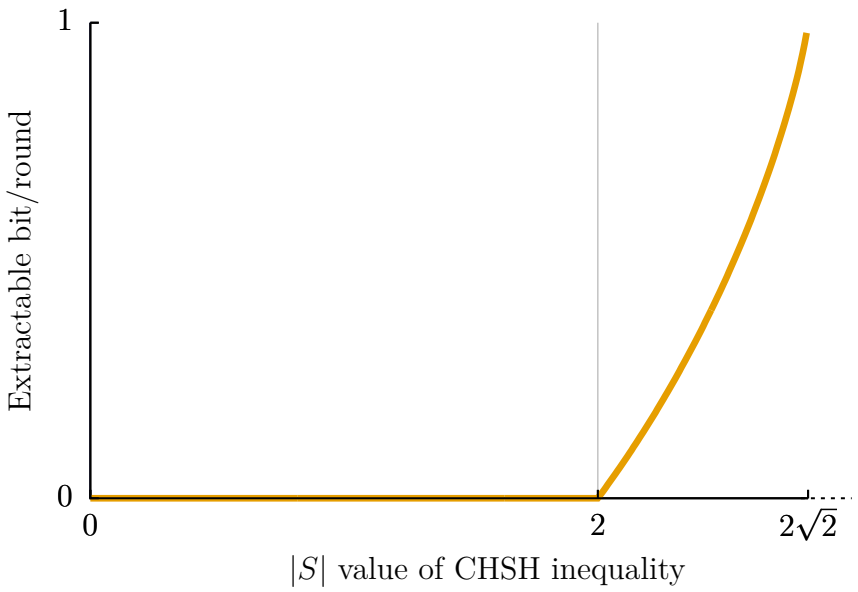


Fig. 1.6 Lower bound for extractable random bits per measurement round as a function of the S value [14]. In this figure, S is assumed to be collected from an experiment with an arbitrarily large number of measurement rounds.

measurement parties. Otherwise, a local hidden variable (LHV) could relay Alice's measurement setting to Bob's measurement device. However, any LHV is limited by the speed of light in vacuum. Thus, one can close the locality loophole if the experiment components are space-like separated. Aspect et al. first closed the locality loophole [15]. In a follow-up locality loophole-free Bell experiment, the separation between Alice's and Bob's measurement devices was more than 10 km [44].

Besides implementing the measurement choice fast enough to prevent signaling, Alice and Bob also have to choose their measurement settings randomly in each measurement round. Any pattern in the choice of measurement basis allows the LHV to influence the measurement outcome. This is called freedom of choice loophole [57]. In 2015, three individual groups closed the three main loopholes simultaneously with photons [20, 18] and electron spins [19]. There are also other loopholes such as coincidence-time loophole and memory loophole [58, 59], which I will not be elaborating in this thesis.

1.4 State-of-the-art on randomness extraction from Bell test

A violation of Bell inequality proves that the system is not local-realistic and the measurement outcome is not predetermined before the measurement. Moreover, the observation of a Bell violation ensures a certain purity of the distributed state. The purity of the quantum state certifies that the measurement devices of the two parties are not too correlated with the external observer [12]. Thus, it is possible to extract certified private randomness from the system violating the Bell inequality.

The extractable randomness from the Bell violation is computed without considering the modeling of experimental devices and is only based on the observed statistics $P(a, b|x, y)$, or the observed S value. Thus, the randomness is device-independent.

In 2010, Pironio et al. [14] first reported a proof-of-principle demonstration of device-independent randomness extraction based on a detection loophole-free Bell test in a Yb+ ions system. They obtained a very high S value (2.414). However, limited by the low repetition rates (3016 events measured in one month), the random bit generation rate was about 1.5×10^{-5} s^{-1}. They also showed that, if the Bell's inequality is calculated from an arbitrarily large number of measurement rounds, the extractable random bits per round is at least

$$r_\infty \geq 1 - \log_2\left(1 + \sqrt{2 - \frac{S^2}{4}}\right) . \tag{1.17}$$

Figure 1.6 shows the correlation between the extractable randomness r_∞ per round and the observed S value.

In 2013, Christensen et al. [25] performed a detection loophole-free Bell test using pulsed Spontaneous Parametric Down-Conversion photon source. Due to the relatively high repetition rates compared to an atomic system, their source was capable of generating secure private quantum random numbers at a rate of 0.4 s^{-1}. This number is about four orders of magnitude higher than the number reported in Pironio's work, but still not high enough to use in most of the real-world applications. In 2018, parallel to our experiment, Liu et al. [60] published their work on quantum random number generation from Bell test in which the random bits generation speed is 114 bits per second. They also used a pulsed photon system and closed the detection loophole. In order to achieve the reported generation rates, they needed to collect more than 100 hours of data. A few months later, their team performed a follow-up experiment [31],

simultaneously closing the detection loophole and locality loophole, resulting in a rate of 181 bits per second. In the same year, Bierhorst et al. [26] demonstrated the experimental randomness generation from a loophole-free Bell test; their random number generation rate is more than 1 s^{-1}.

Chapter 2

Efficient polarization-entangled photon pairs

Photons are appealing fundamental particles for such are easily transmitted, interact little with the environment, and are easily manipulated in their polarization degree of freedom. Moreover, photon pairs are an essential resource in quantum communication [39], computation [61], and clock synchronization [62]. As introduced in the previous chapter, one of the most challenging technical problems for an experimental loophole-free Bell test with photons is the detection loophole [17, 25]. Thus, it is important to build polarization-entangled photon pair source with high coupling efficiency, and detect the photon pairs with efficient single-photon detectors.

UV beams pump a periodically poled Potassium Titanyl Phosphate (PPKTP) [63–67] crystal to generate the photon pairs used in this work [28, 68]. With a large Gaussian pump beam, the generated photons' beam profile from PPKTP crystal is close to a Gaussian beam, resulting in an efficient collection by fiber optics. Section 2.1 shows the experimental setup used to generate and entangle photon pairs. We build a bulk source because the coupling efficiency of an integrated source is relatively low [69, 70]. Section 2.2 demonstrates how to optimize the heralding efficiency of the source. After the optimization, more than 43% heralding efficiency is obtained with two Silicon Avalanche Photo-Diodes [71]. Apart from the down-converted photons pairs, the UV pump beams also generate some uncorrelated wide-band fluorescence photons [72]. These fluorescence photons are recorded as background events. As a consequence, higher efficiency is required to close the detection loophole. Section 2.2.4 describes the method used to reduce the fluorescence.

Besides the high coupling-efficiency source, this chapter also introduces a type of high-efficiency single-photon detector, superconducting transition edge sensor (TES),

optimized for detection at 810 nm [23]. The TESs used in this work are manufactured by Sae woo Nam's research group at NIST and calibrated by my lab partner Jianwei. Section 2.3 also shows the connection between the source and the detectors with low transmission loss.

The last section of this chapter is dedicated to a detection efficiency measurement of the photon pair source together with the TESs.

2.1 Experimental setup of the Sagnac source

2.1.1 Generation and detection of photon pairs

Burnham and Weinberg observed the spontaneous parameter down-conversion process for the first time after the invention of laser [73]. In a SPDC process, a single pump photon has a low chance to split into two daughter photons, usually refereed as signal and idler. This process obeys both energy and momentum conservation rules. There are three different types of SPDC processes depending on the polarization of the down-converted photons. In this study, the two down-converted photons have orthogonal polarizations (type-II).

The PPKTP crystal used in this work is designed for a degenerate collinear process. In order to apply the timing coincidence method to detect the photon pairs [73], a polarization beam splitter (PBS) separates the photon pairs generated from the collinear down-conversion process into two spatial modes. The two modes are then coupled into two single-mode fibers connected to single-photon detectors.

Here, S_1 and S_2 denote the singles rate for each detector, which correspond to the number of events registered by each detector per unit time. If the two detectors fire within a specific coincidence time window τ_c, one records it as a pair detected. The rate of detected pair events is denoted as p, and the heralding efficiency η of the photon pair is defined as the pair to singles ratio

$$\eta = \frac{p}{\sqrt{S_1 \times S_2}}\,. \tag{2.1}$$

Intuitively, the heralding efficiency is the probability of detecting the second photon, conditioned on the first photon of the same pair being registered. There are three main methods to improve heralding efficiency: reducing the transmission losses caused by optical elements, improving the fiber coupling efficiency, and using high-efficiency single-photon detectors. The following sections will detail all of them.

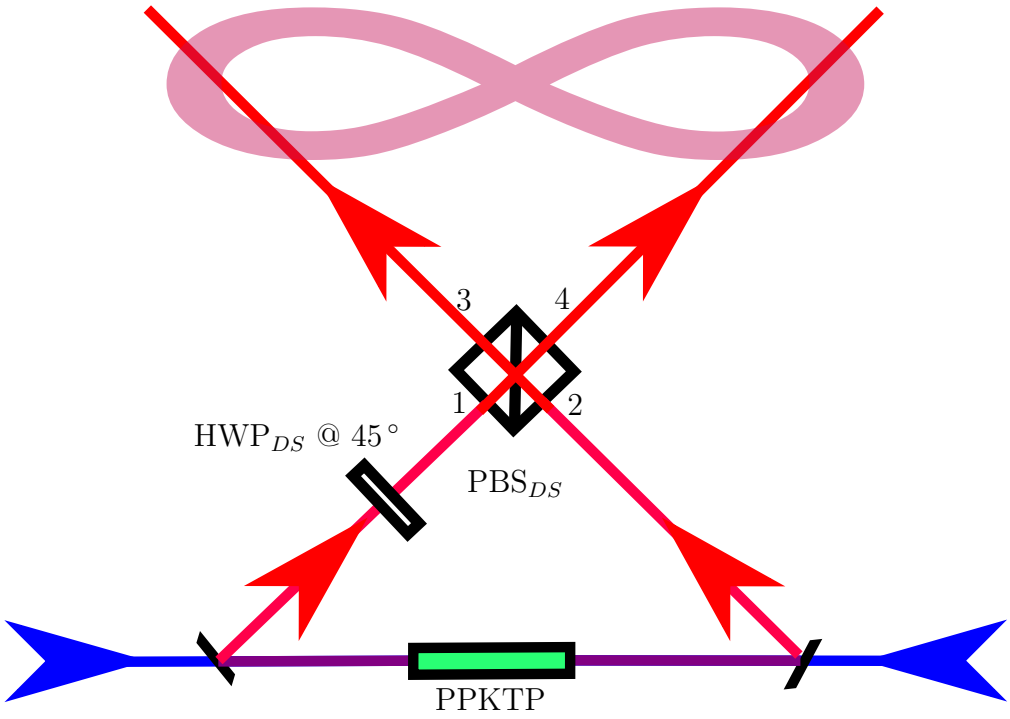


Fig. 2.1 Simplified layout of the Sagnac-style source for polarization-entangled photon pairs. UV light pumps the PPKTP crystal from opposite directions to generate polarization-entangled photon pairs. The collinear 810 nm down-converted photon pairs are emitted in mode 1 or 2 depending on the pump direction. A pair of mirrors direct the two infrared light modes to overlap on a polarization beam splitter (PBS) for the down-converted pairs. The two-photon state between modes 3 and 4 is then polarization-entangled [27].

2.1.2 Entangling the photon pairs

The type-II SPDC process can generate photon pairs with orthogonal polarization, but the generated photon pairs are not entangled. In 1995, Kwiat et al. first demonstrated entanglement generation using the SPDC process in a single crystal [74]. They used a BBO crystal and collected photons pairs at the cross-section of the two down-converted light cones [74, 75]. In this study, the entanglement is generated from a different geometry.

Figure 2.1 shows a simplified layout of the polarization entangled photon pair source. A PPTKP crystal is placed at the middle of a Sagnac interferometer, which is named after France physicist Georges Sagnac who first built the interferometer in 1913 to test the existence of aether [76]. In 2003, two different research groups demonstrated the polarization-entanglement generation based on this geometry [27, 77]. The interferometer includes a PBS (labeled as PBS$_{DS}$), which entangles the down-

converted photon pairs, and two dichroic mirrors, forming an isosceles triangle. After overlapping the two down-converted modes onto the PBS_{DS}, photon pairs generated in the two counter-propagating paths with different polarizations are in the same spatial mode.

In Fig. 2.1, each pump beam enters the Sagnac triangle through a dichroic mirror and pump the PPKTP crystal. The second dichroic mirror reflects the down-converted photon pairs and removes the pump beam out of the Sagnac interferometer. We label the mode propagating clockwise inside the interferometer as "1", and the other down-converted mode as "2". The output modes of the PBS_{DS} are denoted as "3" and "4", corresponding to the two collection arms. Each SPDC process generates two daughter photons H_s and V_i, which represent the horizontally polarized signal photon and the vertically polarized idler photon. First, the photon pairs ($|H_s\rangle_1$, $|V_i\rangle_1$) generated by the left side pump beam in Fig. 2.1 pass through a HWP_{DS} oriented at 45 degrees to the vertical axis, which rotates the polarization of the photon pair to ($|V_s\rangle_1$, $|H_i\rangle_1$). The PBS_{DS} then separates the photon pair into ($|V_s\rangle_3$, $|H_i\rangle_4$) . The photon pair ($|H_s\rangle_2$, $|V_i\rangle_2$) generated by the right side pump beam also travel to the PBS_{DS}, resulting in ($|H_s\rangle_3$, $|V_i\rangle_4$). If the two pump beams have the same power, one can write the photon state in modes 3 and 4 as

$$|\psi\rangle = \frac{1}{\sqrt{2}}\Big(|H_s\rangle_3 |V_i\rangle_4 - \mathrm{e}^{\mathrm{i}\phi} |V_s\rangle_3 |H_i\rangle_4 \Big), \tag{2.2}$$

where the phase ϕ conserves the phase difference between the two pump beams. Details of a phase control procedure will be introduced later.

It is important to note that the entanglement does not emerge from the interference of two photon pairs generated from different pump directions. Generating two photon pairs within the coherence time is rarely happening due to the low down-conversion probability of a single pump photon. Instead, the indistinguishability of the measured photon pair generated from each pump direction leads to the entangled state.

The reason of rotating the polarization of the photon pair ($|H_s\rangle_1$, $|V_i\rangle_1$) is that the vertically polarized signal photon and the horizontally polarized idler photon have different group velocities inside the PPKTP crystal. If HWP_{DS} is not present in the Sagnac loop, distinguishing the photon pair from which pump direction is possible by comparing the arrival times of photons in different collection modes.

Most reported Sagnac-style entangled sources have a geometry that the pump beams and down-converted modes overlap inside the Sagnac interferometer [17, 18, 77, 78].

The advantage of the overlapped scheme is that slow fluctuations inside the Sagnac triangle are canceled out for both the pump and down-converted modes. In our scheme, the pump beam only overlaps with the converted mode at the base of the Sagnac triangle (see Fig. 2.1). This fully decouples alignment degrees of freedom between the pump beam and down-converted modes, making it easy to align the source to obtain high heralding efficiency. However, this geometry requires a phase stabilization process to lock the generated entanglement state.

2.1.3 Characterization of the source

This section provides a detailed description of the source designed for this work based on the described working principle. Figure 2.2 shows a schematic figure and a photograph of the experimental setup. A PPKTP crystal (size: $1 \times 2 \times 10$ mm), cut and poled for type-II spontaneous parametric down-conversion from 405 nm to 810 nm, is placed at the waist of a Sagnac interferometer and pumped from both sides. The pump light is generated by a grating-stabilized laser diode centering at 405 nm (Ondax) with a bandwidth of 160 MHz [79], and coupled into a polarization maintaining (PM) single-mode fiber suitable for 405 nm. The PM fiber not only filters the spatial mode but also stabilizes the pump polarization. A telescope placed after the PM fiber focuses the pump beams at the center of the crystal with variable waists. A PBS, anti-reflection coated for 405 nm, splits the pump beam into two. Each pump beam is independently directed to the crystal in opposite directions by two mirrors. As mentioned in the previous section, the 810 nm light from the two SPDC processes in each direction overlaps at the polarization beam splitter (PBS_{DS}), generating a non-maximally entangled state

$$|\psi\rangle = \cos\theta\,|HV\rangle - e^{i\phi}\sin\theta\,|VH\rangle\ . \tag{2.3}$$

The rotation of the HWP before the 405 nm PBS controls the relative power between the two pump arms, which determines the angle θ in Eq. 2.3. The phase ϕ is controlled by tiling a thin glass plate in one of the pump modes.

In each collection arm, a combination of a HWP and a PBS defines the polarization measurement basis for our experimental Bell test. Another dichroic mirror placed after PBS directs the down-converted photons to a fiber single-mode for 810 nm light (SMF@810), which further filters out the UV photons. An aspheric lens (f = 11 mm from Thorlabs) focuses the 810 nm light into the SMF@810. The single mode fiber

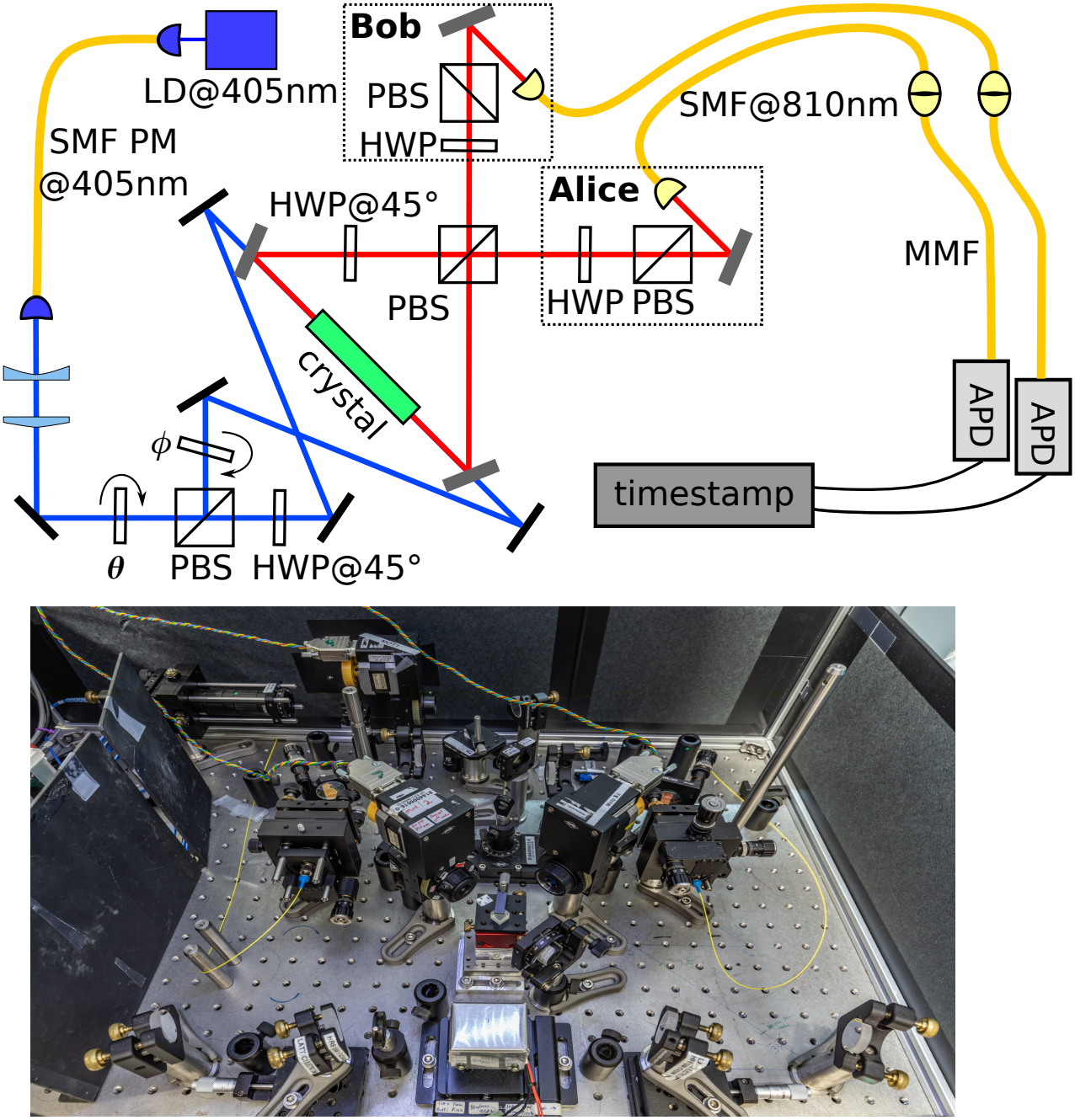


Fig. 2.2 Complete layout of our Sagnac-style entangled photon pair source for the presented experiment. To generate polarization-entangled photon pairs, UV beams pump the PPKTP crystal from opposite directions in a Sagnac configuration. The pump light is generated by a grating-stabilized 405 nm laser diode with narrow bandwidth and coupled into a PM 405 nm single mode fiber. A PBS splits the UV laser beam into two, and two separate mirror sets direct them to the crystal. A thin glass plate inside one pump mode controls their relative phase ϕ, and a half-wave plate before the splitting PBS sets the angle θ. A combination of a HWP and a PBS defines the polarization measurement basis before the down-converted photons coupled into the single mode fiber for 810 nm light.

is mounted on a z-translation stage used to fine-adjust the distance between the lens and the fiber for optimizing the coupling efficiency. An interference filter with a center wavelength of 810 nm and bandwidth of 10 nm is placed before the aspheric fiber coupling lens to suppress wide-band uncorrelated fluorescence photons from the crystal pumped with UV light. Section 2.2.4 will detail more about the fluorescence reduction.

For source calibration, we detect the photon pairs using "Geiger" mode Silicon Avalanche Photodiodes (APDs) detectors [71, 80, 81]. Such APDs are one of the most popular single-photon detector used in quantum optics experiments. The quantum efficiency of APDs at near-infrared wavelength (≈50%) is not sufficient to close the detection loophole. However, after more than 40 years of development, APDs have very reliable performance without a cryogenic cooling system, making them easy to use and fast to install.

2.2 Source optimization

2.2.1 Mode matching

Most of the high-efficiency and low dark-count single-photon detectors are fiber coupled. Thus, it is important to efficiently couple the generated down-converted light into fibers. This is performed through overlapping the optical modes of the collection optics with that of the pump. The optimal pump and collection modes for a high heralding efficiency η_c with collection optics have been well studied in [82, 83].

The pump and the collection modes are difficult to overlap if the focus is tight, which makes the down-converted modes hard to be coupled into single mode fibers. Too tight focusing also leads to a very short Raleigh range; this makes it difficult to position the collection waist at the middle of the crystal. Theoretically, the larger the pump waist, the better the coupling efficiency. However, a large pump beam waist reduces brightness of the source. Moreover, if a pump beam waist is too large, the modes of the down-converted photons could be coupled at the edges of the PPKTP crystal due to the limited clear aperture of our crystal (1 mm×2 mm). It is also essential to ensure that both the pump mode and collection mode are centered in the middle of the crystal, which is also the waist location of the Sagnac-style interferometer, such that the modes are symmetric for both pump directions.

Figure 2.3 depicts the numerically calculated correlations between the heralding efficiency η_c and collection waist ω_c according to the theory in [82] for various pump waist ω_p. The figure shows that it is possible to achieve over 99% heralding efficiency if

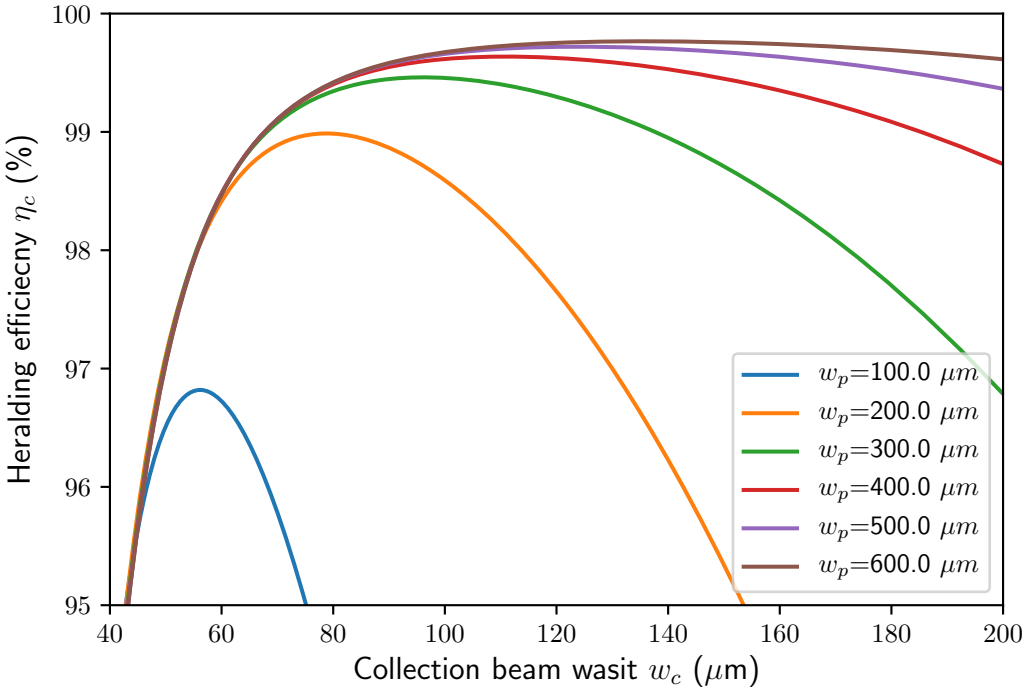


Fig. 2.3 Numerically calculated correlations between the heralding efficiency η_c and collection waist ω_c according to the theory in [82]. This simulation assumes that both the pump and collection modes are focused in the middle of the crystal. Each line represents a different pump waist ω_p. The horizontal axis is collection beam waist ω_c for both signal and idler modes. The simulation takes into account the length of our crystal (10 mm), but ignores the effect of the limited clear aperture of the crystal (1 mm $\times$ 2 mm) for a large ω_c.

ω_p is larger than 200 μm, while the corresponding optimal ω_c is more than 80 μm. This figure also indicates that for a pump waist larger than 400 μm beam, there is a large tolerance range (more than 100 μm) for the collection waist to obtain high heralding efficiency.

In order to focus different waists in the middle of the PPKTP crystal, at least two lenses are needed to control the two degrees of freedom of a Gaussian beam: waist and position. Both of them have to be capable of moving along the beam propagation direction independently. However, each anti-reflection coated lens contributes approximately 0.5% transmission loss. Moreover, if a beam is not perpendicular to and at the center of a lens, the profile of the beam will be distorted. Thus, it is necessary to minimize the number of lenses, especially in the collection arms.

A variable optical beam expander (BE052-A from Thorlabs), anti-reflection coated at 405 nm, focuses the pump waist at the center of the crystal (around 1.2 m away from the beam expander) with variable pump beam waists (see Fig. 2.2). Only one aspheric lens (C220-B, Thorlabs, f=11 mm) is placed in each collection arm to focus the 810 nm light into a single mode fiber. In comparison to the pump arms, the transmission loss in the collection arms is more important since it reduces the heralding efficiency. Thus, the number of lenses inside the collection arm is less than that in the pump mode. However, this means that only one specific collection waist can be obtained in the middle of the crystal.

The distance from the collection couplers to the waist of the Sagnac interferometer is around 65 cm. The estimated collection waist at the crystal with a f=11 mm lens and 810 nm single mode fiber is around 130 μm; this collection waist is optimal for more than 500 μm pump waist according to the numerical simulation (see Fig. 2.3). To achieve high coupling efficiency, we need to ensure that the collection mode is focused at the waist of the Sagnac interferometer with the design beam waist. Thus, the waist of the beam sent from the collection fiber is verified with a a knife-edge measurement [84]. Under paraxial approximation, the transverse electric field intensity of a collection beam is well approximated by a Gaussian function as

$$I(r,z) = I_0 \left(\frac{\omega_0}{\omega(z)}\right)^2 e^{\left(\frac{-2r^2}{\omega^2(z)}\right)}, \tag{2.4}$$

where $I_0 = I(0,0)$ is the intensity at the center of the beam waist ω_0, and $\omega(z)$ is the spot size at the specific longitudinal position z. For each spot size measurement, a knife edge blocks the beam at location z; then the knife moves in steps of 20 μm in the direction perpendicular to the beam. The intensity of the unblocked portion of the beam changes with the movement of the knife edge, and is recorded by a photodiode. We can obtain the corresponding $\omega(z)$ by fitting the data to a error function. After obtaining one spot size, the knife moves in the z-direction for 2 mm for another knife-edge measurement. For one measurement round, the knife travels along the beam propagation direction for 25 mm.

Figure 2.4 (a) shows a knife-edge measurement for an 810 nm beam sent from one collection coupler (left side of the Sagnac interferometer in Fig. 2.1). The obtained spot sizes at different z are fitted to the expression for the beam parameter $\omega(z)$ for a

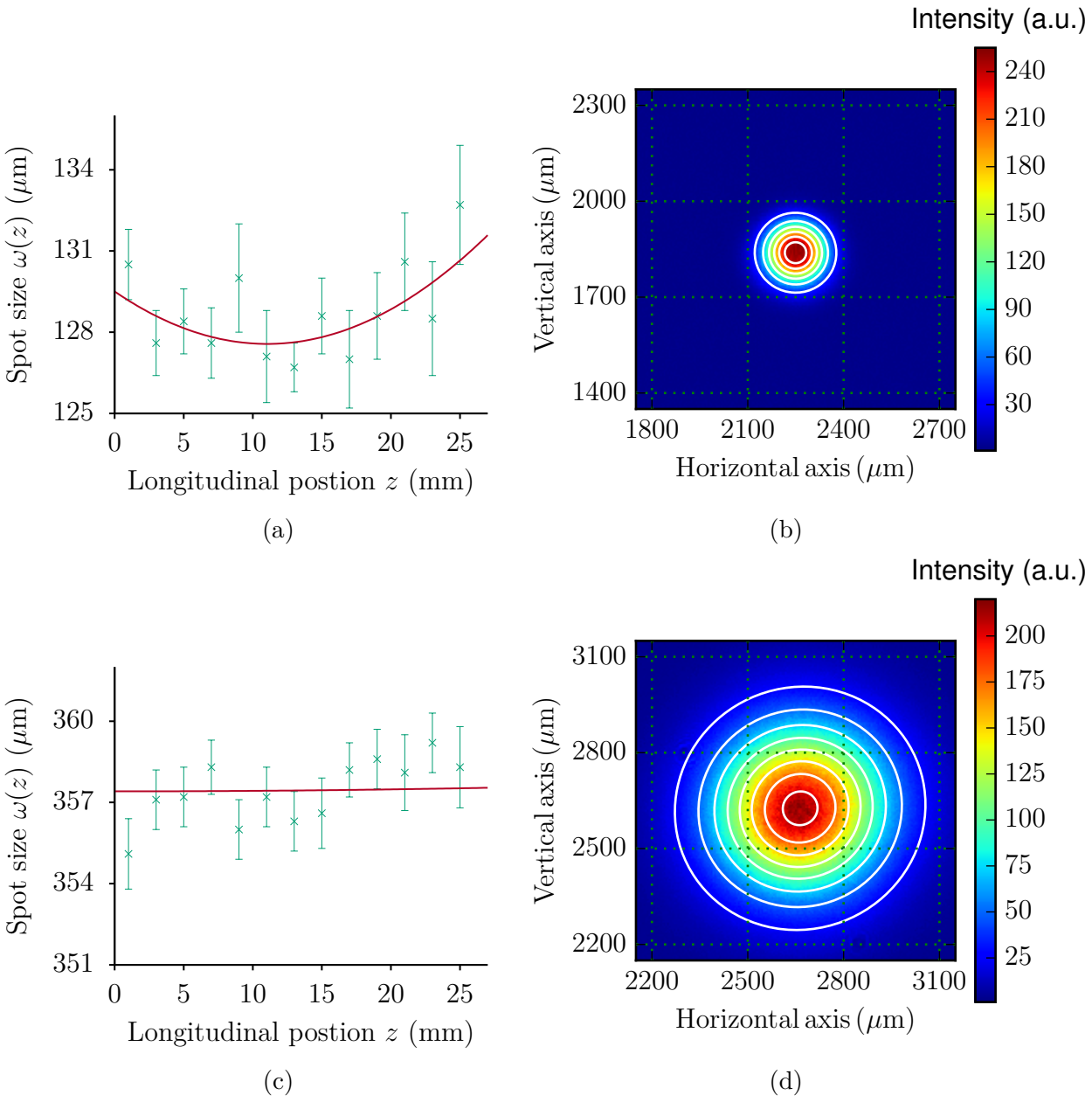


Fig. 2.4 The collection and pump beam profile measurement. Figure (a) and (b) are measurements on a collection beam. Each point in Fig. (a) corresponds to a beam spot size from a knife-edge measurement; we repeat this measurement at different positions in the beam propagation direction. Where, 12.5 mm of the z-axis is the waist of the Sagnac interferometer. The fitted beam waist ω_0 is 127.57±0.32 μm. The position of the beam waist z_0 is 11.04±1.47 mm. Figure (b) Shows a camera image of this beam fitted with an elliptical Gaussian model. The two fitted waists ω_a and $\omega_b$are 127.57±0.01 μm and 124.78±0.01 μm. Figure (c) and (d) are measurements on a pump beam. Different from the Fig. (a), −30 mm of the z-axis is the waist of the Sagnac interferometer. The fitted result are ω_0= 357.41±0.66 μm and z_0 = 0.1±126.9 mm. The fitted result for Fig. (d) are ω_a = 371.90±0.02 μm and ω_b = 356.55±0.02 μm.

paraxial Gaussian beam

$$\omega(z) = \omega_0 \sqrt{1 + \left(\frac{z - z_0}{z_R}\right)^2}, \tag{2.5}$$

where z_0 is the position of the beam waist, ω_0 is the beam waist, and z_R the so-called the Rayleigh range given by

$$z_R = \frac{\pi \omega_0^2}{\lambda} \tag{2.6}$$

for a wavelength λ wavelength of the beam. The fit leads to $\omega_0 = 127.57 \pm 0.32\,\mu$m, and $z_0 = 11.04 \pm 1.47$ mm, where the waist of the Sagnac interferometer is at $z = 12.5$ mm. These values are similar to the calculated result with the input of the properties and positions of the given optical elements. The Rayleigh range of the beam computed by the measured waist is around 63 mm, which is much larger than the fitting uncertainty. The beam thus is focused not far away from the waist of the Sagnac interferometer. For the beam sent from the other collection coupler, we obtain $\omega_0 = 129.16 \pm 0.31\,\mu$m and $z_0 = 10.05 \pm 1.87$ mm, respectively.

We use a camera to capture an image of the 810 nm beam at the waist of the Sagnac interferometer to further check the quality of the Gaussian beam profile. Figure 2.4 (b) shows an image of a beam sent from one coupler. The image is fitted with a two-dimensional elliptical Gaussian model, leading to $\omega_a = 127.57 \pm 0.31\,\mu$m and $\omega_b = 124.78 \pm 0.31\,\mu$m for the profile shown in Fig. 2.4 (b). The similarity between the two fitted waist values confirms that the beam profile is round. Both ω_a and ω_b are comparable to the waist measured by the knife-edge measurement.

After obtaining good collection modes, we insert a PPKTP crystal mounted on a five-axis translation stage in the setup and optimize the pump waist for high heralding efficiency. Here, the crystal is only pumped from one direction, and the heralding efficiency is measured using APDs. Figure 2.5 shows the measured heralding efficiency and theoretical calculated efficiency based on Bennink's model [82] with a fixed collection waist (128 μm) obtained from the previous measurement. The efficiency values have been corrected for all optical losses and the detectors' efficiency, but not for the lens aberration. The large uncertainty of each data point is mainly caused by the efficiency uncertainty of the detectors due to the calibration setup. Each data point in Fig. 2.5 represents an efficiency measurement over 100 seconds with the same detectors, the

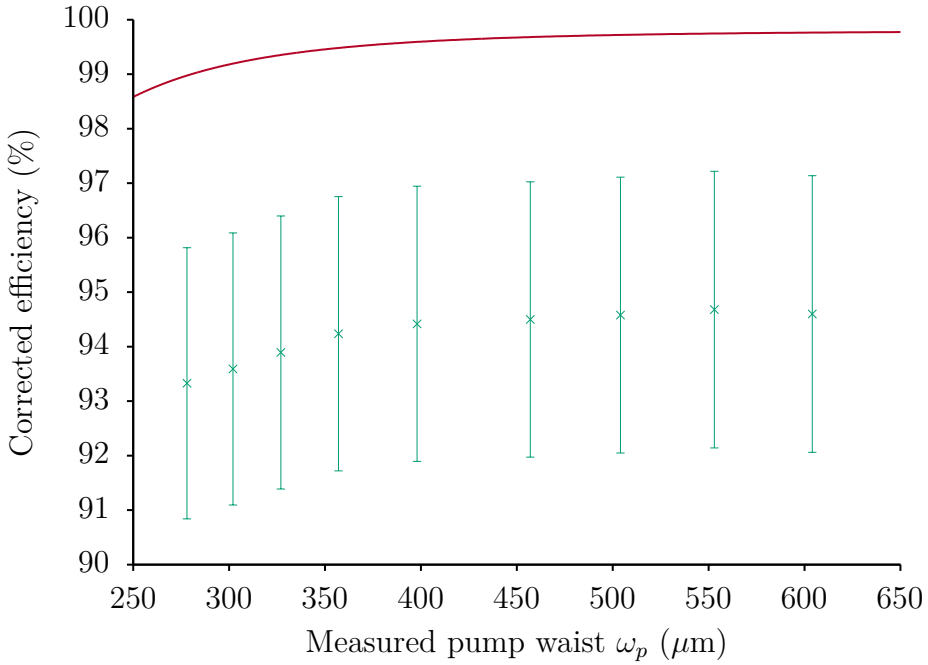
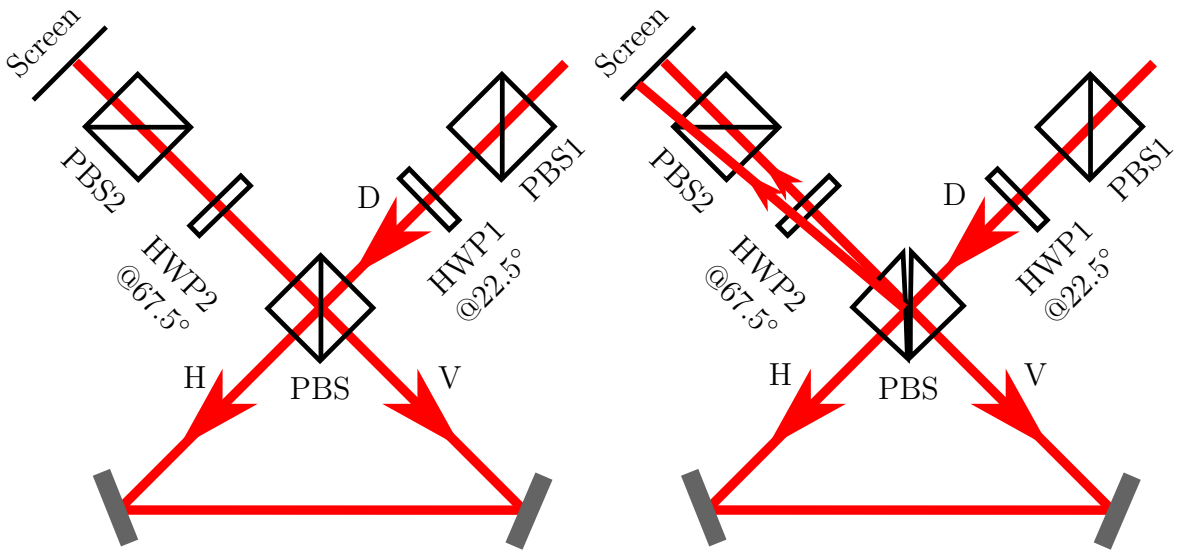


Fig. 2.5 Measured heralding efficiency versus pump beam waist with a fixed collection waist ($\omega_c = 128\,\mu$m). The red line represents the numerically calculated heralding efficiency η_c according to the theory in [82]. The green dots label the experimentally measured heralding efficiency for different ω_p, corrected for optical losses and the detector efficiency, but not for the lens aberration. Each point represents a efficiency value measurement over 100 seconds with same detectors. The corresponding uncertainty from Poisson short noise is $\approx 0.1\%$. The high uncertainty of each data point is mainly caused by the efficiency uncertainty of the detectors.

corresponding uncertainty due to Poisson short noise is around 0.1%. Thus, the figure can clearly show how the measured efficiency values change with different pump waists. Finally, the pump waist is chosen as 357 μm. The measured efficiency with this pump waist is not too different from the efficiency with the optimal waist (See Fig. 2.5). However, the generated pair rate is two times higher. A high pair rate is beneficial for extracting more randomness for a given acquisition. This will be discussed in Chapter 4. Figure 2.4 (c) and (d) show a knife-edge measurement and a fitted camera image of a pump beam. When we perform the knife-edge measurement on the pump beam, the crystal is already placed in the Sagnac interferometer. To preserve the alignment of the crystal, the knife-edge measurement is performed slightly away from the waist of the Sagnac interferometer. In Fig. 2.4(c), the origin of the horizontal axis is about 30 mm away from the center of the crystal. In other words, the waist of the Sagnac interferometer is located at z = -30 mm. The fitted waist resulting from Fig. 2.4 (c) is



(a) (b)

Fig. 2.6 Sagnac interferometer alignment. Figure (a) shows a Sagnac interferometer beam alignment diagram with PBS free of wedge error. First, one sends light from the right corner and set the polarization to diagonal with PBS1 and HWP1, then aligns the Sagnac PBS to overlap the H and V polarization beam inside the Sagnac loop, and at the output of the interferometer. An interference pattern can be observed on the screen by setting HWP2 to 67.5°. The detail of the alignment procedure is described in the main text. Figure (b) illustrates why good interference pattern can not be observed if the PBS exhibits a wedge error, even if the beams perfectly overlap inside the Sagnac loop.

357.41±0.66 μm, and the fitted position of of the beam waist is close the crystal, with a fitting uncertainty about 100 mm. However, the Rayleigh range of a 405 nm beam with such a waist is more than 1 meter. Thus, the high uncertainty is still acceptable. The two fitted waists for Fig. 2.4 (d) are ω_a = 371.90±0.02 μm and ω_b= 356.55±0.02 μm, The image is taken 30 mm after the waist of the Sagnac interferometer. For the other pump direction, the measured beam waist and position are very similar.

2.2.2 Alignment of the Sagnac interferometer

The mode matching method introduced in the previous section only helps to obtain high heralding efficiency for a single pass source. To obtain polarization-entangled states, however, it is critical to build a well-aligned Sagnac interferometer to obtain high efficiency as defined in section 2.2 for both pump directions.

Figure 2.6 (a) explains the alignment procedure for the Sagnac interferometer. In this work, we design the Sagnac interferometer with an isosceles right triangle geometry. The base of the triangle (*triangle base* in this section) is used as a reference. The alignment procedure for our Sagnac interferometer can be divided into a few steps:

1. Send 810 nm light from the right upper corner and align it along the line 45° against the triangle base with a pinhole (150 μm diameter) at fixed height (100.5 mm) above the optical table.

2. Insert PBS1 and HWP1 @22.5° and adjust them to make sure that the beam still travels along the line 45° against the bottom edge.

3. Put the two mirrors, each of them sat on a translation stage, at the bottom of the triangle. Adjust the mirror mount and use the same pinhole to ensure the beam parallel to the bottom edge after the first mirror and propagate along the other 45° line after the second mirror.

4. Put the Sagnac PBS (at the center of the Fig. 2.6) into the setup. By adjusting the position and three rotation axes of the PBS, the H polarization and V polarized beam could overlap inside the Sagnac loop with the accuracy of the 150 μm pinhole.

5. Now, an interference pattern should be visible on the screen in Fig 2.6 (a). Fine adjust the Sagnac PBS to improve on the visibility of the interference.

One can evaluate the quality of the interference by measuring the polarization visibility at the place of the screen in Fig. 2.6. The intensity with HWP2@67.5° (HWP2@22.5°) is labeled as m (M). The definition of a visibility V is

$$V = \frac{M - m}{M + m}\,. \tag{2.7}$$

With this method, a visibility over 99.5% has been achieved.

However, even with this high visibility, we still could not obtain a symmetrical high efficiency for both pump directions. To verify the suspicion that the asymmetric efficiency is caused by the wedge error of the Sagnac PBS, which is the deviation between the two prisms, we checked if the beams are overlapped well inside the Sagnac loop after obtaining high visibility. A 150 μm pinhole at the crystal position worked as a marker. Since a PBS does not significantly affect the horizontal polarization

beam (H) but reflects the vertical polarization beam (V), the H beam still has similar transmission though the pinhole if the Sagnac PBS is absent. However, the transmission of the V beam was one order of magnitude lower. Figure. 2.6 (b) shows that with a PBS with a wedge error, even if the beams with different polarizations perfectly overlap inside the Sagnac loop, they will still separate at the output of the Sagnac PBS.

An optically contacted PBS not only has smaller wedge error, but also preserves a better beam profile when compared with glued PBS because of the absence of non-uniform glue between the two prisms. However, the supplier for optically contacted PBS used in the alignment procedure described above could only specify a wedge error < 8'. Therefore, we had to order post-selected optically contacted PBSs with prismatic deviation < 30".

To identify the PBS with the smallest wedge error, we first rebuild the Sagnac interferometer with these new PBSs and optimized it for high visibility, then checked the transmission of the reference pinhole for both the H and the V beams at the waist of the Sagnac interferometer. For the best PBS in the new batch, the transmission of the V beam was close to 90% of the H beam.

The Sagnac interferometer with the post-selected PBS now shows a similarly high heralding efficiency for both pump directions. The measured efficiency using two APDs were 43.36±0.09% and 43.15±0.09%. After correcting for the optical losses and the detector's efficiency, the efficiency of the source reached become 94.07±2.51% and 93.65±2.50% for the two pump directions.

2.2.3 Visibility of the maximally entangled state

After obtaining a high efficiency for both pump direction, we checked the quality of the maximally entangled state emerying from the source through a polarization correlation visibility measurement [85]. By choosing the amplitude-mixing angle $\theta = 45°$ and the phase $\phi = 2\pi$, Eq. 2.3 reduces to a maximally entangled singlet state

$$|\psi\rangle = \frac{1}{\sqrt{2}}|HV\rangle - \frac{1}{\sqrt{2}}|VH\rangle \ . \tag{2.8}$$

As introduced before, a HWP and a PBS define the measurement basis in each collection arm. Any linear polarization basis can be implemented by rotating the HWP with a motor. During a visibility measurement, we fix Alice's HWP angle (θ_{Alice}), and count the number of coincidences as a function of Bob's HWP angle (θ_{Bob}). The definition of

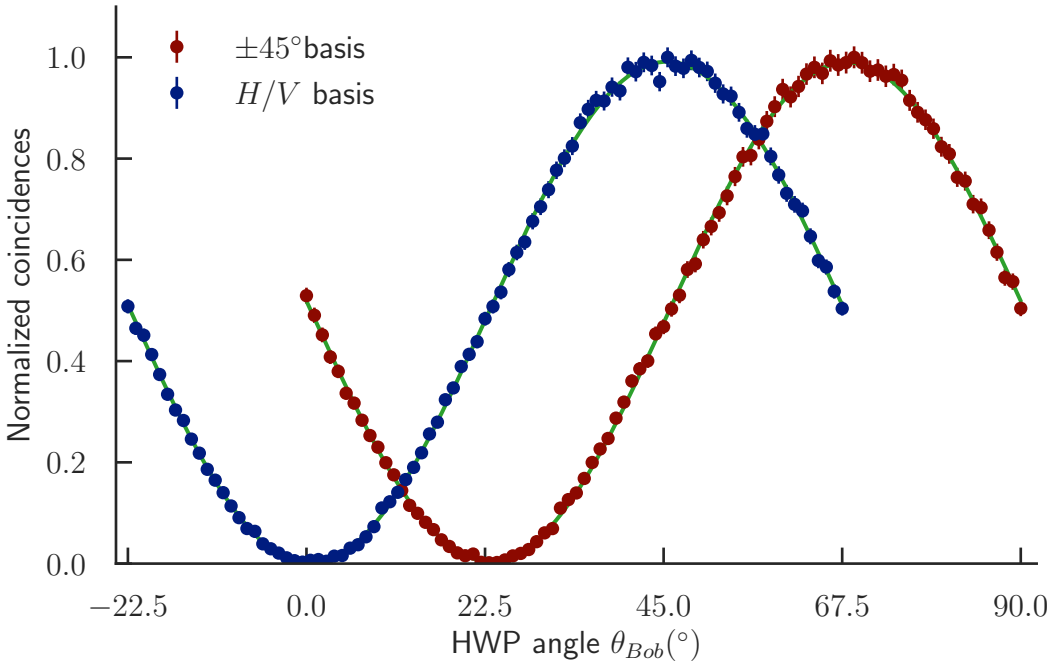


Fig. 2.7 Polarization correlation for a maximally entangled state. The source is set to prepare a maximally entangled state. Red and blue dots refer to normalized measured coincidence number in ±45° and H/V basis. The visibility extracted from a sinusoidal fit is 99.1±0.3% in the ±45° basis, and 99.9±0.3% in the H/V basis. The vertical axis is normalized coincidence counts. The integration time to obtain each data point is 1 second.

a visibility V is the contrast of the maximum (M) and minimum (m) values of the coincidences (see Eq. 2.7).

Equation 2.8 describes a state where the polarization of the photon pairs is anti-correlated. Hence, if $\theta_{Alice} = 0°$, then the minimum (maximum) coincidences will occur at $\theta_{Bob} = 0°$ ($\theta_{Bob} = 45°$), and the corresponding visibility is refereed to as $V_{H/V}$ ($V_{\pm 45°}$).

The high visibility measured in H/V basis is expected since there is always one H polarized photon and one V polarized photon in each down-converted pair in our scheme. Therefore, evaluating the quality of entanglement requires visibility measurement in another basis, which should be orthogonal to the H/V basis on the Bloch sphere. The other basis used here is the ± 45 ° basis.

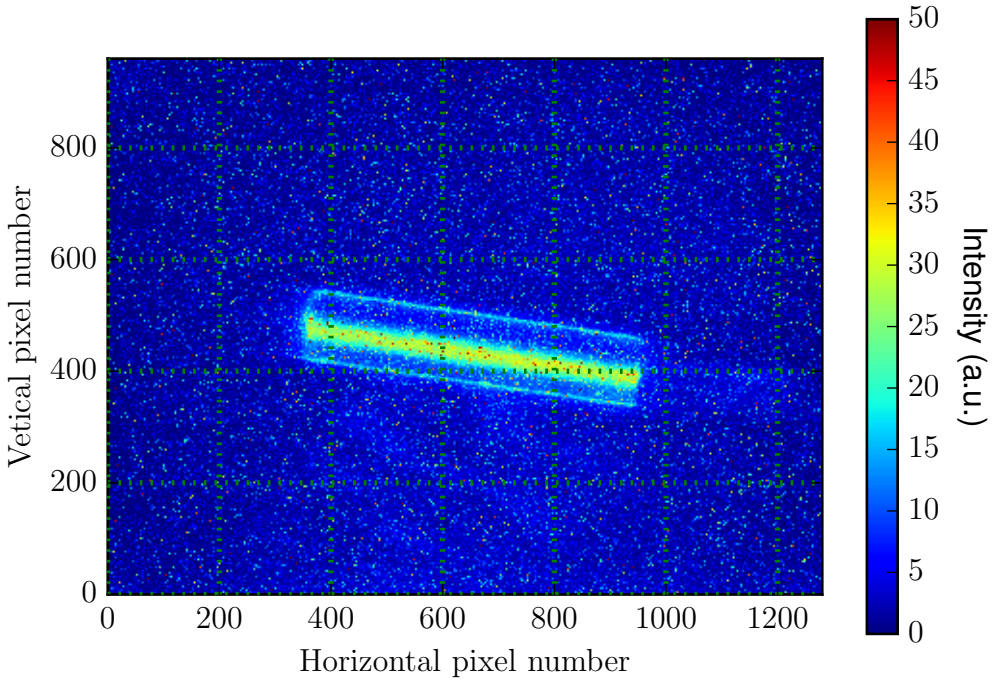


Fig. 2.8 Fluorescence of the PPKTP crystal recorded by a camera. Two 810 nm±10 nm interference filters (FF01-810/10-25) from Semrock filter block the pump photons. The transmission of these filters is more than 98% in the transmission window. We illuminate the crystal with a beam of ≈ 5 mW from a UV laser and integrate over 30 ms for this image.

Figure 2.7 shows the visibility measurement in both the H/V and the $\pm 45°$ basis. The polarization visibility in the $\pm 45°$ (H/V) basis, computed by fitting the coincidence number to a $\sin^2$ function, is 99.1±0.3% (99.9±0.3%).

2.2.4 Background events reduction

Background events not only reduce the heralding efficiency, but also increase the efficiency requirement to close the detection loophole [49]. There are three main background events sources: fluorescence photons from the source, ambient light from the environment, and electronic noise of the photon detectors (dark counts). Optical shielding the source and the single-photon detectors can remove most of the ambient photons. We first focus on studying the fluorescence from the source. The next section will briefly discuss the dark counts of the used single-photon detectors.

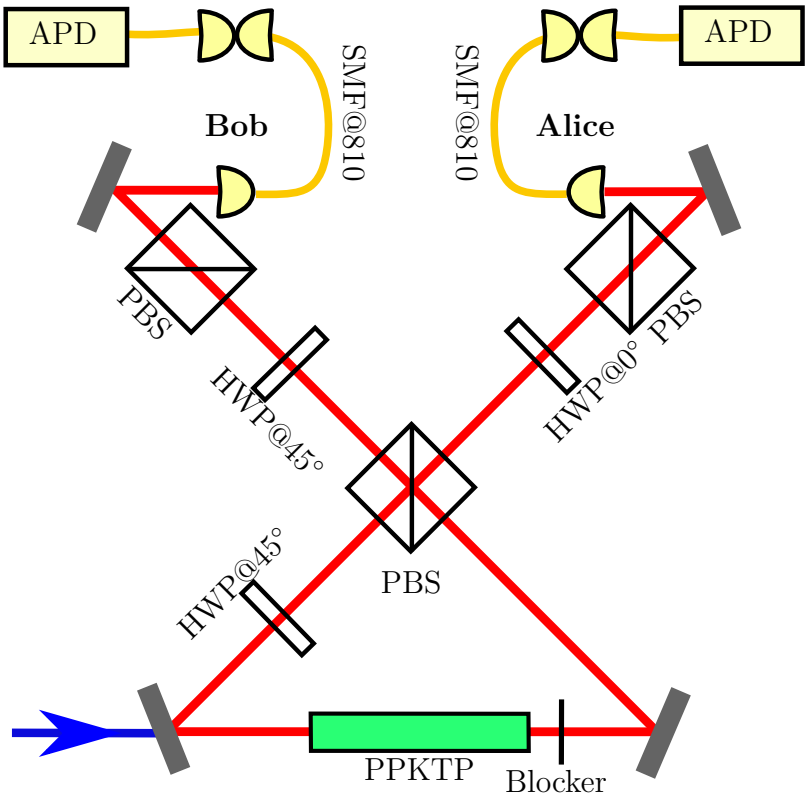
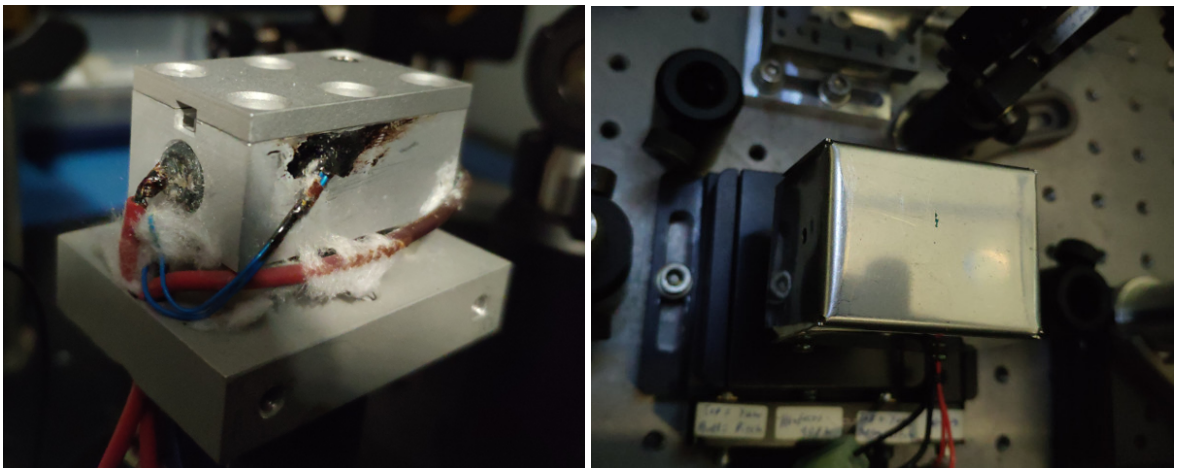


Fig. 2.9 Modified source setup to quantify the fluorescence. UV beam only pumps the PPKTP crystal from one direction and the down-converted pairs are blocked after the crystal. Both measurement bases are set optimal for collecting the backward direction fluorescence photons. We measure the photons coupled into the single mode fibers by two APDs.

UV light generates fluorescence in different materials. Despite many research efforts, the mechanism of the fluorescence generated by UV-pumped KTP crystals is not very clear yet [72]. Figure 2.8 shows an image of a PPKTP crystal illuminated with 5 mW of 405 nm laser light. We took this image through two interference band pass filters (center wavelength 810 nm, bandwidth 10 nm, Semrock) to suppress the light at 405 nm with 10^{-8} transmission. The brightness of the image does not significantly change with one or two filters: this indicates that the most intense scattering region in Fig. 2.8 is caused by fluorescence photons near 810 nm, and not by residual UV light scattered into the camera. Figure 2.8 was took with two filters and 30 ms integration time.

Figure 2.9 shows a modified source setup to quantify the fluorescence photons coupled into the collection fibers. The PPKTP crystal under investigation is only illuminated from one direction, and down-converted photons are blocked inside the Sagnac interferometer after the crystal. Only the photons emitted in the backward



(a) (b)

Fig. 2.10 Images of an oven with the crystal. Image (a) shows the oven with the crystal before putting in the source. There is a heating resistor under the crystal used to heat the crystal, and a thermistor besides the crystal used to measure the temperature. A feedback loop limits the heat speed under 1 degree/minute. Image (b) is the oven inside the source. The oven is insulated with rock wool to reduce the heat to influence the mechanical stability of the source. There is a metal case used to cover the oven.

direction can reach the PBS of the Sagnac interferometer. Both of the measurement bases are set for collecting the backward photons. The fluorescence photons are then coupled into the SMF@810 connected with APDs. The events registered at each detector (minus its dark-counts) constitute a measurement of the fluorescence, labeled as F_1 and F_2 respect to the detectors. The detected fluorescence on both detectors are similar, which suggests that fluorescence photons of the PPKTP crystal are unpolarized. We then remove the beam blocker and optimize the measurement basis for collecting down-converted photons at each detectors resulting in rates S_1 and S_2. By assuming the emission of the fluorescence is uniform in all spatial direction, the rate of fluorescence in the backward direction is equal to that of the direction co-propagating with the down-converted light. The fluorescence to signal ratio in each measurement party then can be defined as F_i / S_i, where i= 1 or 2.

The PPKTP crystal with 10 μm polling period (Raicol) is designed for 405 nm $\rightarrow$ 810 nm, degenerate type-II SPDC at room temperature [86]. The measured fluorescence to signal ratio for this crystal is around 5%. The supplier claimed that baking the crystal at high temperature could help to reduce the fluorescence. They believed that using the crystal in a high-humidity environment could degrade it.

We baked the crystal at 100 degree Celsius in a vacuum chamber for 120 hours. However, the fluorescence level of the crystal remained approximately the same after this baking. The baking temperature was further increased to 175 degree Celsius for another 120 hours. The measured fluorescence reduced from 5% to about 3.5%. Since baking at even higher temperature could damage the anti-reflection coating of the crystal, we could only increase the baking time. However, the measured fluorescence to signal ratio after the long time baking (2 weeks) almost remained the same.

With more than 3% noise photons, the required heralding efficiency to violate the Bell inequality without detection loophole is more than 85% according to Eberhard's theory [49]; this is almost impossible to achieve with current technology. It is necessary to find a method to reduce the fluorescence.

One popular theory about crystal fluorescence under UV light is that defects in the crystal may work as emission centers, and the spectrum of the fluorescence may change with the temperature [87–91]. To explore this option, PPKTP crystal with a 9.55 μm poling period were tried. This poling period is designed for 405 nm $\rightarrow$ 810 nm degenerated type-II SPDC process at 165 degree Celsius.

Figure 2.10 shows a simple oven used in this work to heat this crystal. A 9 Ω resistor under the crystal works as a heating source. A 1.46 MΩ@25° thermistor integrated inside the oven serves to measure the temperature. A feedback loop limits the heating speed to 1 degree/minutes. According to the manufacturer the anti-reflection coating of the crystal would peel off if the heating rate exceeds this rate. To reduce the overall heat generated by the oven, which may affect mechanical stability of the source, we insulate the oven with rock wool and cover it with a metal case. Figure 2.10 (b) shows a photo of the oven inside the source.

With the new high-temperature crystal, the fluorescence to signal ratio measured at both Alice's and Bob's sides are reduce to less than 0.2%.

2.3 High-efficiency photon detector

2.3.1 Transition edge sensor

In the above sections, the measurements and calibrations were carried out using APDs. However, to close the detection loophole, the required minimum efficiency is 66.7% [49]. The two APDs used in the calibration stage have 47.6% and 51.5% quantum efficiency. They had to be replaced by more efficient detectors.

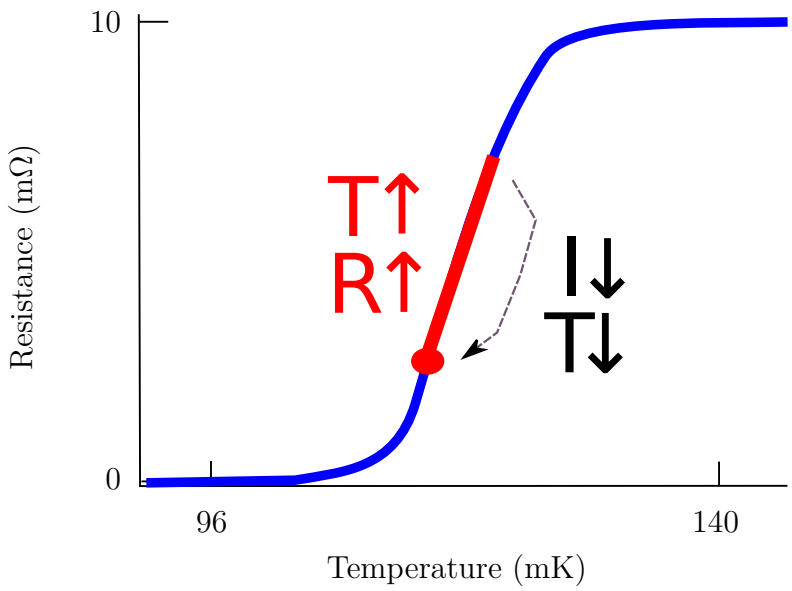


Fig. 2.11 Conceptual diagram of the change of TES resistance with temperature. By applying a voltage bias across the device, the TES could self-regulate at its operating point [92]. The temperature of the superconductor increases after receiving the thermal energy from a single photon. This causes the resistance of the superconductor to increase along the red path.

There are two types of photon detectors used in recently reported detection loophole-free Bell test [17, 18, 20, 26, 45, 60]: Superconducting Nanowire Single-Photon Detectors (SNSPD), and Transition-Edge Sensors(TES). Both of them are superconducting photon detectors. The highest measured detection efficiency for TES is more than 98% [29, 30]. However, there is no report on SNSPD shows more than 93% efficiency [24]. Although the SPSPD have a much smaller jitter time compared with TES, TES is better candidate for this work since the efficiency is more important in the detection loophole-free Bell test.

A TES consists of a superconducting film maintained near its critical temperature T_c such that the energy of a photon is enough to take it partly along the superconducting to normal phase transition [86] (see Fig. 2.14). The sudden increase in resistance can be detected electronically since the slope of the phase transition is very steep.

Sae Woo Nam's research group from NIST manufactured our TES for this work. A Bragg stack optimized for 810 nm allows the detector to have near-unit detection efficiency [29]. The energy of an infrared photon could only drive the TES to move along the transition edge in Fig. 2.14. If two photons arrive at the same time, they will drive the detector further along the transition phase. This means that the TES does not

have any intrinsic dead-time, and can resolve the number of monochromatic incident photons. The TES's photon number resolution property (up to thousands of photons) has been published on NIST's website [93]. My lab partner Jianwei demonstrated an approach to assign detection times to overlapping detection events in the regime of low signal-to-noise ratio by fitting to a heuristic model [94]. Jianwei also calibrated the TESs for this work.

We use an Adiabatic Demagnetization Refrigerator (ADR) cryostat [95, 96] to cool the detectors. There are two main cooling steps: (I) cooling the temperature to 2.5 K by a pulse tube cooler. (II) Using the adiabatic demagnetization of strongly paramagnetic salts brings the temperature of a cold finger (a copper rod supporting the detectors in their housing) to a minimum of 30 mK. This step only reduces the temperature once and slowly warms up after the cooling. It takes more than ten hours to warm up to more than 80 mK; this is called the hold time of our ADR. The critical temperature (T_c) of our TES is around 140 mK. The operating temperature of our TES is between 70-100 mK. Since the minimum temperature is 30 mK, a small magnetic field is applied to the salt pills (paramagnetic material thermal contact with cold finger) to increase the temperature of the TES. To maintain the operating temperature, a software PID control loop gradually decreases this magnetic field.

The optimal operating temperature with the best signal to noise ratio varies for each adiabatic demagnetization cooling process. Thus we have to find the optimal temperature after every cooling process.

Figure 2.12 shows the schematic of the TES readout circuit. We use a shunt resistor R_{shunt} to convert the constant current I_{TES} into a constant voltage bias across the TES. I_{TES} was supplied and controlled from outside the cryostat. After the TES absorbs a photon's energy, the increase of the TES's resistance causes more current flowing through the coil L_{in}.

We use a Superconducting Quantum Interference Device (SQUID) amplifier [97–99] to detect the small change in this current flow. The current flowing through the coil affects the magnetic field in the SQUID, and thereby the voltage drop across it. The signal is further amplified outside of the cryostat.

As mentioned before, my lab partner Jianwei invented a newly developed fitting method to identity TES pulse even if two successive TES signals traces are partially overlapping. However, we did not apply the fitting method here. This is because a long Bell measurement produces millions of TES traces. Post-processing these traces consumes massive computing power. Instead, we use a traditional Schmitt trigger mechanism [100], implemented by a simple two-level discriminator to measure the

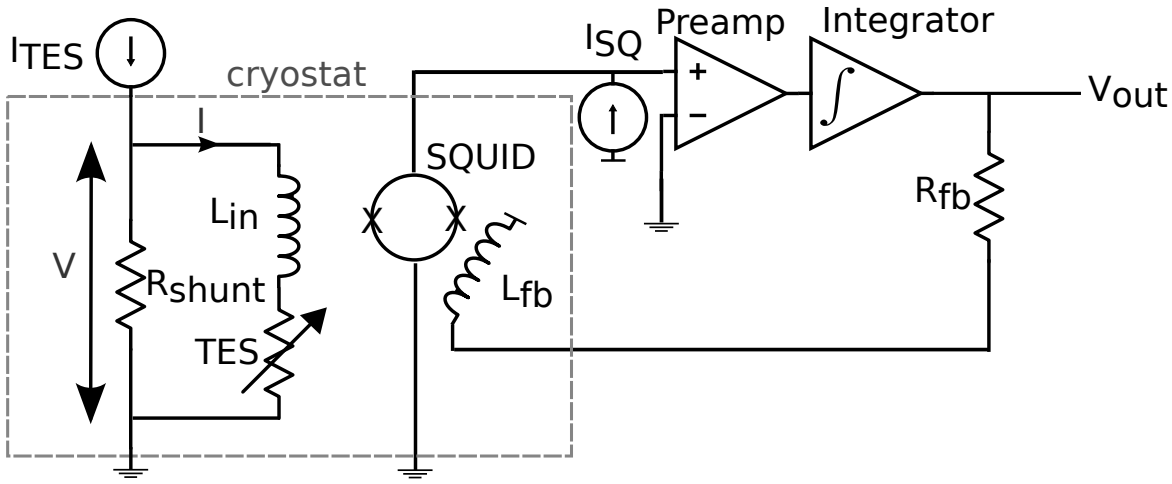


Fig. 2.12 Schematic of the TES readout circuit. The TES is voltage-biased by a constant current source I_{TES} through shunt resistor $R_{\mathrm{shunt}} \ll R_{\mathrm{TES}}$. The SQUID array amplifier picks up changes in TES resistance from L_{in}. The signal is further amplified outside of the cryostat. Signal feedback via R_{fb} and coil L_{fb} linearizes the SQUID response.

arrival time information of each photon. Figure 2.13 shows an example of how the discriminator works. A qualifier flag is raised when a signal exceeds a threshold V_{set}, and lowered by the first subsequently crossing of threshold V_{reset}. A time-stamp card records the time t_{set} as the arrival time of the photons. If there is another photon arrival between t_{set} and t_{reset} (the time of the signal subsequently crossing of threshold V_{reset}), Only the first event will be recorded. Thus, the two-level discriminator introduces around 1 μs artificial dead-time to the TES. The dead-time duration varies with the two threshold levels.

The following steps are used to find the optimal V_{set} for the rising edge of the TES signal. The reset threshold is fixed at a relatively low value. A counter records the detected event rate for different V_{set}. The count rate should decrease very quickly with the increase of the V_{set} at low voltage level due to the electronic noise of the TES. If the signal-to-noise ratio is high, at a certain threshold range, the count rate should stay approximately constant over a plateau.

Once V_{set} exceeds the minimal signal height caused by a real 810 nm photon, further increase in the V_{set} will reduce the registered count rate quickly. Figure 2.14 shows a sample of this relationship between the count rate and set threshold of the discriminator. We first vary the V_{set} after a cooling process to find the optimal threshold range for distinguishing n = 0 and n = 1 (grey area in Fig 2.14), then fine tune the $\mathrm{V_{set}}$ in this

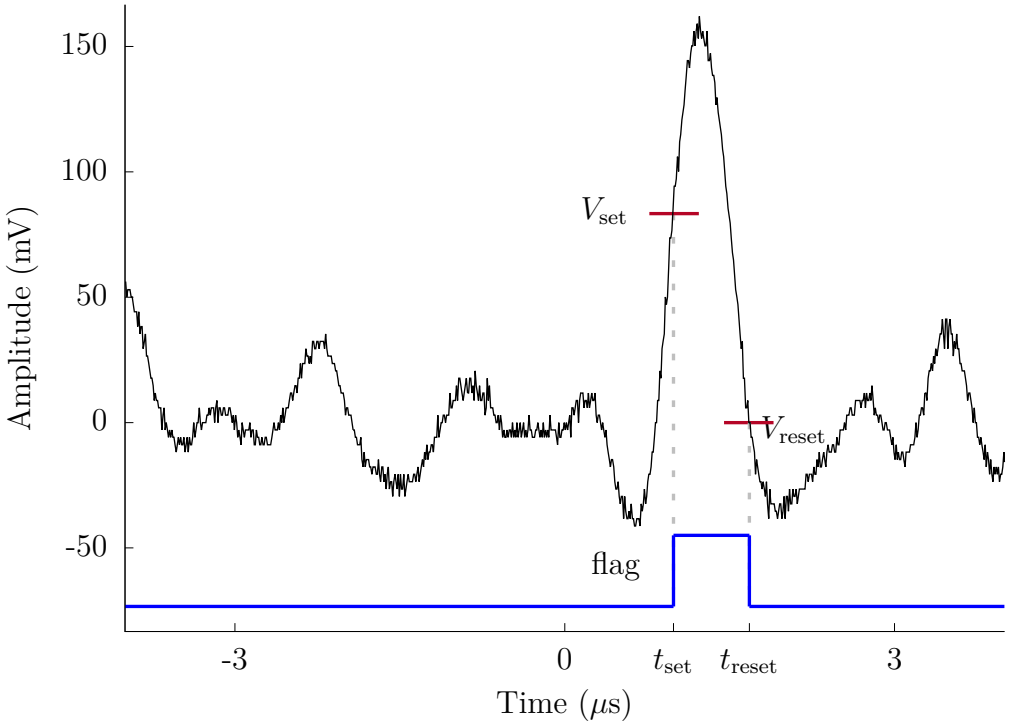


Fig. 2.13 Identification a photon in a trace with background noise by a traditional Schmitt trigger mechanism [100]. The implemented discriminators have two levels: a qualifier flag is raised when the signal passes threshold V_{set}, and lowered by the first subsequently crossing of threshold V_{reset}. We record the time t_{set} as the arrival time of the photons.

area with the pair source to find the voltage threshold with the best efficiency and low dark-count rate.

After the optimization, the highest efficiency is obtained with a dark count rate about $10\pm3\,s^{-1}$ for both detectors.

2.3.2 From source to detectors

This section introduces a few methods to couple the entangled photon pairs to the detectors. The TES manufactured by the NIST team is coupled with a single-mode fiber for 1550 nm (SMF-28e). However, the polarization-entangled photon pairs are coupled into SMF@810, which is single-mode for 810 nm. There are few methods to transfer photons between the two fibers. The simplest way is directly plugging the fiber connectors into a mating sleeve. Although the core-size of SMF-28e is bigger than

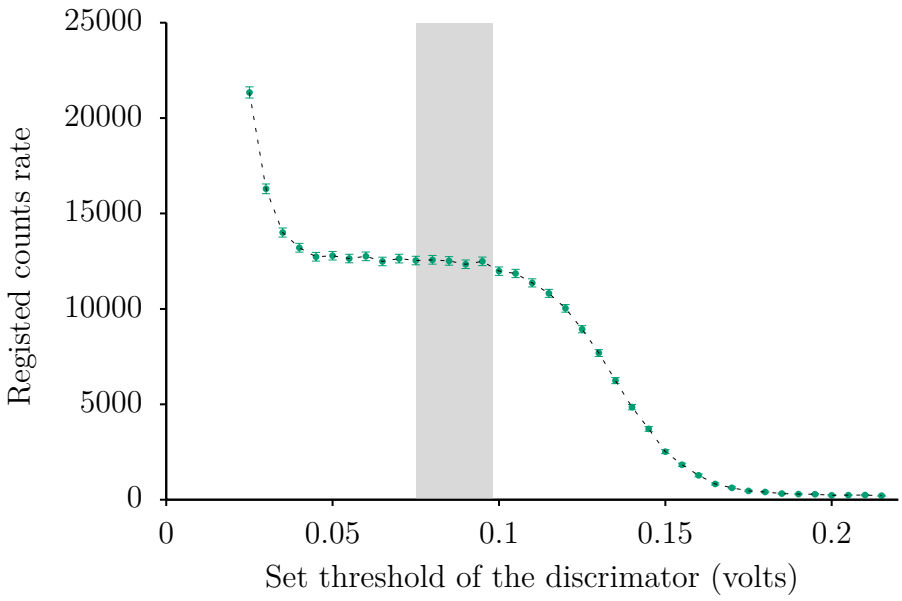


Fig. 2.14 Measured count rates as a function of the "set" voltage threshold V_{set} of the discriminator. The reset voltage threshold V_{reset} is fixed at relative low level (around 0). The integration time to obtain each points is one second. The gery area is where we fine tune the V_{reset} by measuring the pair source efficiency.

that of SMF@810, the measured transmission from SMF@810 to SMF-28e fiber with a mating sleeve is close to 90%.

The second method is using a free space link to couple the light into the SMF-28e, which is also the method used in this work. An aspheric lens (C230B, Thorlabs, f = 4.51 mm) collimates the emitted photons from a SMF@810 fiber connected to the source. Another aspheric lens is placed in front of the SMF-28e fiber to couple the 810 nm photons to TES. By carefully adjusting the pointing and the waist of the beam, we can achieve more than 95% transmission.

Even higher transmission can be achieved by directly splicing a SMF@810 and a SMF-28e fiber. The measured transmission by splicing is more than 96%. However, direct splicing does not allow the installation of active polarization devices between the source and the detectors, which helps to close to the locality loophole and may be implemented in the future. Figure 2.15 shows the full diagram of the experiment setup.

2.4 Detection efficiency measurement

Finally, with the high efficient transition-edge sensor, we could measure the detection efficiency of the pair source. Figure 2.16 (a) and (b) show the temporal cross correlation

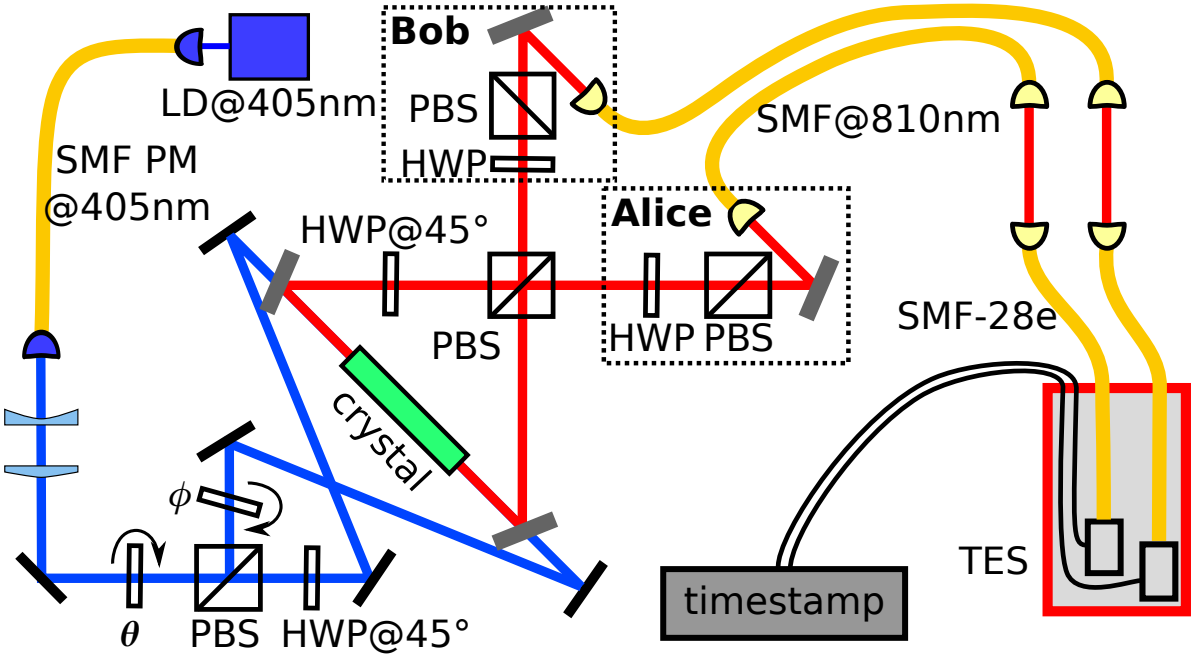


Fig. 2.15 Full Schematic of the experiment setup. The source is coupled with two TESs detectors through a free space link. The photons' time arrival information output from the TESs is recorded by a 2 ns resolution time-stamp card.

$G^{(2)}$ of photon pairs generated from different pump directions of the pair source. This function $G^{(2)}(\Delta t)$ is the probability that given the arrival time of one photon at one detector, another photon arriving at the other detector after a time Δt. A time-stamp card with 2 ns resolution records the arrival time information of the two detectors, which are labeled with t_1 and t_2. The number of coincidences p is identified by computing $G^{(2)}(\Delta t = t_1 - t_2)$, and integrating $G^{(2)}$ within a coincidence time window τ_c. A long cable is used to physically delay Bob's signal, which leads to the peak of the $G^{(2)}$ at 774 ns. Different from the heralding efficiency defined in Eq. 2.1, we correct the number of accidental coincidences n_{acc} by integrating $G^{(2)}$ over an accidental coincidence window τ_{acc} (in Fig. 2.16 $\tau_c = \tau_{acc}$ =700 ns). Thus, the expression of the heralding efficiency η becomes

$$\eta = \frac{p - n_{acc}}{\sqrt{S_1 \times S_2}}, \tag{2.9}$$

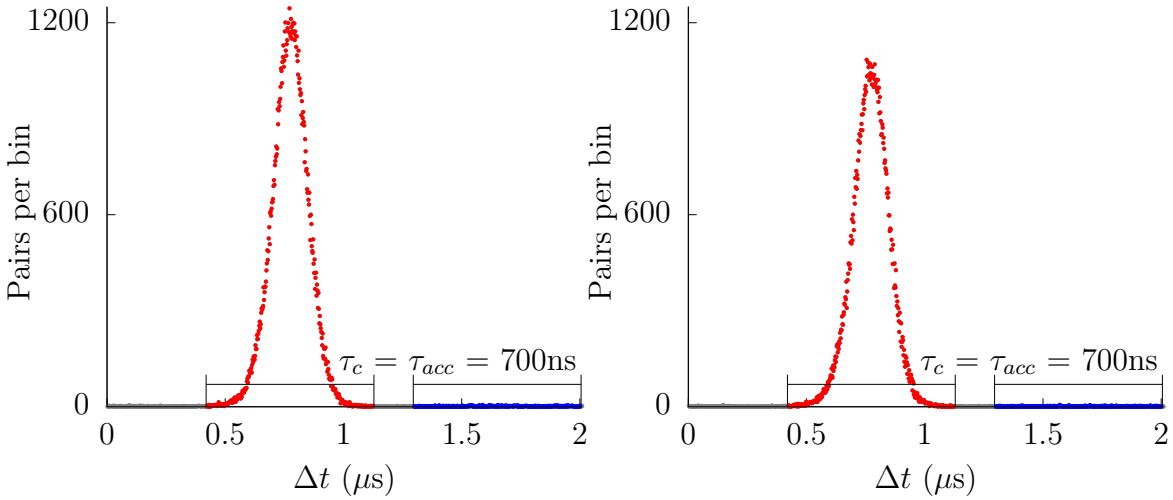


Fig. 2.16 The $G^{(2)}$ measured between two TESs connected to the high-efficiency source. Figure (a) and (b) are the $G^{(2)}$ of the photon pairs generated from different pump directions. The number of photon pairs measured for plotting each figures are more than 100 thousands. We calculate the coincidence rates p by integrating the data points (red color) over the coincidence window τ_{acc}, and the accidental coincidence pairs by integrating the data points (blue color) over the accidental coincidence window τ_{acc}, where $\tau_{acc} = \tau_c = 700$ ns. The corrected heralding efficiency for Fig. (a) and (b) are 83.01±0.30% and 82.04±0.31%.

where the S_1 and S_2 are registered number of detection counts from the respective detectors. We find a efficiency of 83.01±0.30% for one pump direction, and 82.04±0.31% for the other (Fig. 2.16).

Chapter 3

Detection loophole-free Bell test

This chapter shows an experimental violation of a Bell inequality without detection loophole using the setups described in the previous chapter.

The first section introduces a method which bins measurement time to define a round of an experimental Bell test using a continuous-wave (CW) pumped source. Based on this method, Section 3.1.2 describes a model used to calculate the S parameter of a CHSH-type Bell inequality [46].

We can optimize the violation with this model by varying the entanglement state, the measurement bases, and the time bin width. Section 3.2 introduces how the optimal entanglement state is experimentally prepared for the Bell test. The last section of this chapter shows the observed violation without fair-sampling assumption using this method.

3.1 Time binning method

3.1.1 Concept of the time binning

The Bell test is a statistical test that needs many repetitions. In each repetition, or so-called round, every measurement party produces an outcome. Most reported detection loophole-free Bell tests using photon pairs were performed with pulsed pumped SPDC sources, in which one measurement round can be naturally defined as one pump pulse duration [18, 20, 25, 26, 31]. However, the repetition rate of a pulsed SPDC source is limited by the repetition rate of the used pulse laser, which limits the random bits generation rate. Thus, we developed a new method to define a measurement round for a continuous-wave pumped source [101, 102].

Figure 3.1 shows an example of the photon-detection times recorded by Alice and Bob. The dots represent the photon detection events on each measurement party. We define measurement rounds by organizing the detection events into uniform time bins [1]. If a party's detector does not fire in a given round, that party labels the output as $+1$. On the contrary, when the detector fires, the outcome is labeled as -1. This convention allows only one detector per measurement party to be used [49, 17, 105].

Figure 3.2 illustrates this time binning method with a data sample, where the outcome $+1$ (-1) is simplified as $+$ $(-)$. For a two party system, there are four different outcomes: "+1+1", "+1−1", "−1+1", and "−1−1". The S parameter of a CHSH inequality is constructed by the correlation E of the different measurement bases (see Eq. 1.1). In Eq. 1.2, the correlation E is defined as the probability of the firing of detectors with the same label minus the probability of the firing of detectors with different labels. In a finite rounds experiment with the binning method, the estimated correlation E_{xy} can be written as

$$E_{xy} = \frac{N_{+1+1} + N_{-1-1} - N_{+1-1} - N_{-1+1}}{N}, \tag{3.1}$$

where $N_{\pm 1 \pm 1}$ represents the number of measured events with results corresponding to the respective sub-labels after N rounds of measurements. The index x and y refer to the measurement basis.

Since the bin width τ is independent of the detection time, τ can be considered as a degree of freedom in an experimental Bell test. Figure 3.3 illustrates that for a given detection timing sample, the correlation E can change with the binning time width τ. For $\tau = 20\,\mu$s, one finds that $E = -\frac{1}{9}$. For $\tau = 30\,\mu$s, the correlation has a value of $\frac{2}{3}$. The large τ reduces the contribution of a single pair to the correlation E.

3.1.2 Modeling the CHSH inequality with the binning method

This section presents a model based on the binning method to estimate the observed CHSH parameter S for continuous-wave pumped sources.

If the time bin width τ is much longer than the coherence time of the generated single photons, the average number of photon pairs per round, μ, of the CW-pumped SPDC source can be considered as an emission of independent pairs, distributed

[1] The binning is set independently of the detection time, thus, avoiding the coincidence loophole [103, 104]

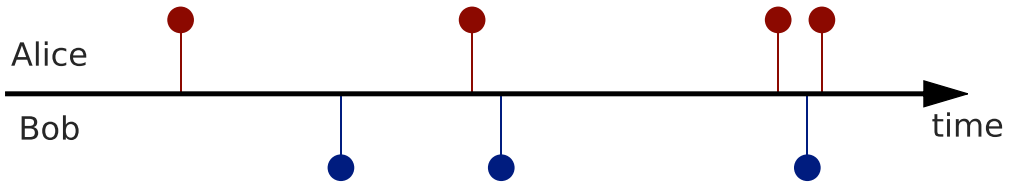


Fig. 3.1 Schematic of the registered photons for a CW pumped down-conversion source. Red (blue) dots represent Alice's (Bob's) detected photons.

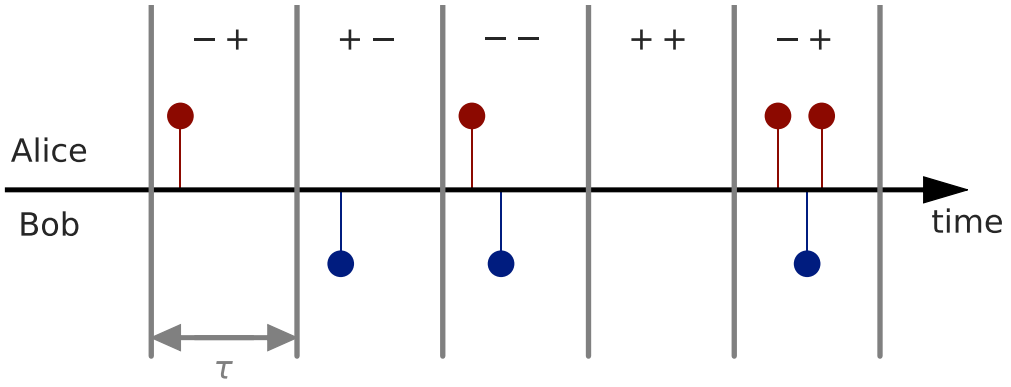
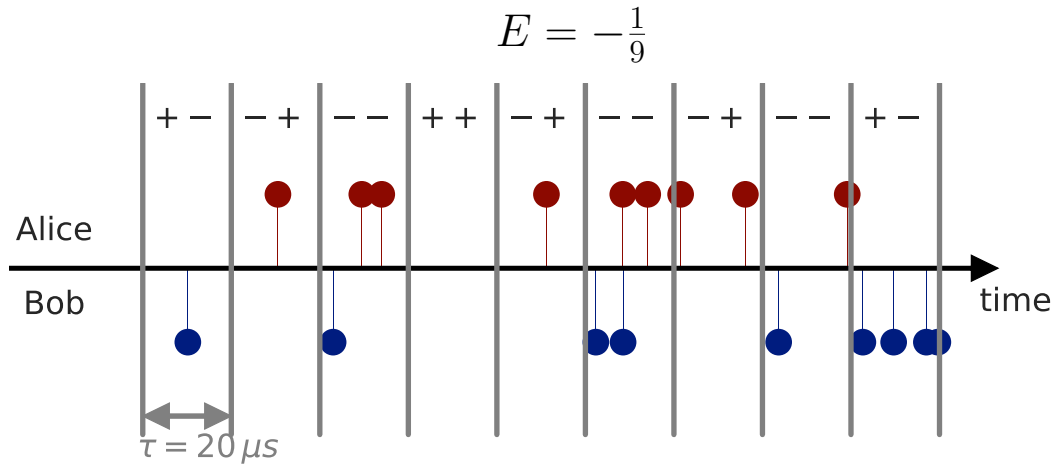
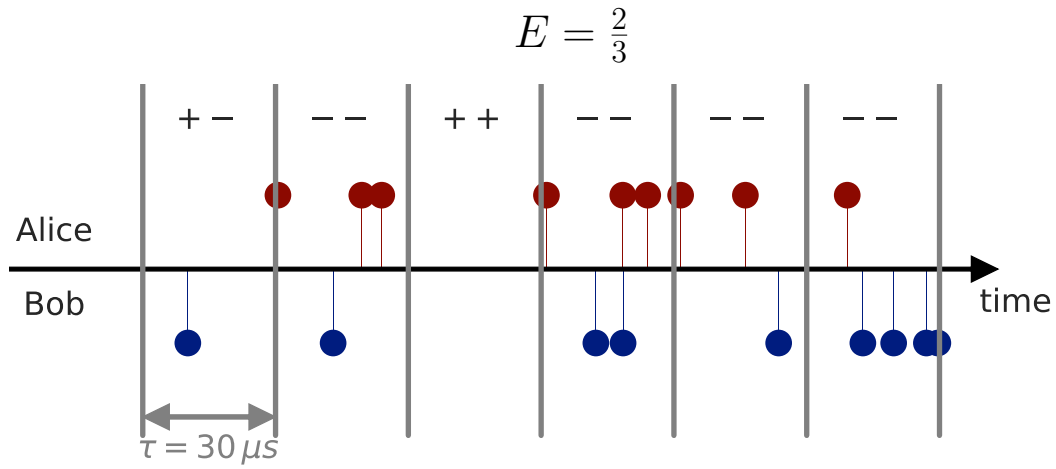


Fig. 3.2 Time-binning of the events into interval of length τ. For each detector, one uses -1 to label the outcome of having detected one or more photons, and $+1$ to label a round with on photodetection events. For a two measurement parties system, there are four outcomes: "+1+1", "+1−1", "−1+1", and "−1−1". One can use that to construct the correlation E_{xy} according to Eq. 3.1, where x and y refer to the settings of the measurement basis.



(a)



(b)

Fig. 3.3 Correlation E_{xy} of the same data sample changes with bin width. In Fig. (a), by setting the bin width at $20\,\mu$s, one finds that $E = -\frac{1}{9}$. In Fig. (b), $\tau = 30\,\mu$s, the correlation has a value of $\frac{2}{3}$.

according to Poissonian statistics. The mean number of detection events is $\mu = R{\cdot}\tau$, where R represents the photon pairs generation rate of the source.

Since the down-converted photon pairs are emitted independently, we can estimate the observed CHSH parameter S using the following steps. First, each pair is converted into classical information $(\alpha, \beta) \in \{+, -\}$ with probability

$$P_Q(\alpha, \beta|x, y) = \mathrm{Tr}(\rho \Pi_\alpha^x \otimes \Pi_\beta^y)\,, \tag{3.2}$$

where Π are measurement operators, and ρ is the density matrix of the measured quantum state. In this calculation, perfect detection is assumed. If some of the events have $\alpha = -$ ($\beta = -$), Alice's (Bob's) detector may be triggered, leading to the observed outcome $a = -1$ ($b = -1$). On the contrary, $\alpha = +$ ($\beta = +$) results in the outcome $a = +1$ ($b = +1$).

For the purpose of studying the violation of a CHSH-type Bell inequality, one can expand Eq. 1.1 as

$$E_{xy} = P(-1, -1|x, y) + P(+1, +1|x, y) - P(-1, +1|x, y) - P(+1, -1|x, y)\,. \tag{3.3}$$

According to the Kolmogorov axioms, $P(-1, -1|x, y)+P(+1, +1|x, y)+P(-1, +1|x, y)+P(+1, -1|x, y) = 1$ [106]. Thus, E_{xy} can be rewritten as

$$E_{xy} = 1 - 2P(-1, +1|x, y) - 2P(+1, -1|x, y)\,. \tag{3.4}$$

With the convention of outcomes, $P(-1, +1|x, y)$ is the probability associated with the case where Alice's detector fires and Bob's does not. Thus, Bob's detector should not be triggered by any photon from the pair source. Assuming a perfect detection efficiency for Alice, and Bob's detection efficiency is η_B, each pair contributes to $P(-1, +1|x, y)$ with

$$P_Q(-, +|x, y) + (1 - \eta_B)P_Q(-, -|x, y) =: D(-)\,. \tag{3.5}$$

Similarly, each pair contributes to $P(+1,+1|x,y)$ with

$$P_Q(+,+|x,y) + (1-\eta_B)P_Q(+,-|x,y) =: D(+)\,. \tag{3.6}$$

For a CW-pumped source, multiple pairs can fall into the same measurement round. For these v pairs , at least one of the α's must be $-$ to fire the detector. Thus, a configuration where k values of α are $-$ leads to $a=-1$ with probability $1-(1-\eta_A)^k$ (i.e. at least one $\alpha=-$ must trigger a detection). There can be $\binom{v}{k}$ such configurations. Thus, the v pair events contribute to $P(-1,+1|x,y)$

$$D_v = \sum_{k=1}^{v} \binom{v}{k} [1-(1-\eta_A)^k] D(-)^k D(+)^{v-k}\,. \tag{3.7}$$

Carrying out this summation leads to

$$P(-1,+1|x,y) = \sum_{v=0}^{\infty} P_\mu(v) D_v\,, \tag{3.8}$$

where the $P_\mu(v)$ is the possibility of v pair events calculated from a Poissonian pair distribution with an average of μ events per interval. The calculation of $P(+1,-1|x,y)$ is similar.

The above derivations do not take into account the background events, which will slightly modify each probability term in Eq. 3.4. Let us still consider $P(-1,+1|x,y)$ first. The background events that fall into Bob's empty bin reduce $P(-1,+1|x,y)$. However, the background events that fall into Alice's bins will not affect $P(-1,+1|x,y)$, since these time bins already contain detection events, and multiple detections still will be labeled as -1. Thus, one can rewrite $P(-1,+1|x,y)$ as

$$P(-1,+1|x,y) = \sum_{v=0}^{\infty} P_\mu(v) D_v e^{-\mu_b}, \tag{3.9}$$

where $e^{-\mu_b}$ is the probability of zero background event for each bin at Bob's side, calculated from the Poissonian distribution model with a expectation value μ_b.

Using the described model, one can numerically find the optimal state and measurement basis for the largest S value for a system with measured efficiency and background events. The optimal state and basis are not exactly the same as the case considering each round contains a photon pair [49]. However, these values are similar since the violation is mostly contributed by the single-pair events.

3.2 Preparation for performing the Bell test

3.2.1 Optimal state and measurement basis for our system

The optimal state depends on the detection efficiency and background rates [49]. However, both of them may change for different measured datasets. In this chapter, one dataset is used as an example to demonstrate a experimental Bell violation. The result based on this dataset was also reported in [101].

The photon pair generation rate of this dataset is around $2.4\times10^4\,\mathrm{s}^{-1}$. Alice and Bob have system detection efficiencies of 82.42%±0.31% and 82.24%±0.30%, the corresponding background rates are 45.7s±6.8 s^{-1} and 41.5±6.4 s^{-1}. With these values as inputs, we numerically found the optimal state and measurement bases for the highest violation using the described model,

$$|\psi\rangle = 0.900\,|HV\rangle + 0.437\,|VH\rangle\ . \tag{3.10}$$

The corresponding phase ϕ, and the angle θ for preparing this state in the format of Eq. 2.3 are 0° and -25.89°. For this state, the ratio of $|HV\rangle$ to $|VH\rangle$ photon pairs is equal to $\cot^2\theta = \cot^2(-25.89°) = 4.246$.

The optimal measurement bases calculated from our model are different from a standard Bell test (See Section 1.3). The four bases are α_0 = -7.2°, α_1 = 28.7°, β_0 = 82.7°, and β_1 =-61.5°.

3.2.2 Optimizing and stabilizing the phase ϕ

For the source presented in this thesis, the tilt of a motorized thin glass placed in one pump mode controls the phase ϕ. The procedure to optimize and stabilize the phase ϕ can be described by the following steps.

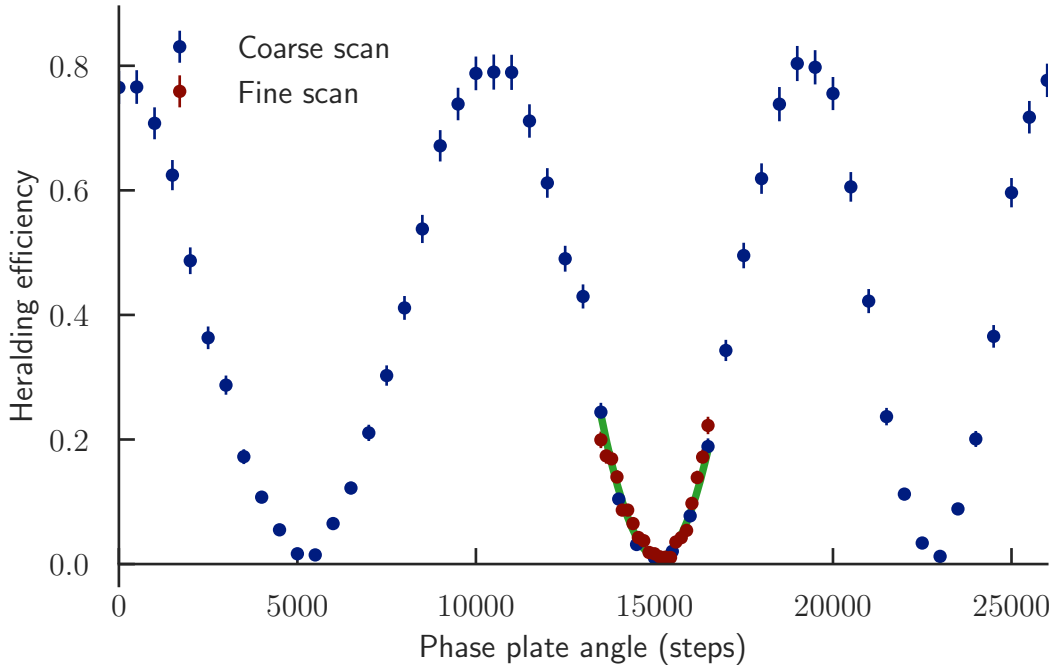


Fig. 3.4 Tilting the phase plate to minimize the phase ϕ. In this measurement, both Alice and Bob's set their HWPs at 22.5° (DD basis). We first move the phase plate in coarse steps to find the approximate position of the minimum, and then in fine steps near that position.

1. Balance the beam power of the two pump directions, and set both Alice's and Bob's HWP at 22.5° (called DD basis)[2].

2. Move the phase plate in coarse steps, and record the heralding efficiency values. Then, find the approximate optimal position where the efficiency is the lowest (blue points in Fig. 3.4).

3. Move the phase plate in fine steps near the position found in Step 2, and record the heralding efficiency. Then fit the corresponding efficiency values into a quadratic model to find the optimal phase plate position (red points in Fig. 3.4).

4. Measure the visibility in ±45° basis (see Fig. 2.7) with the optimal phase plate position found in Step 3.

[2]If the pump power of the two pump directions is the same and $\phi = 0$, the state generated by the source is a one of the maximally entangled state described by Eq. 2.8, where the polarization of the two photons should be anti-correlated in any measurement basis. Thus, the lower the efficiency measured in the DD basis, the closer the phase ϕ is to 0.

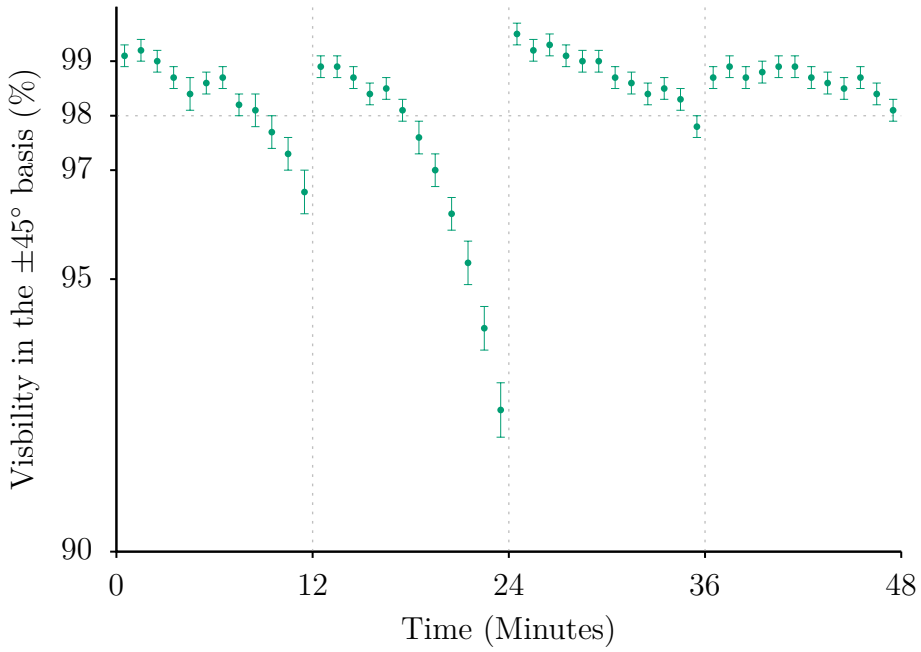


Fig. 3.5 Visibility measurement over time for testing the stability of the phase ϕ. We measure the visibility in the $\pm 45°$ basis every minute to find the data acquisition time duration of the Bell test after optimizing the phase plate. The phase ϕ is adjusted every 12 minutes.

5. If the measured visibility is more than 98.5%, start data acquisition for the Bell test. Otherwise, repeat Step 3.

6. After 6 minutes of data acquisition, repeat Step 3 to ensure that the phase ϕ is always close to 0.

Small drifts in the setup, e.g. temperature changes of the source leads to a slow phase drift over time, which requires the Step 6 to be performed. Figure 3.5 shows a visibility measurement in $\pm 45°$ basis over a period of 12 minutes. A phase optimization process is conducted before each period. This figure indicates that the phase stable time varies between optimization processes. To ensure that the source always generates a near optimal state, we repeat the optimization process every 6 minutes during the data acquisition.

3.2.3 Optimizing the angle θ

After minimizing the phase ϕ, we also need to accurately set the angle θ, which is determined by the relative pump power between the two pump directions. The rotation

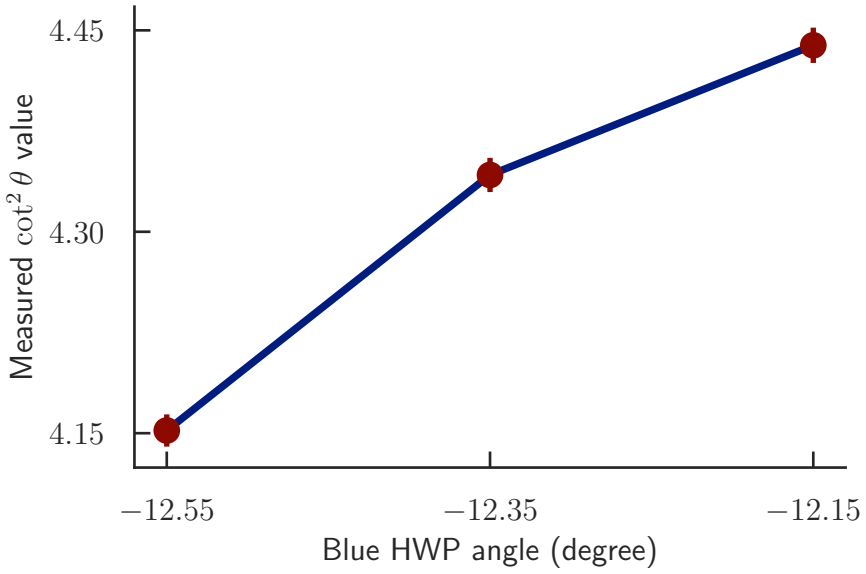
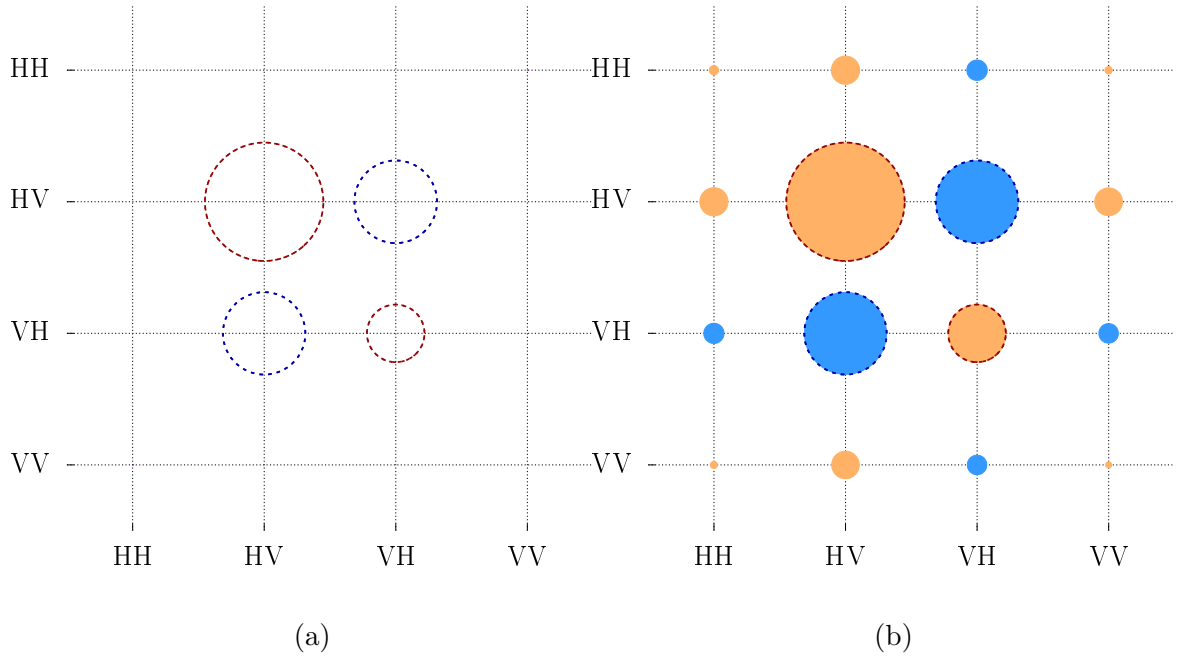


Fig. 3.6 Ratio of the number of detected photon pairs between different pump directions versus the angle of the HWP θ_B. The angle θ of the generated entanglement state is controlled by rotating the HWP after the 405 nm telescope. The value $\cot^2\theta$ is equal to the ratio of $|HV\rangle$ photon pairs rate to $|VH\rangle$ photon pairs rate. The optimal θ for our system is -25.89°, corresponding to $\cot^2\theta = 4.246$.

of a HWP (labeled as blue HWP) before the PBS that splits the pump beam to controls the relative power. We calibrated the angle of the blue HWP θ_B by measuring the power at the transmission port of the blue PBS, where the θ_B with maximum transmission is labeled as 0°. The unbalanced transmission and reflection of the PBS, together with the scattering loss of the thin glass phase plate causes a difference in the value of $\cot^2(2\theta_{HWP})$ and the ratio of the beam power between the two pump modes. Therefore, $2\theta_B \neq \theta$.

Equation 2.3 shows that the ratio of the $|HV\rangle$ photon pairs rate to the $|VH\rangle$ photon pairs rate is equal to $\cot^2\theta$. For the calculated optimal state, θ = -25.89°, and $\cot^2\theta = 4.246$. Similar to the phase optimization process, we optimize the θ_B in coarse and fine steps. Figure 3.6 shows the measurement result in 3 fine steps (within 0.4°).

The source is only connected to two TESs measuring the photons at the transmission port of the PBSs in the collection arms, which means that we cannot measure the number of $|HV\rangle$ and $|VH\rangle$ photon pairs at the same time. Since our pump power fluctuates around 10% every few minutes, the value of $\cot^2\theta$ measured by performing a long measurement in $|HV\rangle$ basis, followed by a switch to the $|VH\rangle$ basis, is not accurate, unless an extra pump power measurement is used to normalize the measured



(a) (b)

Fig. 3.7 Tomography of the optimal non-maximally entangled state. The tomography measurement is performed with four bases on the equator of the Bloch sphere (H, V, D, A) on each party. Thus, the measurement result is mapped to a state only have really part (assume the imaginary party is 0). Figure (a) is the theoretical optimal state for our system, and Figure (b) shows the state diverted from tomography measurement. The calculated fidelity is 99.15%.

photon pairs in different bases. Since the monitoring of the pump power requires extra optics, which reduces the pump power and affects the beam profile, we use a more direct method involving multiple measurements of the $\cot^2\theta$ performed over short time scales. In Fig. 3.4, each data point is derived from 15 measurements of $\cot^2\theta$. For each measurement, both the number of $|HV\rangle$ and $|VH\rangle$ photon pairs are recorded with 2 seconds of integration time. A simple linear model is applied to interpret the value of the θ_B^{opt} leading to $\cot^2\theta = 4.246$. The estimated θ_B^{opt} for Fig. 3.4 is $-12.45°$.

After optimizing θ and ϕ, we use a tomography measurement to verify that the state generated by the source is close to the calculated optimal state [107–109]. To perform a complete tomography measurement on a two qubits state, each measurement party should have at least one HWP and one QWP. However, for the reported source, there is no extra space to insert a QWP in each collection arm. For each party, the tomography measurement thus is performed only on the four bases on the equator of the Bloch sphere (H, V, D, A). Consequently, we reconstruct the measured result into

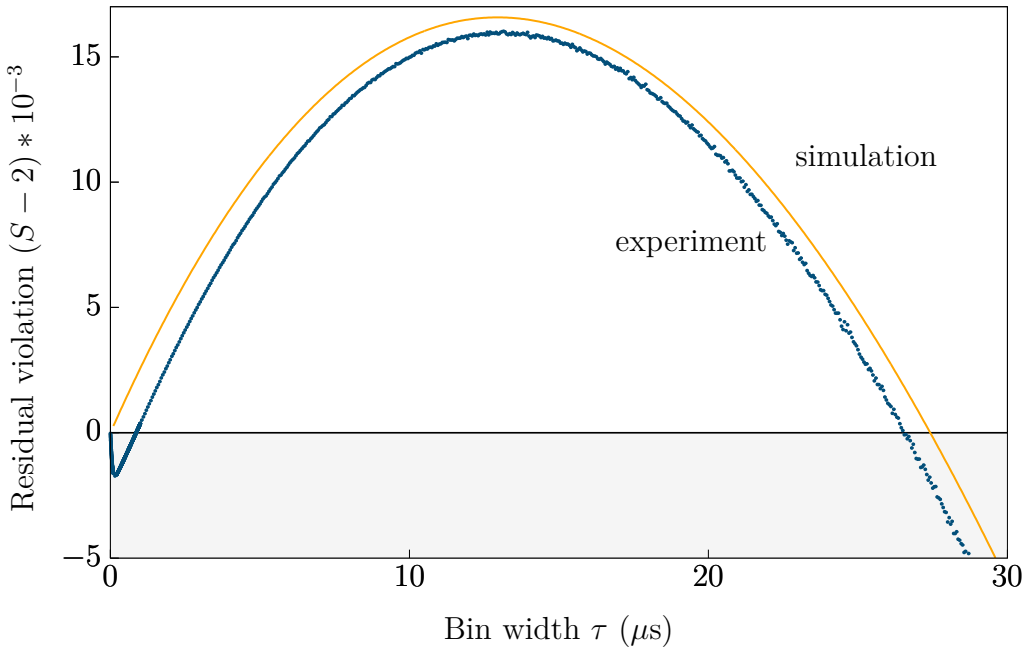


Fig. 3.8 Measured CHSH violation as a function of bin width τ (blue circles). The continuous orange line represents the numerical output of the theoretical model described in the previous section. Both the simulation and experimental data show a violation for certain bin widths. The uncertainty on the measured value, calculated assuming i.i.d., corresponding to one standard deviation due to a Poissonian distribution of the events, is smaller than the symbols. At small bin widths (left corner), the detection jitter ($\approx$ 170 ns) of the used TESs is comparable with the time bin width, resulting in a loss of observable correlation and a fast drop of the S value.

a density matrix where the elements are all real-values (see Fig. 3.7 (b)), then compare the reconstructed state with the calculated optimal state, which is graphically shown in Fig. 3.7 (a). The measured fidelity is 99.15±0.18% [110].

3.3 Experimental violation of Bell inequality

3.3.1 Experimental Bell violation with CW source

This section presents an experimental Bell violation using the binning method with our continuous-wave pumped source.

Figure 3.8 shows that the result of processing the timestamped events for different bin widths τ. The largest violation $S = 2.01602(32)$ occurs at bin width $\tau = 13.150$ μs, which, with the cited pair generation rate of $24 \times 10^3\,\mathrm{s}^{-1}$ and corresponds to an average

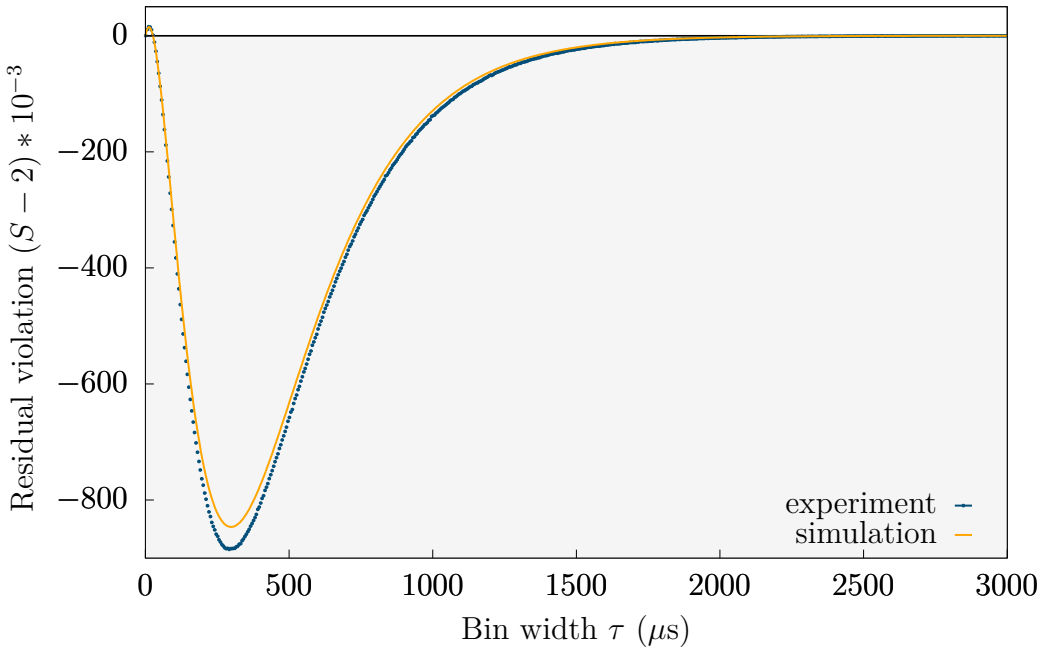
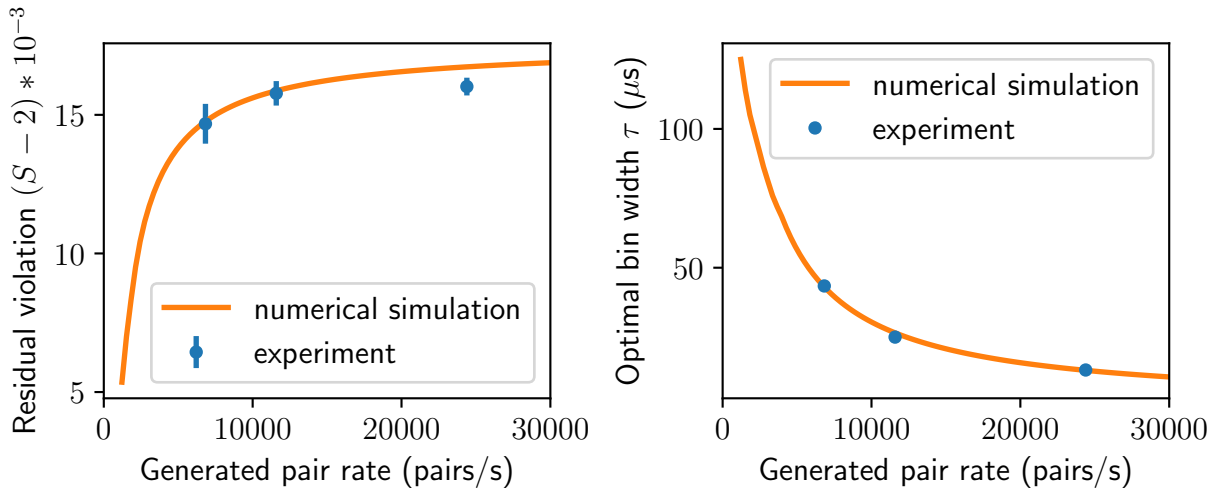


Fig. 3.9 Measured CHSH violation as a function of bin width τ with extended bin width range (blue circles). A theoretical model (orange continuous line) is described in previous section. Both the simulation and experimental data only show a violation at short bin width range. The S value continuously decreases with the increase of τ after it drops below 2 as expected from the simulation. At a certain point, the S value starts to increase with the bin width and ends up close to 2.

number of pairs per round $\mu \approx 0.32$. This number is very close to the theoretic value $\mu = 0.322$ calculated from our model. The uncertainty is calculated with the assumption that the measurement results are independent and identically distributed (i.i.d.) [111, 112].

The non-ideal visibility of the state generated by the photon pair source contributes to a slight discrepancy between the experimental violation and the simulation. Figure 3.8 exhibits that there is no violation when the bin width is very small. This is because that the detection events of pairs are assigned to different rounds when τ is comparable to the detection jitter, decreasing the correlation. This feature is not captured in the simulation, which does not include the jitter time as a parameter.

Figure 3.8 only displays a small range for bin width τ. For longer widths (see Fig. 3.9), the CHSH parameter S continuously decreases with the increase of τ after it drops below 2 as expected from the simulation. For $\mu \gg 1$, almost every time bin will be filled with registered photons, labeled as -1, leading to $P(+1, -1|x, y)$,



(a) (b)

Fig. 3.10 (a) Measured maximal CHSH violation for each dataset versus their pair rates (blue circles). A theoretical model is described by the orange line. A higher pair generation rate results in a higher violation because of better signal to noise ratio (constant detector's intrinsic dark count). (b) Optimal bin width versus different pair rates (blue circles). The orange continuous line represents the theoretical values calculated based on our model. In general, a high pair rate requires a short bin width to ensure that there are enough single-pair events to violate the Bell inequality.

$P(-1,+1|x,y)$, and $P(+1,+1|x,y) \approx 0$, but $P(-1,-1|x,y) \approx 1$. Thus, E values in all measurement bases are close to 1, and the S value increases to ≈ 2.

3.3.2 Violation with different rates

The largest violation that can be obtained from an experimental system is related to both the heralding efficiency and signal to noise ratio. In the present experiment, the detector's intrinsic dark-count, ambient light, and fluorescence from the UV pumped PPKTP crystal contribute to the noise. Although the ratio of the fluorescence photons to down-converted photons is fixed for different pump powers, the detectors' dark-count and ambient photons are constant regardless of the rate of down-converted photons. Therefore, the signal to noise ratio increases with the photon pair generation rate. Figure 3.10 (a) shows the largest violation with different pair rates. The orange line represents the numerical simulation result with a constant dark-count rate from the detectors, assuming the ratio of the fluorescence photon to down-converted photon is 0.135%. As described in Chapter 2, the two-level discriminator, which identifies the photon signal from the TESs' traces, introduces an artificial dead-time to the detectors.

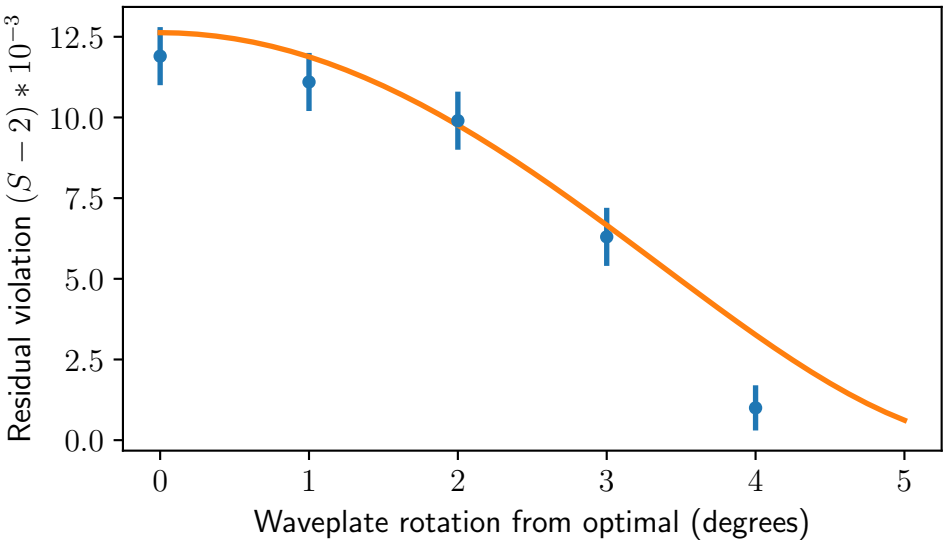


Fig. 3.11 The largest CHSH violation as a function of the angular offset of Alice's HWP from the projection angle α_0 (blue circles). The orange line represents the theoretical value calculated by our model. During this measurement, the overall system efficiency was about 81%. Thus, with zero offset, the S value is ≈ 2.012. This figure shows that our experimental system is able to violate the Bell inequality with the HWP offset of 4 degrees. The difference between the simulation and the experimental violation measured at 4 degrees angular offset is mainly due to the efficiency drift of the source.

The higher the pair rate, the greater the fraction of photons that fall into the dead-time, resulting in a slight reduction of the heralding efficiency. The simulation has not taken into account this effect. Thus, in Fig.3.10, observed violations are closer to those of the simulation when the pair rates are low.

Figure 3.10 (b) shows the optimal bin width τ as a function of the pair rates. If there is no background event, the optimal average number of pairs per round μ is constant (1/e) according to the model described in section 3.1.2. Therefore, the optimal bin width τ should decrease with the increase of the pair rate. Although the background events slightly modify the optimal μ, the optimal bin width τ still follows the similar trend.

3.3.3 Violation with sub-optimal setting

This section report experimental violations with the sub-optimal setting to show the robustness of our experimental system against a large angular offset on one measurement basis. The x-axis of Fig. 3.11 represents the angular offset of Alice's HWP from the projection angle α_0; the corresponding offset angle on the Bloch sphere is four times

of this value. For this measurement, the overall system efficiency was about 81%. Thus, the maximum violation S at zero offset is about 2.012. Even with that, the experimental system presented in this thesis can still tolerate the HWP angle offset of 4 degrees. The violation with 4 degrees offset in Fig. 3.11 fails to match the simulation curve, since the system efficiency drop at the end of the measurement. The effect of the offset on other measurement bases is similar.

The robustness against a large angular offset indicates that our experimental setup can violate the Bell inequality with faster polarization rotation apparatus, like Pockel cells, which cannot set the measurement basis as accurately as a HWP connected to a motor due to electric noise and acoustic ringing [113, 114].

Chapter 4

Device-Independent randomness extraction

The experimental Bell violation shown in the previous chapter indicates that the measurement outcome of our system is only determined at the time of measurement. It is impossible for the adversary (Eve) to predict the outcome with complete confidence. In another words, our system can be used to generate certified private randomness [12].

The amount of extractable certified private randomness depends on how accurately Eve can guess the measurement outcome. Any extraction procedure, at most, preserves the amount of randomness in the measurement outcome [33]. Thus, for N bits generated from an experiment, the length m of the extracted binary string must be bounded by the requirement that $P_{guess}(N) \leq P_{guess}(m)$, where the label P_{guess} represents the best guessing probability of Eve. In the ideal case, one should have $P_{guess}(m) = 2^{-m}$ after the extraction. Therefore,

$$m \leq -\log_2 P_{guess}(N) =: H_{\min}(X|E), \tag{4.1}$$

which is also the definition of the conditional min-entropy [33], where X represents the measurement outcomes, and E stands for Eve and her knowledge about the measurement.

For a device-independent randomness extraction, the guessing probability is only related to the observed violation of the Bell test. The higher the violation, the lesser information Eve has about the measurement outcome, which leads to a lower guessing probability.

4.1 Quantum random number expansion protocol

In order to turn the experimental outcomes into uniformly random bits, we need to employ a randomness expansion protocol, and apply a randomness extractor [115, 116]. This section briefly introduces the protocol used in this work, and its security proof. The details of the protocol and mathematical derivations can be found in [101, 115, 116]. Le Phuc Thinh, Jean-Daniel Bancal, and Alessandro Cerè all have made huge contributions towards choosing the protocol and implementing the extraction in this work [101].

It will be more convenient to adopt the notations and labels used in [115] to explain the details since we follow the protocol presented in that paper. The outcomes are labeled as $a, b \in \{0, 1\}$ (instead of $a, b \in \{+1, -1\}$ in the previous chapter), and language of nonlocal games with winning condition is used. The game winning probability w is then equal to $1/2 + S/8$ in terms of the CHSH value, where

$$w_{\text{CHSH}}(a, b, x, y) = \begin{cases} 1 & \text{if } a \oplus b = x \cdot y\,, \\ 0 & \text{otherwise}\,. \end{cases} \tag{4.2}$$

The maximal winning probability of a classical strategy is 0.75, while the optimal quantum strategy can achieve a winning probability of $(2 + \sqrt{2})/4 \approx 0.85$.

A randomness expansion protocol is a procedure that consumes r bits of randomness, and generates m bits of almost uniform randomness, formally, called a (ϵ_c, ϵ_s)-secure $r \to m$ randomness expansion protocol. Both (ϵ_c, ϵ_s) are set by the user of the protocol, where ϵ_s is the parameter for "soundness"; it controls the bounding randomness security.

In the ideal case, the state of the input ρ_{U_r} and output ρ_{U_m} should be completely mixed on appropriate registers. They should also be completely uncorrelated to Eve's system ρ_E. Thus, one can write the ideal state of the combined system as a tensor product:

$$\rho_{ideal} = \rho_{U_m} \otimes \rho_{U_r} \otimes \rho_E. \tag{4.3}$$

The soundness is defined as follows: in the implementation, the user either aborts or returns an m-bit string $Z \in \{0,1\}^m$ with:

$$(1 - \Pr[\text{abort}])\|\rho_{ZRE} - \rho_{ideal}\|_1 \leq \epsilon_{\text{s}}\,, \tag{4.4}$$

where the $(1 - \Pr[\text{abort}])$ is the probability of returning the output random bits, and $\|\rho_{ZRE} - \rho_{ideal}\|_1$ is the distance between the real state ρ_{ZRE} of the combined system and the ideal state $\rho_{U_m} \otimes \rho_{U_r} \otimes \rho_E$. The user gains a chance to implement the protocol only if the distance is close to the soundness parameter ϵ_{s}. Therefore, the smaller the ϵ_{s}, the more secure the bounding randomness.

Another very important security parameter for a randomness protocol is completeness ϵ_{c}, which ensures that the user makes an honest implementation. In other words, the completeness parameter makes sure that the user not always abort the measurement data for post-selection. The completeness parameter is defined as: there exists an honest implementation with

$$\Pr[\text{abort}] \leq \epsilon_{\text{c}}. \tag{4.5}$$

The concept of the honest implementation can be understood more easily after the procedure of implementing the protocol has been introduced.

The protocol used in this work takes a few parameters: expected fraction of test rounds γ , expected winning probability for an honest implementation ω_{exp} , width of the statistical confidence interval for the estimation test δ_{est}, and the overall measurement rounds or so-called block size of the protocol n. In an experimental realization, for every round $i \in \{1, \ldots, n\}$:

- Bob chooses a random bit $T_i \in \{0,1\}$ such that $\Pr(T_i = 1) = \gamma$ using the interval algorithm [117].
- If $T_i = 0$ (randomness generation), Alice and Bob deterministically choose $(X_i, Y_i) = (0,0)$. Otherwise, when $T_i = 1$ (test round) they choose uniformly random inputs (X_i, Y_i).
- Alice and Bob use the physical devices with the inputs (X_i, Y_i) and record their outputs (A_i, B_i).

- If $T_i = 1$, they compute

$$C_i = w_{\text{CHSH}}(A_i, B_i, X_i, Y_i)\,. \tag{4.6}$$

The user aborts the protocol if $\sum_j C_j < (\omega_{\text{exp}}\gamma - \delta_{\text{est}})n$, where j is the index of test rounds, otherwise he/she returns $\text{Ext}(\mathbf{AB}, \mathbf{Z})$, where Ext is a randomness extractor, $\mathbf{AB} = A_1B_1...A_nB_n$, and $\mathbf{Z}$ represents uniformly random seeds. According to the theory described in [115], the probability that the randomness expansion protocol aborts for an honest implementation is

$$\Pr[\text{abort}] \leq \exp\Big(-2n\delta_{\text{est}}^2\Big) =: \epsilon_{\text{est}}\,. \tag{4.7}$$

From the above derivation, it is not difficult to see that an honest implementation ensures that the user does not overestimate the ω_{exp} from the test rounds. Equation 4.7 also constitutes a definition of the error tolerance of the Bell violation estimation ϵ_{est}. The distribution of the string T_i is not uniform unless $\gamma = 1/2$. Thus, an interval algorithm [117] is used to produce the T_i from a uniformly distributed random number source. According to [115], by consuming $6h(\gamma)n$ uniformly random bits (h is the binary entropy function[1]), this algorithm either aborts with a probability of at most

$$\epsilon_{\text{SA}} = \exp\Big(-18h(\gamma)^3 n/\max\{\log\gamma^{-1}, \log(1-\gamma)^{-1}\}\Big) \tag{4.8}$$

or outputs n bits $T_1, \ldots, T_n$; this random bits distribution is within statistical distance of at most ϵ_{SA} to n i.i.d. Bernoulli(γ) random variables. This raises both the completeness and soundness parameters of the final protocol by ϵ_{SA}. Therefore, $\epsilon_{\text{SA}} + \epsilon_{\text{est}}$ bound the total completeness.

The used protocol ensures that for any $\epsilon_{\text{EA}}, \epsilon' \in (0, 1)$, where ϵ_{EA} is the soundness of the protocol, and ϵ' is called a smoothing parameter, either the protocol aborts with

[1] $h(p) := -p\,\log_2 p - (1-p)\log_2(1-p)$

probability greater than $(1-\epsilon_{\mathrm{EA}})$ or, output n bits with

$$H_{\min}^{\epsilon'}(\mathbf{AB}|\mathbf{XYT}E)_{\rho_{|\mathrm{pass}}} > n\cdot\eta_{\mathrm{opt}}(\epsilon',\epsilon_{\mathrm{EA}})\,, \tag{4.9}$$

where $H_{\min}^{\epsilon'}(\mathbf{AB}|\mathbf{XYT}E)$ is the smooth min-entropy of the experimental output AB after this protocol is applied. This used protocol does not assume i.i.d..

The expression for $\eta_{\mathrm{opt}}(\epsilon',\epsilon_{\mathrm{EA}})$ was worked out in [101, 115] and included[2] here for convenience. Equation 4.9 shows that the experiment outputs AB have at least $n\cdot\eta_{\mathrm{opt}}(\epsilon',\epsilon_{\mathrm{EA}})$ entropy. Together with Eq. 4.1, one can roughly estimate the amount of extractable random bits.

To analyze the soundness of the entire extraction procedure, one also needs to take into account the effect of the used extractor, named the Trevisan extractor [116]; it is a seed length efficient extractor, and secures against quantum adversary with quantum side information. This extractor [3] takes $2n$ binary outcomes from the experimental setup of the Bell test and d binary random bit seeds as inputs, then outputs m binary random bits ($\{0,1\}^{2n}\times\{0,1\}^{d}\to\{0,1\}^{m}$), where $d=a(2\ell)^2$. If

$$H_{\min}(\mathbf{AB}|E)\geq 4\log\frac{1}{\epsilon_1}+6+m, \tag{4.10}$$

[2]

$$\begin{aligned}
\eta_{\mathrm{opt}}(\epsilon',\epsilon_{\mathrm{EA}}) &= \max_{\frac{3}{4}<\frac{p_t(1)}{\gamma}<\frac{2+\sqrt{2}}{4}} \eta(\omega_{\mathrm{exp}}\gamma-\delta_{\mathrm{est}},p_t,\epsilon',\epsilon_{\mathrm{EA}})\,,\\
\eta(p,p_t,\epsilon',\epsilon_{\mathrm{EA}}) &= f_{\min}(p,p_t)-\frac{1}{\sqrt{n}}2\left(\log 13+\frac{\mathrm{d}}{\mathrm{d}p(1)}g(p)|_{p_t}\right)\sqrt{1-2\log(\epsilon'\epsilon_{\mathrm{EA}})}\,,\\
f_{\min}(p,p_t) &= \begin{cases} g(p) & \text{if } p(1)\leq p_t(1)\,,\\ \frac{\mathrm{d}}{\mathrm{d}p(1)}g(p)|_{p_t}\cdot p(1)+\left(g(p_t)-\frac{\mathrm{d}}{\mathrm{d}p(1)}g(p)|_{p_t}\cdot p_t(1)\right) & \text{if } p(1)>p_t(1)\end{cases}\\
g(p) &= \begin{cases} 1-h\left(\frac{1}{2}+\frac{1}{2}\sqrt{16\frac{p(1)}{\gamma}\left(\frac{p(1)}{\gamma}-1\right)+3}\right) & \text{if } \frac{p(1)}{\gamma}\in\left[0,\frac{2+\sqrt{2}}{4}\right]\\ 1 & \text{if } \frac{p(1)}{\gamma}\in\left[\frac{2+\sqrt{2}}{4},1\right]\end{cases}
\end{aligned}$$

[3]

$$\begin{aligned}
a &= \left\lceil\frac{\log(m-2e)-\log(2\ell-2e)}{\log(2e)-\log(2e-1)}\right\rceil\\
\ell &= \left\lceil\log 2n+2\log\frac{2}{\epsilon_1}\right\rceil
\end{aligned}$$

then the extractor promises

$$\frac{1}{2}\left\|\rho_{\mathrm{Ext}(\mathbf{AB},\mathbf{Z})\mathbf{Z}E} - \rho_{ideal}\right\|_1 \leq m\epsilon_1, \tag{4.11}$$

where ϵ_1 is the 1 bit extractor error tolerance.

Since the protocol promises that the entropy of the input to the extractor AB is more than $n \cdot \eta_{\mathrm{opt}}(\epsilon', \epsilon_{\mathrm{EA}})$, by setting of the length m of the extricable random bits satisfies

$$n \cdot \eta_{\mathrm{opt}}(\epsilon', \epsilon_{\mathrm{EA}}) = 4 \log \frac{1}{\epsilon_1} + 6 + m, \tag{4.12}$$

one can obtained the soundness of the extractor is $m\epsilon_1$. Combined with the input sampling soundness ϵ_{SA}, the soundness ϵ_{EA}, and smoothing parameter ϵ' of the protocol, the total soundness is bounded by $\epsilon_{\mathrm{SA}} + \epsilon_{\mathrm{EA}} + \epsilon'/2 + m\epsilon_1$.

4.2 Extractable randomness from experimental Bell test

4.2.1 Output randomness analysis

The previous section described our randomness expansion protocol. It is sufficient for the purpose of obtaining a rough estimation of the randomness output, but further optimization can be done. Since $m \leq 2n$, we can let $m\epsilon_1 \leq 2n\epsilon_1 =: \epsilon_{\mathrm{EX}}$ and replace the term $m\epsilon_1$ in the overall soundness with ϵ_{EX}. The insertion of $\epsilon_1 = \epsilon_{\mathrm{EX}}/(2n)$ back into Eq. 4.12 gives us the number of random bits that can be extracted

$$m = n \cdot \eta_{\mathrm{opt}}(\epsilon', \epsilon_{\mathrm{EA}}) - 4 \log n + 4 \log \epsilon_{\mathrm{EX}} - 10\,. \tag{4.13}$$

The extractable random bit per round is then equal to

$$r_n = \left(\eta_{\text{opt}}(\epsilon', \epsilon_{\text{EA}}) - 4\frac{\log n}{n} + 4\frac{\log \epsilon_{\text{EX}}}{n} - \frac{10}{n} \right) . \tag{4.14}$$

For $n \to \infty$, one obtains the asymptotic extractable number of random bits:

$$r_\infty = \left[1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{\frac{S^2}{4} - 1} \right) \right] . \tag{4.15}$$

To calculate the output random bit rate in finite statistics, it is necessary to set all the protocol parameters — $\gamma, \delta_{\text{est}}, n$, and ϵ's, which are constrained by the completeness and soundness security parameters. Here, we take a simple approach without optimizing over the variables $\gamma, \delta_{\text{est}}, \epsilon$'s. For each block size n, the γ value determines the ϵ_{SA} via Eq. 4.8, which then fixes δ_{est} via $\epsilon_{\text{est}} = 10^{-10} - \epsilon_{\text{SA}}$. The remaining ϵ's are chosen in a $1:2:1$ ratio of $\epsilon_{\text{EA}} : \epsilon' : \epsilon_{\text{EX}}$, which is guaranteed to add up to the specified level of completeness and soundness.

4.2.2 Extractable randomness with observed violation

The extractable random bit rate is a more important parameter for the users of most applications requiring random numbers as input. Figure 4.1 presents the extractable randomness rate r_n/τ with various block sizes n. In this calculation, we assume $\gamma = 0$, use the observed S values shown in Fig. 3.8 as inputs, and apply the security parameter $\epsilon_{\text{c}} = \epsilon_{\text{s}} = 10^{-10}$. For comparison, Fig. 4.1 also shows the asymptotic value r_∞/τ computed with S values given by a simulation, which utilizes source efficiency and dark-count as inputs. As explained in Chapter 3, the detection jitter time affects the observable violation especially when the bin width τ is comparable to it. This causes the extractable bit rate to undergo a sharp drop for short time widths. It is important to note that the highest randomness rate is not obtained at maximal violation of the inequality, where the highest randomness per round is observed (see Fig. 3.8 and Fig. 4.1). It turns out to be advantageous to sacrifice randomness per measurement round in favor of a larger number of rounds per unit time. This optimization will be

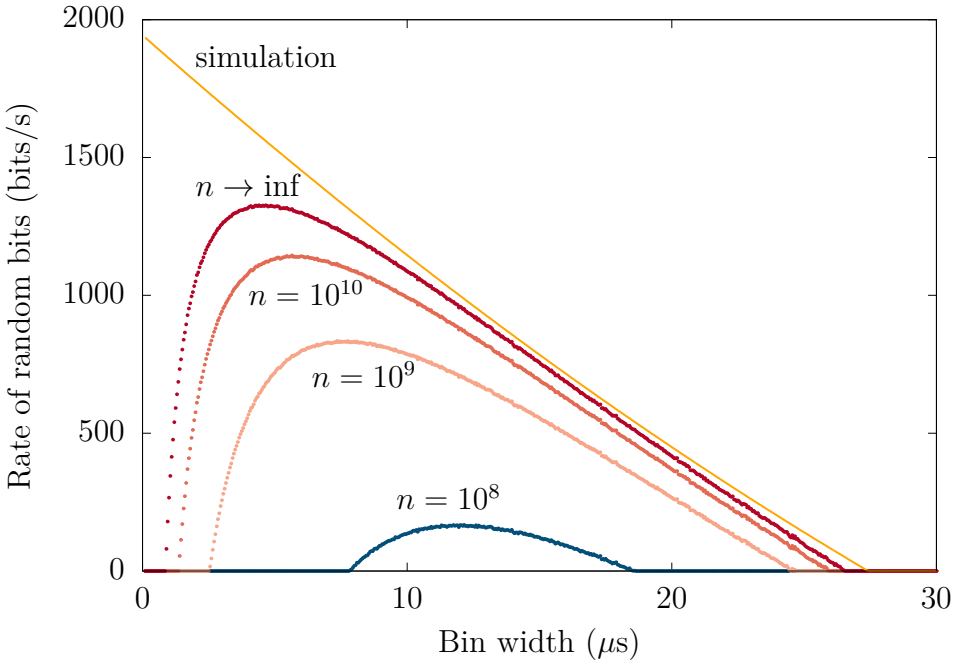


Fig. 4.1 Random bit generation rate r_n/τ as a function of τ for different block sizes n. The points are calculated via Eq. 4.14 for finite n (Eq. 4.15 for $n \to \infty$), and the violation measured in the experiment (shown in Fig. 3.8), assuming $\gamma = 0$ (no testing rounds) and $\epsilon_c = \epsilon_s = 10^{-10}$. The continuous line is the asymptotic rate calculated via Eq. 4.15, using S values calculated from a simulation based on our binning model (described in Chapter 3) with the same security assumptions.

part of the calibration procedure for a random number generator with an active switch of measurement bases.

In Fig. 4.1, the curve with an infinite block size $n \to \infty$ shows that about 1300 random bits/s can be extracted from our setup when $\tau = 4.40\,\mu$s. If we consider blocks of size $n = 10^8$, with $\tau = 12.15\,\mu$s, the calculated random bit rate is ≈ 167 bits/s, a rate comparable with recent reported results [60, 31], but with the advantage that the time required to acquire a single block is approximately 20 minutes instead of more than a hundred hours in [60, 31]. Increasing the block size by one order of magnitude to $n = 10^9$, with $\tau = 7.35\,\mu$s, the rate of generated randomness increases to ≈ 834 bits/s, the corresponding acquisition time for such a single block ≈ 2 hours, and is compatible with the experimental stability of our source. These numbers are not optimal; more sophisticated analysis demonstrated higher randomness extraction for the same detected violation [26, 118].

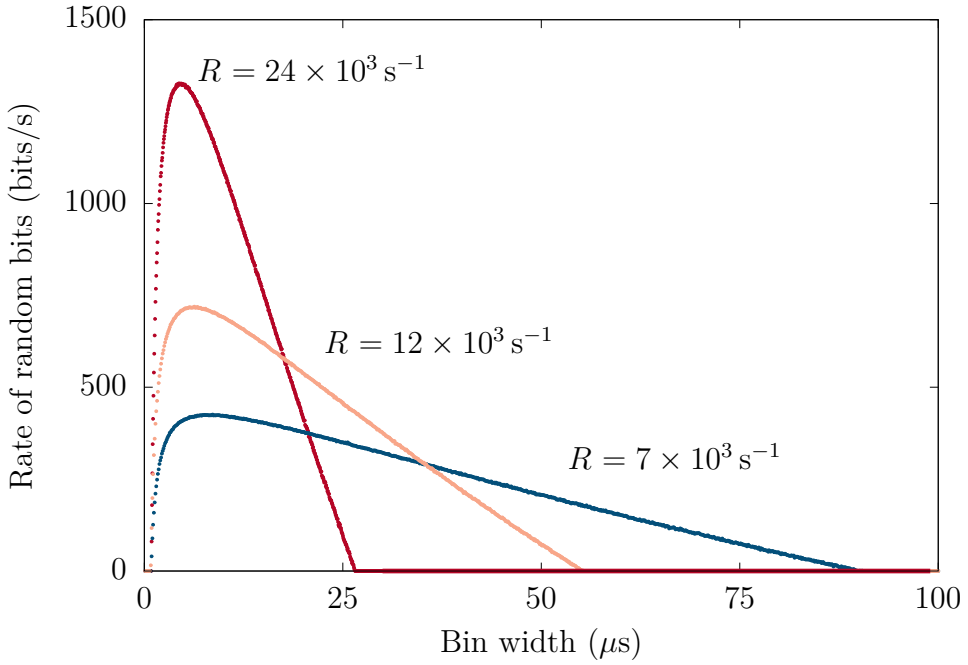


Fig. 4.2 Extractable random bit rates with infinite block size ($n \to \infty$) for different down-converted photon pair rates. There are three datasets with different pair rates (R in the figure represent the rate), but almost same heralding efficiency (details can be found in Section 3.3.2). This figure shows that an increase in the pair rates results in higher extractable random bit rates.

4.2.3 Extractable randomness with different pair rates

In the previous section, the pair rate was fixed at $24{\times}10^3\,\mathrm{s}^{-1}$. This section shows the extractable random bit rates with infinite block size for different down-converted photon pair rates (see Fig. 4.2). There are three datasets with pair rates around $7{\times}10^3\,\mathrm{s}^{-1}$, $12{\times}10^3\,\mathrm{s}^{-1}$, and $24{\times}10^3\,\mathrm{s}^{-1}$. The corresponding S values are 2.01467(72), 2.01577(44), and 2.01602(32), respectively, which were also illustrated in Fig. 3.10. Although the largest violation for these various datasets is similar, the highest extractable random bit rates in Fig. 4.2 are almost linear to the pair rates.

We expect that the random bit rate will further increase with even higher pair rates. This can be implemented by increasing the pump power, and is ultimately limited by the detection time jitter. Thus, the use of efficient superconducting nanowire detectors with tens of ps jitter time will be a significant advantage.

4.3 Random bits extraction

4.3.1 Extracting random bits from the demonstration dataset

For the described experimental setup, the measurement basis cannot be actively changed in each round to exactly follow the protocol introduced in Section 4.1. Instead, this section describes a concrete procedure to extract the a string of random bits from the 42.8 minutes dataset used to demonstrate the violation.

We dedicate a fraction γ_{calib} of the dataset to estimating the winning probability w_{exp}. The security parameters $\epsilon_{\text{s}}, \epsilon_{\text{c}}$ are set *a priori* (both $= 10^{-10}$). Here the honest implementation is defined as an implementation which reproduces w_{exp} during the calibration stage with probability

$$P(w_{\text{exp}} \geq w_{\text{calib}}) \leq \epsilon_{\text{calib}}\,, \tag{4.16}$$

where the w_{calib} is obtained from the calibration fraction of the dataset. The choice of $\epsilon_{\text{calib}} = 10^{-10}$ guarantees that the Bell violation will not be overestimated, and ensures that the whole certification procedure succeeds with a large probability. Then, one can write w_{exp} as

$$w_{\text{exp}} = w_{\text{calib}} - \delta_{\text{calib}}\,, \tag{4.17}$$

where we use the upper bound

$$\delta_{\text{calib}} \leq \sqrt{\frac{\log(1/\epsilon_{\text{calib}})}{2n}}, \tag{4.18}$$

valid for all winning probabilities ω_{calib}, leading to a conservative estimation. We optimize the calibration fraction γ_{calib} and the bin width τ to maximize the extractable randomness from the demonstration dataset, obtaining $\gamma_{\text{calib}} = 22\%$ and $\tau = 8.9\ \mu$s.

After optimizing these parameters, w_{exp} is calculated via Eq. 4.17 and Eq. 4.18. The data used to extract random bits is also verified that it has violated more than

Fig. 4.3 The result of the extraction illustrated with black and white pixels. The left side square contains 175 288 156 bits from the Bell test output. The small square at the right side is the extracted 617 920 random bits.

the threshold $w_{\text{exp}} - \delta_{\text{est}}$ calculated via Eq. 4.7, which confirms we made a honest implementation.

Finally, we use the Trevisan extractor to extract the certified bits. The extractor also requires a supply of seed randomness. A random number generator described in [119] provides the seeds for this work. There are 175 288 156 bins in the reminding dataset with 8.9 μs bin width. With these measurement rounds, the extractor generates 617 920 random bits. The calculated rate of extracted random bits considering the total measurement time ($\approx$ 42.8 minutes), which includes the acquisition time for the calibration fraction γ_{calib} (around 7.5 minutes), the source phase optimization time (around 8 minutes), and the time used to rotate the waveplates (less than 1 minute)

is ≈ 240 bit/s. If one only considers the net measurement time, the random bit rate becomes ≈ 396 bit/s.

Figure 4.3 illustrates the result of the extraction using black and white pixels. It is evident that the size of the bit string generated from the experiment is much larger than the size of the extracted random bits string. However, the distribution of the n bits from the experimental Bell test are obviously non-uniform.

We used the NIST Statistical Test Suite to ensure that the quality of generated strings is at least on par with acceptable pseudo-randomness [120]. As mentioned in Chapter 1, statistical tests can only verify the uniformity of the generated random string, but cannot certify its privacy. The string generated from this dataset passed all the tests that are meaningful for this relatively short sample, assuming an acceptable significance level $\alpha = 0.01$. The result of the individual tests are summarized in table 4.1.

Test	P–value	Proportion
Frequency	0.590949	96/97
Block Frequency	0.275709	95/97
Cumulative Sums Forward	0.964295	96/97
Cumulative Sums Backward	0.637119	96/97
Runs	0.162606	97/97
Longest Run of Ones	0.590949	96/97
Discrete Fourier Transform	0.183769	96/97

Table 4.1 Result of the NIST Statistical Test Suite for the bits extracted from the dataset. We split the random bits into 97 sequences of 6300 bits each.

4.3.2 More randomness from longer acquisition

Figure 4.1 indicates that a faster random number generator can be obtained with a larger block size n. For example, when $n = 10^9$, with $\tau = 7.35\,\mu$s, the rate of generated randomness increases to ≈ 834 bits/s, and the time required to acquire a single block is ≈ 2 hours. The source introduced in this thesis could stably output polarization-entangled photon pairs with high efficiency for tens of hours. We thus acquired a long dataset (around 17.3 hours) with a violation and generated pair rate similar to the 42.8 minutes demonstration data. In this dataset, the time for data acquisition was around 11.3 hours, and the remaining 6 hours were used to find the optimal phase angle and set the measurement bases.

For this longer acquisition, the calculated optimal calibration fraction γ_{calib} is around 8%, and the optimal bin width (τ) is 5.35 μs. Via Eq. 4.14, we found that the extractable random bits m from this large dataset is 35 799 872. The corresponding rate, computed base on the entire 17.3 hours, is $\approx$ 573 bits/s.

These reported rates do not include the processing time of the Trevisan extractor. This classical computation took 9 hours to process the 42.8 minutes dataset on a machine processing 24 threads in parallel. For the long measurement, the estimated extraction time is around $\approx$ 18 years if run on the same hardware. In order to reduce this time to a few days, it would be necessary to employ thousands of cores. We decided not to pursue this effort as we did not think that it would add further value to the presented results.

Conclusion

This thesis presented an experiment on a detection loophole-free Bell violation with a continuously pumped photon pair source. The photon pairs were generated through a spontaneous parametric down conversion process, and measured with highly efficient transition-edge sensors, reaching an overall detection efficiency of more than 82%, with a lower rate of background events (less than 0.2%).

Section 3.2.2 presented in detail the source of photon pairs with a controllable degree of polarization entanglement with a fidelity larger than 99.1%. The precise control of the entanglement allowed us to maximize the observable Bell violation [49]. The reported source could also generate a maximally entangled state with 99.1% visibility on the D/A bases.

Bell tests are carried out in successive rounds. We defined the measurement rounds of Bell tests by organizing the detection events in uniform time bins, and observed a maximum violation of $S = 2.01602(32)$ with average number of pairs per round of ≈ 0.32. The flexible definition of the experimental round with a continuous photon pair source allowed us to study the observable violation as a function of the average number of photon pairs per experimental round. This same flexibility can be exploited to reduce the time necessary to acquire sufficient statistics for the detection loophole-free Bell experiments. Section 3.3 showed that an increase in the pair rate is accompanied by a reduction of the round duration, τ, for the largest violation. This approach shifts the experimental repetition rate limitation from the photon statistics to the other elements of the setup, e.g., the detector time response or the active polarization basis switching speed.

The observation of a Bell violation certifies the generation of private randomness. The number of random bits that can be extracted per measurement round $r(\tau)$ is a function of the CHSH parameter $S(\tau)$. The random bit generation rate is equal to $r(\tau)/\tau$. Hence, the optimal round duration is a trade-off between the experimentally observed CHSH parameter $S(\tau)$ and the number of rounds per unit time $1/\tau$. While the optimal round duration would be infinitesimally short in a ideal scenario (Fig. 4.1), it is

limited in our system by the detectors jitter time $\approx 170\,\mathrm{ns}$. The calculated asymptotic random number generation rate of our experimental setup is $\approx 1300\,\mathrm{s}^{-1}$.

In order to extract uniformly distributed random bits from the experimental Bell test, we employed a randomness expansion protocol [115]. Such a protocol includes n rounds forming a block in which $n\gamma$ rounds are used to violate the Bell inequality, and the rest of the $n(1-\gamma)$ rounds work as the input for a quantum-proof randomness extractor [116]. We calculated the extractable randomness rate r_n as a function of the block size n, the observed violation S, and the security and uniformity parameters $\epsilon_s = \epsilon_c = 10^{-10}$. With a block size of $n = 10^8$ and $\tau = 12.150\ \mu\mathrm{s}$, the calculated rate of random bit rate is $\approx 167\,\mathrm{s}^{-1}$. This number is comparable with recently reported results in [31, 60], but the data acquisition time for such a block is approximately 20 minutes instead of more than hundred hours in [31, 60]. If the block size is increased to $n = 10^{10}$, the optimal random bit extraction rate will be around thousands of bits per second, and the corresponding acquisition time will still be relatively short (less than 20 hours).

Finally, we applied the Trevsion extractor to our 42.8 minutes dataset, which was used to demonstrate the Bell violation, and extracted 617920 random bits. The corresponding bit generation rate is $\approx 240\,\mathrm{s}^{-1}$. If one only considers the net measurement time (excluding the calibration, phase lock, and waveplate rotation time), the rate becomes $\approx 396\,\mathrm{s}^{-1}$.

Currently, the certified random number generation speed of the device-independent random number generator reported in this thesis represents a significant advance toward reaching the goal of a practical source of certified randomness for secure information processing applications.

Outlook

The reported randomness generation rate in this thesis is mainly limited by the jitter time of the single-photon detectors and the photon pair generation rate, which can be overcome by replacing the used transition edge sensors with faster detectors and increasing the pump power of the source. Moreover, by using a fast polarization switch and space-like separating our measurement devices, it is possible to generate random numbers that are completely loophole-free.

References

[1] A. K. Ekert. Quantum cryptography based on Bellâs theorem. *Physical Review Letters* **67**, 661 (1991).

[2] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science* **560**, 7 (2014).

[3] M. T. McClellan, J. Minker, and D. E. Knuth. *The Art of Computer Programming, Vol. 3: Sorting and Searching*, volume 28 (1974). ISBN 0201896850.

[4] R. Motwani and P. Raghavan. *Randomized algorithms* . ISBN 9780521474658.

[5] D. P. Kroese, T. Brereton, T. Taimre, and Z. I. Botev. Why the Monte Carlo method is so important today. *Wiley Interdisciplinary Reviews: Computational Statistics* **6**, 386 (2014).

[6] G. Marsaglia. Random Numbers Fall Mainly in the Planes. *Proceedings of the National Academy of Sciences* **61**, 25 (1968).

[7] G. J. Chaitin. *Information, randomness & incompleteness : papers on algorithmic information theory*. World Scientific (1990). ISBN 9810201540.

[8] W. Trappe and L. C. Washington. *Introduction to cryptography : with coding theory*. Pearson Prentice Hall (2006). ISBN 0131862391.

[9] B. Schneier. *Applied cryptography : protocols, algorithms, and source code in C* . ISBN 9781119096726.

[10] M. Born. *Physics in My Generation*. Heidelberg Science Library. Springer New York, New York, NY (1968). ISBN 978-0-387-90008-7.

[11] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden. Optical quantum random number generator. *Journal of Modern Optics* **47**, 595 (2000).

[12] A. Acín and L. Masanes. Certified randomness in quantum physics. *Nature* **540**, 213 (2016).

[13] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics* **1**, 195 (1964).

[14] S. Pironio, A. Acín, S. Massar, A. B. De La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe. Random numbers certified by Bell's theorem. *Nature* **464**, 1021 (2010).

[15] A. Aspect, J. Dalibard, and G. Roger. Experimental test of Bell's inequalities using time- varying analyzers. *Physical Review Letters* **49**, 1804 (1982).

[16] J. F. Clauser and M. A. Horne. Experimental consequences of objective local theories. *Physical Review D* **10**, 526 (1974).

[17] M. Giustina, A. Mech, S. Ramelow, B. Wittmann, J. Kofler, J. Beyer, A. Lita, B. Calkins, T. Gerrits, S. W. Nam, R. Ursin, and A. Zeilinger. Bell violation using entangled photons without the fair-sampling assumption. *Nature* **497**, 227 (2013).

[18] M. Giustina, M. A. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J. Å. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger. Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons. *Physical Review Letters* **115**, 250401 (2015).

[19] B. Hensen, H. Bernien, A. E. Dreaú, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature* **526**, 682 (2015).

[20] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam. Strong Loophole-Free Test of Local Realism. *Physical Review Letters* **115**, 250402 (2015).

[21] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland. Experimental violation of a Bell's inequality with efficient detection. *Nature* **409**, 791 (2001).

[22] M. Ansmann, H. Wang, R. C. Bialczak, M. Hofheinz, E. Lucero, M. Neeley, A. D. O'Connell, D. Sank, M. Weides, J. Wenner, A. N. Cleland, and J. M. Martinis. Violation of Bell's inequality in Josephson phase qubits. *Nature* **461**, 504 (2009).

[23] A. E. Lita, A. J. Miller, and S. W. Nam. Counting near-infrared single-photons with 95% efficiency. *Optics Express* **16**, 3032 (2008).

[24] 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% system efficiency. *Nature Photonics* **7**, 210 (2013).

[25] B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. Lim, N. Gisin, and P. G. Kwiat. Detection-loophole-free test of quantum nonlocality, and applications. *Physical Review Letters* **111**, 130406 (2013).

[26] P. Bierhorst, E. Knill, S. Glancy, Y. Zhang, A. Mink, S. Jordan, A. Rommal, Y. K. Liu, B. Christensen, S. W. Nam, M. J. Stevens, and L. K. Shalm. Experimentally generated randomness certified by the impossibility of superluminal signals. *Nature* **556**, 223 (2018).

[27] M. Fiorentino, G. Messin, C. Kuklewicz, F. Wong, and J. Shapiro. Ultrabright tunable photon-pair source with total-flux polarization-entanglement. *Postconference Digest Quantum Electronics and Laser Science, 2003. QELS.* **195**, 2000 (2003).

[28] D. C. Burnham and D. L. Weinberg. Observation of simultaneity in parametric production of optical photon pairs. *Physical Review Letters* **25**, 84 (1970).

[29] A. E. Lita, B. Calkins, L. A. Pellouchoud, A. J. Miller, and S. Nam. Superconducting transition-edge sensors optimized for high-efficiency photon-number resolving detectors. volume 7681, page 76810D. International Society for Optics and Photonics, (2010). ISBN 9780819481450.

[30] D. Fukuda, G. Fujii, T. Numata, K. Amemiya, A. Yoshizawa, H. Tsuchida, H. Fujino, H. Ishii, T. Itatani, S. Inoue, and T. Zama. Titanium-based transition-edge photon number resolving detector with 98% detection efficiency with index-matched small-gap fiber coupling. *Optics Express* **19**, 870 (2011).

[31] Y. Liu, Q. Zhao, M. H. Li, J. Y. Guan, Y. Zhang, B. Bai, W. Zhang, W. Z. Liu, C. Wu, X. Yuan, H. Li, W. J. Munro, Z. Wang, L. You, J. Zhang, X. Ma, J. Fan, Q. Zhang, and J. W. Pan. Device-independent quantum random-number generation. *Nature* **562**, 548 (2018).

[32] R. Shabanali. Basic Concepts: Definition of Randomness - webmindset. URL http://webmindset.net/definition-of-randomness/.

[33] V. Scarani. *Bell Nonlocality.* manuscript not published yet (2018).

[34] A. C.-C. Yao. Probabilistic computations: Toward a unified measure of complexity. In *18th Annual Symposium on Foundations of Computer Science (sfcs 1977)*, pages 222–227. IEEE, (1977).

[35] T. Keightley. *Natural inheritance*, volume s4-II. Macmillan (1868). ISBN 1525-8610.

[36] R. T. Argenton, (IME/USP), and Wikimedia. Galton box. URL https://commons.wikimedia.org/wiki/File:Galton{_}box.jpg.

[37] W. Macke. L. D. Landau and E. M. Lifshitz Mechanics. Vol. 1 of: Course of Theoretical Physics. 165 S. m. 55 Abb. Oxford/London/Paris 1960. Pergamon Press Ltd. Preis geb. 40 s. net. *ZAMM - Zeitschrift für Angewandte Mathematik und Mechanik* **41**, 392 (1961).

[38] J. G. Rarity, P. C. Owens, and P. R. Tapster. Quantum random-number generation and key sharing. *Journal of Modern Optics* **41**, 2435 (1994).

[39] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger. Quantum cryptography with entangled photons. *Physical Review Letters* **84**, 4729 (2000).

[40] M. Lawlor. Dealing with leachate at solid waste disposal sites. *Public Works* **107**, 74 (1976).

[41] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger. Violation of bell's inequality under strict einstein locality conditions. *Physical Review Letters* **81**, 5039 (1998).

[42] A. Aspect, P. Grangier, and G. Roger. Experimental realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A new violation of Bell's inequalities. *Physical Review Letters* **49**, 91 (1982).

[43] J. G. Rarity and P. R. Tapster. Experimental violation of Bells inequality based on phase and momentum. *Physical Review Letters* **64**, 2495 (1990).

[44] W. Tittel, J. Brendel, B. Gisin, T. Herzog, H. Zbinden, and N. Gisin. Experimental demonstration of quantum correlations over more than 10 km. *Physical Review A - Atomic, Molecular, and Optical Physics* **57**, 3229 (1998).

[45] J. Handsteiner, A. S. Friedman, D. Rauch, J. Gallicchio, B. Liu, H. Hosp, J. Kofler, D. Bricher, M. Fink, C. Leung, A. Mark, H. T. Nguyen, I. Sanders, F. Steinlechner, R. Ursin, S. Wengerowsky, A. H. Guth, D. I. Kaiser, T. Scheidl, and A. Zeilinger. Cosmic Bell Test: Measurement Settings from Milky Way Stars. *Physical Review Letters* **118**, 060401 (2017).

[46] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters* **23**, 880 (1969).

[47] S. J. Freedman and J. F. Clauser. Experimental test of local hidden-variable theories. *Physical Review Letters* **28**, 938 (1972).

[48] J. A. Larsson. Loopholes in Bell inequality tests of local realism. *Journal of Physics A: Mathematical and Theoretical* **47**, 424003 (2014).

[49] P. H. Eberhard. Background level and counter efficiencies required for a loophole-free Einstein-Podolsky-Rosen experiment. *Physical Review A* **47** (1993).

[50] P. M. Pearle. Hidden-variable example based upon data rejection. *Physical Review D* **2**, 1418 (1970).

[51] A. Garg and N. D. Mermin. Detector inefficiencies in the Einstein-Podolsky-Rosen experiment. *Physical Review D* **35**, 3831 (1987).

[52] A. Garg and N. D. Mermin. Detector inefficiencies in the Einstein-Podolsky-Rosen experiment. *Physical Review D* **35**, 3831 (1987).

[53] J. Å. Larsson. Bell's inequality and detector inefficiency. *Physical Review A - Atomic, Molecular, and Optical Physics* **57**, 3304 (1998).

[54] G. Garbarino. Minimum detection efficiencies for a loophole-free observable-asymmetric Bell-type test. *Physical Review A - Atomic, Molecular, and Optical Physics* **81**, 032106 (2010).

[55] A. Garuccio. Hardys approach, Eberhards inequality, and supplementary assumptions. *Physical Review A* **52**, 2535 (1995).

[56] J. Å. Larsson and J. Semitecolos. Strict detector-efficiency bounds for n-site Clauser-Horne inequalities. *Physical Review A - Atomic, Molecular, and Optical Physics* **63**, 1 (2001).

[57] T. Scheidl, R. Ursin, J. Kofler, S. Ramelow, X.-S. Ma, T. Herbst, L. Ratschbacher, A. Fedrizzi, N. K. Langford, T. Jennewein, and A. Zeilinger. Violation of local realism with freedom of choice. *Proceedings of the National Academy of Sciences* **107**, 19708 (2010).

[58] J. A. Larsson and R. D. Gill. Bell's inequality and the coincidence-time loophole. *Europhysics Letters* **67**, 707 (2004).

[59] J. Barrett, D. Collins, L. Hardy, A. Kent, and S. Popescu. Quantum nonlocality, Bell inequalities, and the memory loophole. *Physical Review A - Atomic, Molecular, and Optical Physics* **66**, 9 (2002).

[60] Y. Liu, X. Yuan, M. H. Li, W. Zhang, Q. Zhao, J. Zhong, Y. Cao, Y. H. Li, L. K. Chen, H. Li, T. Peng, Y. A. Chen, C. Z. Peng, S. C. Shi, Z. Wang, L. You, X. Ma, J. Fan, Q. Zhang, and J. W. Pan. High-Speed Device-Independent Quantum Random Number Generation without a Detection Loophole. *Physical Review Letters* **120**, 010503 (2018).

[61] W. Chen, H. Ning, J. Li, X. Mao, and B. Wang. Flight path detection of bird targets in radar images. *Chinese Journal of Electronics* **18**, 192 (2009).

[62] C. Ho, A. Lamas-Linares, and C. Kurtsiefer. Clock synchronization by remote detection of correlated photon pairs. *New Journal of Physics* **11**, 045011 (2009).

[63] J. C. Jacco. KTiOPO4 (KTP) Past, Present, And Future. volume 0968, page 93. International Society for Optics and Photonics, (1989).

[64] F. C. Zumsteg, J. D. Bierlein, and T. E. Gier. KxRb1-xTiOPO4: A new nonlinear optical material. *Journal of Applied Physics* **47**, 4980 (1976).

[65] D. S. Hum and M. M. Fejer. Quasi-phasematching. *Comptes Rendus Physique* **8**, 180 (2007).

[66] M. M. Fejer, D. H. Jundt, R. L. Byer, and G. A. Magel. Quasi-Phase-Matched Second Harmonic Generation: Tuning and Tolerances. *IEEE Journal of Quantum Electronics* **28**, 2631 (1992).

[67] P. A. Franken and J. F. Ward. Optical harmonics and nonlinear phenomena. *Reviews of Modern Physics* **35**, 23 (1963).

[68] A. McGurn. *Nonlinear optics*, volume 213. Academic Press (2018). ISBN 9783642194092.

[69] X. Lu, Q. Li, D. A. Westly, G. Moille, A. Singh, V. Anant, and K. Srinivasan. Chip-integrated visible-telecom entangled photon pair source for quantum communication. *Nature Physics* .

[70] S. Tanzilli, H. De Riedmatten, W. Tittel, H. Zbinden, P. Baldi, M. De Micheli, D. Ostrowsky, and N. Gisin. Highly efficient photon-pair source using periodically poled lithium niobate waveguide. *Electronics Letters* **37**, 26 (2001).

[71] D. Renker. Geiger-mode avalanche photodiodes, history, properties and problems. *Nuclear Instruments and Methods in Physics Research, Section A: Accelerators, Spectrometers, Detectors and Associated Equipment* **567**, 48 (2006).

[72] S. M. Hegde, K. L. Schepler, R. D. Peterson, and D. E. Zelmon. Room-temperature near IR fluorescence of high optical quality KTP. volume 6552, page 65520V. International Society for Optics and Photonics, (2007). ISBN 0819466743.

[73] D. C. Burnham and D. L. Weinberg. Observation of simultaneity in parametric production of optical photon pairs. *Physical Review Letters* **25**, 84 (1970).

[74] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih. New high-intensity source of polarization-entangled photon pairs. *Physical Review Letters* **75**, 4337 (1995).

[75] J. A. Armstrong, N. Bloembergen, J. Ducuing, and P. S. Pershan. Interactions between light waves in a nonlinear dielectric. *Physical Review* **127**, 1918 (1962).

[76] G. Sagnac. The Luminiferous Ether is Detected as a Wind Effect Relative to the Ether Using a Uniformly Rotating Interferometer. Technical report, (1913).

[77] B. S. Shi and A. Tomita. Generation of a pulsed polarization entangled photon pair using a Sagnac interferometer. *Physical Review A - Atomic, Molecular, and Optical Physics* **69**, 4 (2004).

[78] S. Ramelow, A. Mech, M. Giustina, S. Groeblacher, W. Wieczorek, A. Lita, B. Calkins, T. Gerrits, S. W. Nam, A. Zeilinger, and R. Ursin. Highly efficient heralding of entangled single photons. *Optics Express* **21**, 6707 (2012).

[79] R. Spectroscopy, F. Doubling, G. Sensing, R. Lasers, L. Imaging, B. Combining, P. Therapy, and V. Lasers. Wavelength Stabilization Gratings Features : • Applications : Specifications : Wavelength Stabilization Gratings Laser Wavelength Stabilization with PowerLocker ®. Technical report, (2012).

[80] D. L. Robinson and D. A. Hays. Photon detection with cooled avalanche photodiodes theory and preliminary experimental results.PDF. (1985).

[81] Laser Components GmbH. Silicon Geiger Mode Avalanche Photodiode Description. Technical report.

[82] R. S. Bennink. Optimal collinear Gaussian beams for spontaneous parametric down-conversion. *Physical Review A - Atomic, Molecular, and Optical Physics* **81**, 053805 (2010).

[83] G. D. Boyd and D. A. Kleinman. Parametric interaction of focused Gaussian light beams. *Journal of Applied Physics* **39**, 3597 (1968).

[84] J. M. Khosrofian and B. A. Garetz. Measurement of a Gaussian laser beam diameter through the direct inversion of knife-edge data. *Applied Optics* **22**, 3406 (1983).

[85] Z. Ficek and S. Swain. *Quantum Interference and Coherence: Theory and Experiments*. Springer (2010). ISBN 0959813814685833.

[86] S. K. Joshi. Entangled Photon Pairs: Efficient Generation and Detection, and Bit Commitment. (2014).

[87] V. Dipl-Phys Alexandra Mech and oUniv Prof DDrhc Anton Zeilinger. Titel der Dissertation " Experimental test of a Bell inequality with nonmaximally entangled states ". (2012).

[88] C. Canalias, J. Hirohashi, V. Pasiskevicius, and F. Laurell. Polarization-switching characteristics of flux-grown KTiOP O 4 and RbTiOP O 4 at room temperature. *Journal of Applied Physics* **97**, 1322 (2005).

[89] K. T. Stevens, L. E. Halliburton, M. Roth, N. Angert, and M. Tseitlin. Identification of a Pb-related Ti3+center in flux-grown KTiOPO4. *Journal of Applied Physics* **88**, 6239 (2000).

[90] M. G. Roelofs. Identification of Ti3+ in potassium titanyl phosphate and its possible role in laser damage. *Journal of Applied Physics* **65**, 4976 (1989).

[91] A. Deepthy, M. N. Satyanarayan, K. S. Rao, and H. L. Bhat. Photoluminescence studies on gray tracked KTiOPO4single crystals. *Journal of Applied Physics* **85**, 8332 (1999).

[92] K. D. Irwin. An application of electrothermal feedback for high resolution cryogenic particle detection. *Applied Physics Letters* **66**, 1998 (1995).

[93] NIST. Adding Up Photons with a TES. URL http://www.nist.gov/pml/div686/tes.cfm.

[94] J. Lee, L. Shen, A. Cerè, T. Gerrits, A. E. Lita, S. W. Nam, and C. Kurtsiefer. Multi-pulse fitting of Transition Edge Sensor signals from a near-infrared continuous-wave source. *Review of Scientific Instruments* **89**, 123108 (2018).

[95] W. F. Giauque and D. P. MacDougall. Attainment of temperatures below 1°absolute by demagnetization of Gd2(SO4)38H2O [12]. *Physical Review* **43**, 768 (1933).

[96] F. Pobell. *Matter and methods at low temperatures*. Springer Berlin Heidelberg, Berlin, Heidelberg (2007). ISBN 3540463569.

[97] R. C. Jaklevic, J. Lambe, A. H. Silver, and J. E. Mercereau. Quantum interference effects in Josephson tunneling. *Physical Review Letters* **12**, 159 (1964).

[98] K. D. Irwin and G. C. Hilton. Transition-edge sensors. *Topics in Applied Physics* **99**, 63 (2005).

[99] M. E. Huber, A. M. Corey, K. L. Lumpkins, F. N. Nafe, J. O. Rantschler, G. C. Hilton, J. M. Martinis, and A. H. Steinbach. DC SQUID series arrays with intracoil damping to reduce resonance distortions. *Applied Superconductivity* **5**, 425 (1997).

[100] O. H. Schmitt. A thermionic trigger. *Journal of Scientific Instruments* **15**, 24 (1938).

[101] L. Shen, J. Lee, L. P. Thinh, J. D. Bancal, A. Cerè, A. Lamas-Linares, A. Lita, T. Gerrits, S. W. Nam, V. Scarani, and C. Kurtsiefer. Randomness Extraction from Bell Violation with Continuous Parametric Down-Conversion. *Physical Review Letters* **121** (2018).

[102] J. D. Bancal, L. Sheridan, and V. Scarani. More randomness from the same data. *New Journal of Physics* **16**, 033011 (2014).

[103] J. A. Larsson and R. D. Gill. Bell's inequality and the coincidence-time loophole. *Europhysics Letters* **67**, 707 (2004).

[104] B. G. Christensen, A. Hill, P. G. Kwiat, E. Knill, S. W. Nam, K. Coakley, S. Glancy, L. K. Shalm, and Y. Zhang. Analysis of coincidence-time loopholes in experimental Bell tests. *Physical Review A - Atomic, Molecular, and Optical Physics* **92**, 032130 (2015).

[105] J. D. Bancal, L. Sheridan, and V. Scarani. More randomness from the same data. *New Journal of Physics* **16** (2014).

[106] Kolmogorov, A. N. (En alemán) Grundbegriffe der Wahrscheinlichkeitsrechnung. Berlín: Julius Springer. O Traducción: Kolmogorov, Andrey (1956) Foundations of the Theory of Probability. Technical report, (1933).

[107] D. F. James, P. G. Kwiat, W. J. Munro, and A. G. White. Measurement of qubits. *Physical Review A - Atomic, Molecular, and Optical Physics* **64**, 15 (2001).

[108] G. M. D'Ariano, M. G. Paris, and M. F. Sacchi. 2 Quantum Tomographic Methods. Technical report, (2004).

[109] A. G. White, D. F. James, P. H. Eberhard, and P. G. Kwiat. Nonmaximally entangled states: Production, characterization, and utilization. *Physical Review Letters* **83**, 3103 (1999).

[110] R. Jozsa. Fidelity for mixed quantum states. *Journal of Modern Optics* **41**, 2315 (1994).

[111] P. Bierhorst. A robust mathematical model for a loophole-free Clauser-Horne experiment. *Journal of Physics A: Mathematical and Theoretical* **48**, 1 (2015).

[112] D. Elkouss and S. Wehner. (Nearly) optimal P values for all Bell inequalities. *npj Quantum Information* **2**, 16026 (2016).

[113] M. Roth, M. Tseitlin, and N. Angert. Oxide crystals for electro-optic Q-switching of lasers. *Glass Physics and Chemistry* **31**, 86 (2005).

[114] G. D. Goodno, Z. Guo, R. J. D. Miller, I. J. Miller, J. W. Montgomery, S. R. Adhav, and R. S. Adhav. Investigation of-BaB 2 O 4 as a Q switch for high power applications. Technical Report 13, (1995).

[115] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick. Practical device-independent quantum cryptography via entropy accumulation. *Nature Communications* **9**, 459 (2018).

[116] W. Mauerer, C. Portmann, and V. B. Scholz. A modular framework for randomness extraction based on Trevisan's construction. (2012).

[117] T. S. Han and M. Hoshi. Interval algorithm for random number generation. *IEEE Transactions on Information Theory* **43**, 599 (1997).

[118] E. Knill, Y. Zhang, and P. Bierhorst. Quantum Randomness Generation by Probability Estimation with Classical Side Information. (2017).

[119] Y. Shi, B. Chng, and C. Kurtsiefer. Random numbers from vacuum fluctuations. *Applied Physics Letters* **109**, 41101 (2016).

[120] L. E. Bassham, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks, N. A. Heckert, J. F. Dray, and S. Vo. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical report, (2010).