Randomness Extraction and Clock Synchronization with Continuous Parametric Down-Conversion

Lee Jianwei

M.Sc., National University of Singapore

Supervisor: Professor Christian Kurtsiefer

Examiners: Professor John Rarity, Professor Hugo Zbinden,
Assistant Professor Travis Nicholson

Centre for Quantum Technologies
National University of Singapore

This dissertation is submitted for the degree of
Doctor of Philosophy

August 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.

Lee Jianwei

August 2019

Acknowledgements

First, I would like to thank my supervisor Prof. Christian Kurtsiefer for his patience and guidance throughout my PhD career. His humility, despite his expertise and professional standing is something I greatly admire and respect. I would also like to thank my lab partner Shen Lijiong with whom I shared many hours of labor in the laboratory and many helpful discussions. Special thanks to my post-doc Alessandro Cerè who taught me to strive for high standards of clarity in writing, presentation, and code.

A big thank you to my office mate Adrian Nugraha Utama, whose enthusiasm and intelligence is simply awe-inspiring. Thank you for inspiring me to expand my interests and your collaboration in contributing to physics education. I would also like to thank Mattias Seidler and Le Phuc Thinh for proofreading my thesis, Brenda Chng for her technical assistance, and Siddarth Joshi who laid important technical milestones for the randomness extraction experiment in his PhD thesis [1]. A big thank you to Prof. Valerio Scarani, Jean-Daniel Bancal, and Le Phuc Thinh for their theoretical contribution to the randomness extraction experiment. I would also like to thank present and past colleagues[1] who have taught and inspired me in various ways throughout my PhD. Special thanks to Ms. Janet Lim for remembering the birthdays of our group members. Kudos to our administrative folks[2] and talented support staff [3] who play crucial roles in scientific research. Special thanks to various PhD students[4] who organized monthly gatherings.

I would also like to thank Prof. Antia Lamas-Linares and James Troupe for presenting us the opportunity to collaborate in the clock synchronization experiment, and also Poh Hou Shun for his guidance on constructing the BBO-based entangled photon sources used for synchronization. I would also like to appreciate our collaborators from NIST: Thomas Gerrits, Adriana Lita,

[1] Matthias Steiner, Victor Leong, Janet Lim, Tan Peng Kian, Shi Yicheng, Ng Boon Long, Chow Chang Hoong, Yeo Xi Jie, Nguyen Chi Huan, Wilson Chin, Gleb Maslennikov, Syed Abdullah Aljunid, Tien Tjuen Ng, and Meng Khoon Tey.

[2] Especially Lim Ah Bee, Evon Tan, Jenny Hogan, Lim Siew Hoon, Amell Lim, Kelly Giam, Jessie Ho, Resmi P. Raju, Jacky Lim and Yvonne Toh, whom I interacted mostly with.

[3] Bob Chia, Teo Kok Seng, Lian Chorng Wang, Mohammad Imran and Ren Yaping.

[4] Hermanni Juuso Elias Heimonen and Tseng Ko-Wei.

and Sae Woo Nam, for their advice, and providing us samples of their transition-edge sensors. Special thanks to Prof. Belal E. Baaquie who taught me Quantum Field Theory, which has nothing to do with this thesis, but was a wonderful journey just the same.

I would also like to thank my Thesis Advisory Committee comprising of Prof. Valerio Scarani, Prof. Jens Martin, and my thesis supervisor.

Last but not least, I would like to thank my parents Lee Leong Seng and Quek Soy Soy, and my sister Lee Eng Joo, whose love enables me to pursue my work every day. Special thanks to my church buddies Christopher Chang and Jotham Teo, and to the One who makes all things beautiful in His time.

Abstract

This thesis introduces two protocols related to secure communication: private randomness generation and clock synchronization. The first enables measuring a Bell violation with a continuous source of entangled photon pairs, which eliminates the intrinsic deadtime present in previous experiments conducted with pulsed sources. This dramatically reduces the total acquisition time required for generating private random numbers from a detection loophole-free Bell experiment, while maintaining a competitive rate. With a total acquisition time of 43 min, we generated 617920 bits of private randomness, corresponding to ≈ 240 bits/s.

As the randomness generation rate depends on the rate of photon pairs detected, we also developed an algorithm suitable for extracting photodetection times from overlapping pulses generated by our detectors (transition-edge sensors), increasing the maximum detectable flux rate by an order of magnitude.

In the second protocol, we demonstrate absolute clock synchronization between two spatially separated rubidium clocks with correlated photon pairs. The technique exploits the tight timing correlation between each pair, produced in spontaneous parametric down-conversion, to achieve a precision of 51 ps for an averaging time of 100 s, with pair rates of order $200\,\mathrm{s}^{-1}$. Bidirectional exchange of photons over a symmetric delay channel allows remote clocks to be synchronized without *a priori* knowledge of their spatial separation, while a Bell inequality check allows parties to verify the origin of the synchronization signal. Protocol vulnerability is investigated by exploiting its reliance on a symmetric synchronization channel: we demonstrate how an asymmetric delay can be introduced with polarization-insensitive elements to create an error in time synchronization ≈ 25 ns while evading detection.

List of Publications & Conferences

The main results of this thesis have been reported in the following articles:

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).

4. **Jianwei Lee**, Lijiong Shen, Alessandro Cerè, James Troupe, Antia Lamas-Linares, and Christian Kurtsiefer. **Asymmetric delay attack on an entanglement-based bidirectional clock synchronization protocol**. *Applied Physics Letters*, **115**, 141101 (2019).

The results have also been presented at the following conferences:

1. **[Invited Talk]** Remote clock synchronization with entangled photon pairs. *SPIE Optics and Photonics*, San Diego, CA, USA (2019).

2. **[Talk]** Symmetrical Clock Synchronization with Time-Correlated Photon Pairs. *Conference on Lasers and Electro-Optics (CLEO)*, San Jose, CA, USA (2019).

3. **[Poster]** Multi-Pulse Fitting of Transition Edge Sensor Signals from a Near-Infrared Continuous-Wave Source. *Conference on Lasers and Electro-Optics (CLEO/Europe-EQEC)*, Munich, Germany (2019).

4. **[Talk]** Towards a loophole-free violation of Bell's Inequality. *Institute of Physics Singapore Meeting (IPS)*, Singapore (2015).

Table of contents

List of figures

Chapter 1

Introduction

This thesis focuses on two resources that are critical, though not limited, to secure communication: randomness generation and clock synchronization. In both cases, quantum entanglement is used to enhance security – certifying the secrecy of a sequence of random numbers, and providing a verification mechanism for a synchronization signal, respectively. This chapter introduces the challenges faced in each area, and the specific contributions made with our use of entangled photons generated from continuous spontaneous parametric down-conversion (SPDC).

Randomness Generation

The use of random numbers extends to many applications in modern science and technologies, from Monte Carlo simulations to classical and quantum cryptography [9–11]. Despite widespread reliance on random numbers for security applications, many methods used to certify their secrecy are unsatisfactory [12]. Intuitively, a sequence of numbers is considered random when no pattern can be detected in it. However, a lack of a discernible pattern does not necessarily guarantee that an adversary is unable to predict the sequence with a high probability of success [13]. Such is the case with pseudo-random number generators that deterministically produce a statistically random sequence with an arithmetic procedure [14]. Alternatively, random numbers can also be derived from physical phenomena, e.g. atmospheric turbulence, that are hard to predict [15]. However, we have to be convinced that the complexity of the physical process renders predicting its output insurmountable for an adversary. This then requires a trusted, deterministic model for the underlying process, and assumes that the adversary has finite computational power [13]. Even if random numbers are extracted from a quantum process which is believed to fundamentally random, a device that is believed to work

based on this process may not be faithfully implemented, could be unknowingly coupled to an adversary's system, or could be providing a pre-recorded sequence of results of which the adversary also has a copy [16]. Consequently, certification of random number generators that does not rely on modeling their inner workings is necessary to ensure secrecy.

Device-independent quantum number generator (DIQNRG) protocols provide such a certification by measuring the correlations observed with entangled particles [12]. Certification is based on testing a so-called Bell inequality, which is violated when the measurement outcomes cannot be correlated with any outside process or variable, which in turn, guarantees that an adversary cannot predict the outcomes. Importantly, certification does not involve modeling the inner workings of the generator – only its output is tested. Although several experimental Bell tests have been demonstrated (e.g. with entangled ions, photons, and NV-centres), photonic implementations have so far yielded the highest randomness generation rates due to the high repetition rates inherent in these systems [17–22]. However, the detection efficiencies of photonic systems have only recently been made competitive with the advent of superconducting single-photon detectors [23, 24]. Prior to this, the Bell tests were performed assuming that the detected fraction of photons was representative of the whole system – this "fair sampling" assumption could have been exploited by an adversary to artificially induce a violation with the detected fraction of photons [25, 26]. Collecting a representative fraction of photons requires a minimum detection efficiency of $\approx 66.7\,\%$ [2]; failure to meet this requirement is known as the detection loophole.

For photonic systems, the reported random bit rates extracted from a detection loophole-free Bell test is typically on the order of tens per second [27], and is mainly limited by the repetition rate of the pulsed photon sources.

In this work, we demonstrate that by using a continuous source of entangled photons, we obtain a randomness generation rate competitive with current state-of-the-art experiments using pulsed sources, but with shorter acquisition times. This is due to the fact that a continuous source does not have an intrinsic deadtime as opposed to a pulsed source. The detection loophole is closed with high-efficiency single-photon detectors (transition-edge sensors) [28] and a polarization-entangled photon pair source with high photon pair collection efficiency [29]. We show that for a fixed overall detection efficiency and photon pair generation rate, the observed violation and random bit generation rate depend on the width of the time bins used to organize the detection events [30].

Clock Synchronization

The ability to synchronize remote clocks plays an important role in our infrastructure, from maintaining coherence in the electrical grid, to allowing precise positioning and navigation, high-speed trading, and distributed data processing. In most protocols, remote parties deduce their clock offset by measuring signal propagation times with their devices and comparing the result with a trusted value [31–33]. Protocol security then relies on an independent characterization of propagation times [34], which can be difficult for mobile parties or under changing conditions. Bidirectional protocols circumvent this issue by synchronizing with counter-propagating signals, and are secure assuming that propagation times are independent of propagation directions [34]. Although convenient, this assumption exposes the protocol to attacks that introduce unknown asymmetric channel delays; attacks which cannot be detected by better encryption or authentication [34]. Existing countermeasures [35–37] , e.g. monitoring round-trip times [36], are not completely foolproof, and have been evaded by sophisticated intercept, spoofing and delay techniques [38].

In this work, we describe a distance-independent protocol using counter-propagating single photons originating from photon pairs [39]. Tight time correlations of photon pairs generated from SPDC enable precise synchronization. The single-photon regime allows, in principle, an additional security layer when synchronizing with entangled photon pairs; Monogamy of entanglement [40] ensures that a counterfeit photon entangled with the legitimate signal cannot be generated, allowing parties to verify the origin of received signals. The no-cloning theorem [41] prevents intercept, copy and resend of an identical quantum state with an arbitrary delay. Any tampering of the synchronization channel that reduces the entanglement between photon pairs can be detected by a Bell inequality check [42].

We first demonstrate the timing aspect of the protocol. While clock synchronization based on SPDC has been demonstrated, previous works require knowing *a priori* the signal propagation times [43–45], controlling them with a balanced interferometer [46], or were performed with clocks sharing a common frequency reference [47, 48]. Here, we synchronize remote clocks referenced to independent frequency standards using two separate SPDC pair sources. We obtain a synchronization precision consistent with the intrinsic frequency instabilities of our clocks, while changing their relative separation [49].

Next, we explore the security aspect of the protocol: in particular, its vulnerability to an asymmetric delay attack performed without measuring the quantum state of the synchronizing signal. This attack receives special attention as it seems relatively simple to implement with polarization-independent circulators, while potentially evading detection by testing a Bell inequality. However, a recent proposal suggests that even polarization-insensitive circulators,

which rotate input polarizations back to the same state, impose a measurable change in entanglement [50]. The proposal was based on the fact that the phase change after a cyclic quantum evolution is measurable under certain conditions [7], and have been observed in previous experiments involving entangled photons [51–54]. We examine the circulator-based asymmetric delay attack considered in Ref. [50] and experimentally verify that it *cannot* be detected non-locally while creating an error in time synchronization of $25.24(2)$ ns between two rubidium clocks [55].

Thesis Outline

This thesis is organized as follows: Chapter 2 introduces the Bell inequality, the time binning method used to define each Bell measurement round, and the protocol used to extract random numbers from the measurement outcomes. Chapter 3 describes the high-efficiency photodetectors and polarization-entangled photon source implemented to close the detection-loophole for the Bell experiment. The amount of Bell violation, and the randomness that can be extracted, is also presented in this chapter. Chapter 4 introduces the timing extraction protocol for overlapping electrical pulses produced by our detectors, increasing the maximum number of photodetection events that can be identified. This enables higher random bit generation rates in future experiments. Chapter 5 describes the bidirectional clock synchronization protocol and demonstrates its precision when synchronizing two independent rubidium clocks. Chapter 6 reports on the vulnerability of the synchronization protocol to asymmetric delay attacks implemented with polarization-insensitive circulators. Finally, in Chapter 7 we conclude the thesis and discuss the outlook of each experiment.

Chapter 2

Theory of Randomness Extraction from a Bell experiment

In this thesis, the violation of a Bell inequality is used to certify the privacy of random numbers that can be extracted from measurements performed on polarization-entangled photon pairs. In this chapter, we first show how the Bell inequality indicates that the measurement outcomes are uncorrelated with any outside process or variable, which enables privacy certification [56]. Next, we present a novel time-binning strategy used to organize a stream of measurement outcomes due to our continuous source of entangled photons, and the model used to numerically simulate the expected Bell violation. Finally, we outline an algorithm that extracts random numbers from the measurement outcomes, taking into account finite statistics and considerations related to the security of the extracted bits [57].

2.1 The Bell test

The Bell test was first formulated in 1964 as an answer to Einstein, Podolsky, and Rosen (EPR), who questioned if quantum mechanics (QM) was an incomplete theory [56]. EPR argued that since QM describes entangled particles that could be correlated to each other despite being space-like separated, QM must be an inadequate description of nature, given that they are unwilling to give up the notion of "local-realism" [58]. Locality refers to the postulate that any causal influence cannot propagate faster than the speed of light, while realism is the assumption that measurement outcomes are predetermined before measurement – both concepts are congruent with physical intuition.

However, experimental Bell tests on entangled systems have repeatedly verified that nature is in fact, not local-realistic [17–22, 59–63]. Conversely, users can use a Bell test to verify that

their systems are both entangled and pure [16]. The purity of their states ensures that their devices are not too correlated with the environment or with an external observer, ensuring privacy. Entanglement certifies that the local state of each party is mixed, and is therefore a source of randomness. Moreover, as only measurement outcomes are used to evaluate the Bell inequality, privacy certification does not rely on modeling the inner workings of any experimental apparatus – security is evaluated in a device-independent way. This is convenient in a security context, since it allows users to evaluate the devices without having to make any assumptions about them, e.g. that they have been correctly implemented by an external provider [16].

2.1.1 Derivation of the CHSH type Bell inequality

Since locality plays a crucial role in the formulation of a Bell test, the test cannot be performed on a single-qubit system – the simplest scenario that can be tested requires two distant observers, Alice and Bob, interacting with a two-qubit system. In this section, we follow Ref. [13] and derive the CHSH-type (John Clauser, Michael Horne, Abner Shimony and Richard Holt) Bell inequality used to analyze this system.

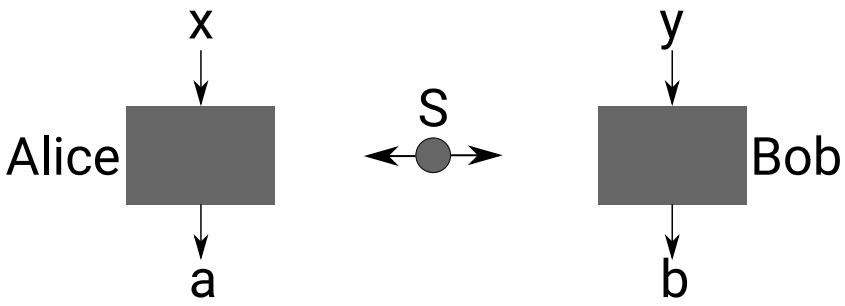


Figure 2.1: Scheme for a CHSH-type Bell test. A source (S) distributes two physical systems to distant observers, Alice and Bob. Each party has a measurement device with two settings $x, y \in \{0,1\}$ and two outputs $a, b \in \{-1,1\}$. Bell tests are carried out in successive rounds. For each round, each party chooses a measurement setting and records the outcome. Sufficient rounds are repeated to estimate the joint probability distribution $P(a,b|x,y)$ of obtaining outcomes a and b given the settings x and y. These probabilities are used to evaluate if a local-realistic theory describes the measurement outcomes.

In the CHSH Bell test (Fig. 2.1), Alice chooses one of two possible measurement settings, denoted by $x \in \{0,1\}$, and Bob likewise a setting denoted by $y \in \{0,1\}$. Once measurements are performed, their outcomes are recorded as $a \in \{-1,1\}$ and $b \in \{-1,1\}$ [64].

For any local-realistic theory, the measurement outcomes at Alice, a, should be due only to her measurement setting x, and perhaps some causal influence, encoded by a variable λ. The

same causal influence could affect Bob as well, since Alice's system could have previously interacted with Bob's system. An example of such an interaction could be due to the sharing of a pair of entangled particles that were created at a common location in the past (Fig. 2.1 point S). In addition, due to her space-like separation from Bob, Bob's measurement setting y and result b, cannot influence a, and vice-versa. Consequently, the joint probability of the measurement outcomes $P(a,b|x,y,\lambda)$ should reflect only the local influences affecting each individual party, and factorize according to:

$$P(a,b|x,y,\lambda) = P(a|x,\lambda)P(b|y,\lambda). \tag{2.1}$$

The observed probability distribution of $P(a,b|x,y)$ over several tests depends rather on the probability distribution $q(\lambda)$ of the variables λ – variables which may not necessarily be under experimental control but may evolve over the different test runs

$$\begin{aligned} P(a,b|x,y) &= \int d\lambda\, P(a,b|x,y,\lambda)\, q(\lambda|x,y) \\ &= \int d\lambda\, P(a|x,\lambda)P(b|y,\lambda)q(\lambda), \end{aligned} \tag{2.2}$$

where the condition

$$q(\lambda|x,y) = q(\lambda) \tag{2.3}$$

requires that measurement choices be made independently.

If the joint probabilities $P(a,b|x,y)$ satisfy the decomposition rule imposed by locality (Eq. 2.2), CHSH showed that the correlation function E_{xy}

$$E_{xy} := P(a=b|x,y) - P(a\neq b|x,y) \tag{2.4}$$

for different measurement results xy satisfy the following inequality

$$|S| \leq 2, \tag{2.5}$$

where

$$S = E_{00} + E_{01} + E_{10} - E_{11}. \tag{2.6}$$

To show this, we first rewrite the correlation function (Eq. 2.4) in a compact form

$$E_{xy} = \sum_{ab} abP(a,b|x,y), \tag{2.7}$$

since the measurement outcomes $a, b \in \{-1, 1\}$ implies that the product of the outcome ab is related to their correlation

$$ab = \begin{cases} 1 & \text{if } a = b \\ -1 & \text{if } a \neq b. \end{cases} \tag{2.8}$$

Evaluating E_{xy} for $P(a,b|x,y)$ expected for a local-realistic theory (Eq. 2.2), we obtain

$$\begin{aligned} E_{xy} &= \sum_{ab} ab \int d\lambda q(\lambda) P(a|x,\lambda) P(b|y,\lambda) \\ &= \int d\lambda q(\lambda) \sum_a aP(a|x,\lambda) \sum_b bP(b|y,\lambda) \\ &= \int d\lambda q(\lambda) \langle a_x \rangle_\lambda \langle b_y \rangle_\lambda . \end{aligned} \tag{2.9}$$

This allows us to compute S (Eq. 2.6):

$$\begin{aligned} S &= \int d\lambda q(\lambda) \langle a_0 \rangle_\lambda \langle b_0 \rangle_\lambda + \langle a_0 \rangle_\lambda \langle b_1 \rangle_\lambda + \langle a_1 \rangle_\lambda \langle b_0 \rangle_\lambda - \langle a_1 \rangle_\lambda \langle b_1 \rangle_\lambda \\ &:= \int d\lambda q(\lambda) S_\lambda . \end{aligned} \tag{2.10}$$

Noting that $q(\lambda) \geq 0$ for all λ allows us to apply the triangle inequality, obtaining

$$|S| \leq \int d\lambda q(\lambda) |S_\lambda| \tag{2.11}$$

whose integrand is upper bounded

$$\begin{aligned} |S_\lambda| &= |\langle a_0 \rangle_\lambda \langle b_0 \rangle_\lambda + \langle a_0 \rangle_\lambda \langle b_1 \rangle_\lambda + \langle a_1 \rangle_\lambda \langle b_0 \rangle_\lambda - \langle a_1 \rangle_\lambda \langle b_1 \rangle_\lambda | \\ &= |\langle a_0 \rangle_\lambda [\langle b_0 \rangle_\lambda + \langle b_1 \rangle_\lambda] + \langle a_1 \rangle_\lambda [\langle b_0 \rangle_\lambda - \langle b_1 \rangle_\lambda] | \\ &\leq |\langle a_0 \rangle_\lambda | \, |\langle b_0 \rangle_\lambda + \langle b_1 \rangle_\lambda | + |\langle a_1 \rangle_\lambda | \, |\langle b_0 \rangle_\lambda - \langle b_1 \rangle_\lambda | \\ &\leq \text{Max}\{|\langle a_0 \rangle_\lambda |, |\langle a_1 \rangle_\lambda |\} \; [\, |\langle b_0 \rangle_\lambda + \langle b_1 \rangle_\lambda | + |\langle b_0 \rangle_\lambda - \langle b_1 \rangle_\lambda | \,] \\ &\leq |\langle b_0 \rangle_\lambda + \langle b_1 \rangle_\lambda | + |\langle b_0 \rangle_\lambda - \langle b_1 \rangle_\lambda | \end{aligned} \tag{2.12}$$

since $\text{Max}\{|\langle a_0 \rangle_\lambda |, |\langle a_1 \rangle_\lambda |\} \leq 1$.

Without loss of generality[1], we can assume that $\langle b_0 \rangle_\lambda \geq \langle b_1 \rangle_\lambda \geq 0$, which leads to $|S_\lambda| \leq 2\langle b_0 \rangle_\lambda \leq 2$, and thus $|S| \leq 2$. We summarize the result by stating that the following CHSH inequality holds for any local-realistic theory:

$$|E_{00} + E_{01} + E_{10} - E_{11}| \leq 2. \tag{2.13}$$

2.1.2 CHSH violation with polarization-entangled photons

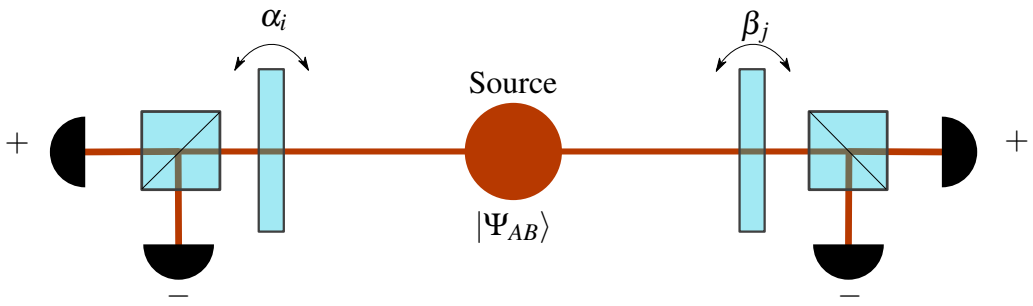


Figure 2.2: A CHSH-type Bell test with photons. A source distributes polarization-entangled photon pairs to Alice and Bob. A half-wave plate (HWP) and a polarization beam splitter (PBS) define the measurement basis for Alice and Bob. Alice (Bob) chooses between two measurement bases α_0 and α_1 (β_0 and β_1) corresponding to different HWP angles. In every measurement round, each party independently chooses a measurement basis. If the "+" ("-") detector fires, the output is labeled as +1 (-1).

We consider now the QM prediction for the expected Bell violation in an experiment involving a pair of polarization-entangled photons in a maximally entangled state

$$|\Psi_{AB}\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle) \tag{2.14}$$

distributed to Alice and Bob (Fig. 2.2). Horizontal and vertical polarizations are represented by H and V, respectively. A half-wave plate (HWP) and a polarization beam splitter (PBS) define different measurement bases. Alice and Bob independently choose measurement settings x and y by rotating their HWPs so that a photon transmitted through the PBS is projected into the state $|\alpha_x\rangle$ and $|\beta_y\rangle$, respectively, registering a result in the "+" detectors. An event in the "-" detectors signifies that the incoming state was projected onto states $|\alpha_x + 90^o\rangle$ and $|\beta_y + 90^o\rangle$.

[1] We lose no generality by assuming that we have serendipitously assigned outcomes for which the "+1" labeled event tends to occur for both measurement settings b_0 and b_1, allowing $\langle b_0 \rangle_\lambda, \langle b_1 \rangle_\lambda \geq 0$; the label assignment is arbitrary and independent for each setting.

The detection event "+"("-") is represented by the +1(-1) outcome in the CHSH expression. When the four measurement settings are set as $\alpha_0 = 0^o$, $\alpha_1 = 45^o$, $\beta_0 = 22.5^o$, $\beta_1 = -22.5^o$, QM predicts

$$E_{00} = E_{01} = E_{10} = \frac{1}{\sqrt{2}}, \qquad E_{11} = -\frac{1}{\sqrt{2}}, \tag{2.15}$$

resulting in $|S| = 2\sqrt{2} > 2$ (Eq. 2.13), which is incompatible with any local-realistic theory.

2.2 Loopholes in Bell tests

The formulation of the Bell inequality shown in the previous section required meeting several conditions, including space-like separation between parties. When these conditions are not met in an experiment, one could come up with a local-realistic theory that accounts for observed violations, and the Bell test is said to be "open to loopholes". The three loopholes usually considered are detection, locality, and freedom-of-choice. Although a Bell violation was first experimentally demonstrated in 1972 [65], these three loopholes have only been closed simultaneously in 2015 due to the significant technological hurdles that have to be overcome for these experiments [20–22].

2.2.1 Detection loophole

In an experimental Bell test, transmission losses between the source and the measurement devices, as well as the finite detector efficiencies, result in measurement rounds where no detector fires for either party. One could discard these measurement rounds and evaluate the Bell inequality based only on the subset of results where both detectors fire. However, this assumes that the accepted data constitutes a fair sample of all the data that could be collected assuming unit system efficiencies. As pointed out by Ref. [25] and Ref. [26], there exists a local-realistic model that exploits the fair-sampling assumption: only photons that favor a Bell violation are selectively detected. Consequently, a minimum detection efficiency is necessary to ensure that a representative sample is collected.

Although it is intuitively appealing to favor using maximally entangled states for violating a Bell inequality, the minimum efficiency required for closing the detection loophole is actually lower with non-maximally entangled states (66.7% instead of 88.3%) [2, 26]. We briefly outline how this result was obtained by Eberhard.

Eberhard derived a Bell inequality[2] that took into account finite detector efficiencies by assigning a "no-click" event with a label "u", in addition to the labels "+" and "-" assigned to the two detected outcomes at each side (see Section 2.1.1).

$$\begin{aligned} J^{\text{ideal}} &= n_{+-}(\alpha_0,\beta_1) + n_{+u}(\alpha_0,\beta_1) + n_{-+}(\alpha_1,\beta_0) \\ &\quad + n_{u+}(\alpha_1,\beta_0) + n_{++}(\alpha_1,\beta_1) - n_{++}(\alpha_0,\beta_0) \geq 0. \end{aligned} \tag{2.16}$$

A QM prediction involves evaluating terms such as

$$n_{++}(\alpha_0,\beta_0) = N\eta^2 \langle\Psi|\,|\alpha_0,\beta_0\rangle\langle\alpha_0,\beta_0|\,|\Psi\rangle := \langle\Psi|\hat{M}|\Psi\rangle, \tag{2.17}$$

where N is the total number of pairs generated by the source, η is the detection efficiency (assumed equal for every detector) and $|\Psi\rangle$ is a non-maximally entangled state parameterized by r

$$|\Psi\rangle = \frac{1}{\sqrt{1+r^2}}\left(|HV\rangle + r|VH\rangle\right). \tag{2.18}$$

Background counts of $N\zeta$ are taken into account by considering instead $J = J^{\text{ideal}} + 2N\zeta$. The corresponding QM prediction is then $J = \langle\Psi|\hat{B}|\Psi\rangle$, where $\hat{B}$ is constructed with operators such as $\hat{M}$ in Eq. 2.17, and a multiple of the identity $2N\zeta\mathbb{1}$.

To observe a Bell violation, Eberhard noted that experimental conditions must allow for a QM prediction where $J < 0$. To consider the worst-case scenario, he numerically varied α_x, β_y, r and η, and looked for the maximum background rate ζ which flipped the last negative eigenvalue of $\hat{B}$ to a positive value. For $\eta < 2/3$, no maximum ζ could be found that meets this condition – no Bell violation is possible. For $\eta \geq 2/3$, the results (Fig. 2.3) show that when a violation is possible, the optimal entangled state does not necessarily correspond to a maximally entangled state.

The detection loophole was first closed with entangled ions [18], and then later with entangled photons by using near-unit efficiency single-photon detectors (transition-edge sensors) [19]. In the latter experiment, the loophole was closed with only two detectors, which can be shown to be possible by rewriting the Eberhard inequality in a form involving only a single "+" outcome for each observer:

$$\begin{aligned} J &= S_+(\alpha_0) + S_+(\beta_0) \\ &\quad - n_{++}(\alpha_0,\beta_1) - n_{++}(\alpha_1,\beta_0) + n_{++}(\alpha_1,\beta_1) - n_{++}(\alpha_0,\beta_0) \geq 0, \end{aligned} \tag{2.19}$$

[2] An intuition behind the form of this inequality and how it relates to a Bell violation using a non-maximally entangled state is provided later in the text via Eq. 2.20.

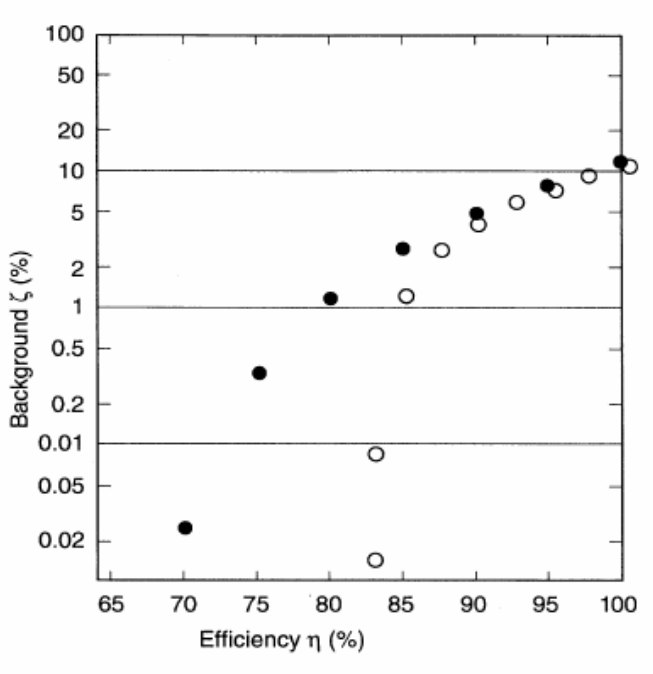


Figure 2.3: Maximum affordable background vs. efficiency for observing a Bell violation: (black dots) obtained by optimizing both a non-maximally entangled state and measurement settings, (white dots) obtained with a maximally entangled state but with optimized measurement settings. Image credit: Ref. [2].

where S_+ indicate single counts at the appropriate detector. Rewriting the inequality as

$$n_{++}(\alpha_0,\beta_1)+n_{++}(\alpha_1,\beta_0)-n_{++}(\alpha_1,\beta_1)+n_{++}(\alpha_0,\beta_0)\leq S_+(\alpha_0)+S_+(\beta_0) \tag{2.20}$$

allows us to intuitively understand why a non-maximally entangled state is more suitable than a maximally entangled state for observing a Bell violation: essentially, using a small value of r, one can choose α_0 and β_0 to nearly block the remaining photons (mainly $|HV\rangle$) from $|\Psi\rangle=(|HV\rangle+r|VH\rangle)/\sqrt{1+r^2}$, thereby reducing the RHS of the inequality in Eq. 2.20, while an appropriate choice of α_1 and β_1 maximizes the LHS [66].

The Eberhard-type inequality was later shown to be equivalent to the CHSH-type inequality [67–69]. We will adopt the CHSH-type inequality for the rest of the thesis, and show how it can be evaluated in a scenario involving only two detectors with finite efficiencies (Section 2.3).

2.2.2 Locality and Freedom-of-choice loopholes

The Bell inequality was constructed assuming that distant parties are unable to signal to one another to affect their measurement outcomes (Eq. 2.1). This is experimentally fulfilled by ensuring that the time required to complete a measurement process is shorter than the time taken for the speed of light to travel from one party to another (Condition I). Additionally, since the parties typically measure systems that share a common source, e.g. each measuring a photon from an entangled photon pair source, they must ensure that their measurement setting is not

correlated with any unknown causal influence originating from the source (Eq. 2.3). Otherwise, their measurement settings cannot be assumed to be independent, creating a "freedom-of-choice" loophole. This loophole is closed by using distinct random number generators to select the measurement settings at Alice and Bob, and space-like separating these devices from the photon pair source (Condition II).

Failure to satisfy both Conditions I and II is known as as the "locality" loophole. A space-time diagram illustrating the space-like separation of the various components necessary for closing this loophole is shown in Fig. 2.4.

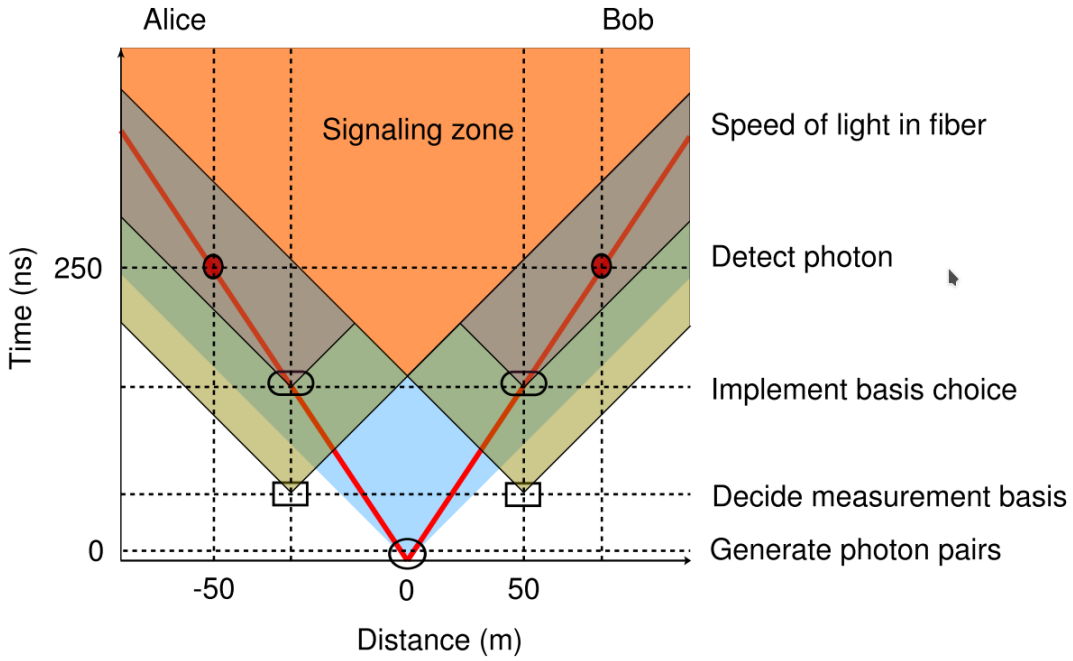


Figure 2.4: Closing the locality loophole requires various events in a Bell experiment to be space-like separated. Thin lines represent the speed of light defining the forward light cones for each event. In this example, the loophole is closed with polarization-entangled photon pairs. The red line represents photon propagation in fibers used for distributing photons to Alice and Bob. Photodetection events (red dots) are space-like separated from each other, and must be completed outside the signaling zone so that measurement outcomes of each party depend only on local measurement settings (basis choices for measuring polarization). The measurement settings have to be completed outside the forward light cone of the photon pair generation event (blue cone). This ensures that the choices are independent and not correlated through any unknown causal influence that could be associated with the pair source. Image Credit: Ref. [1].

The locality loophole was first closed by Aspect *et al.* with polarization-entangled photons, enabled by fast polarization switches that rapidly changed measurement settings compared to photon transit times [17]. In this thesis, we close only the detection loophole with high-

efficiency photodetectors and choose to focus on a novel procedure that organizes detection outcomes from a continuous pair source. A fast polarization switch has been developed in our group for closing the locality loophole in future experiments [1].

2.3 Bell test for a continuous entangled photon source

In this section, we present a scheme that organizes detection events from a continuous source of polarization-entangled photon pairs. The measurement scenario is shown in Fig. 2.1.2, except that Alice and Bob have one detector each. Detection events are organized into measurement rounds with uniform time bins of duration τ, each bin possibly containing multiple detection events. Fig. 2.5 shows the event labeling scheme: detection of one or more events is labeled as "-", while not detecting a photon is assigned a "+". When the measurement settings are at xy, these outcomes from N measurement rounds are used to estimate the correlation

$$E_{xy} = \frac{N_{++} + N_{--} - N_{+-} - N_{-+}}{N}, \tag{2.21}$$

where N_{ij} the number of events corresponding to outcome ij.

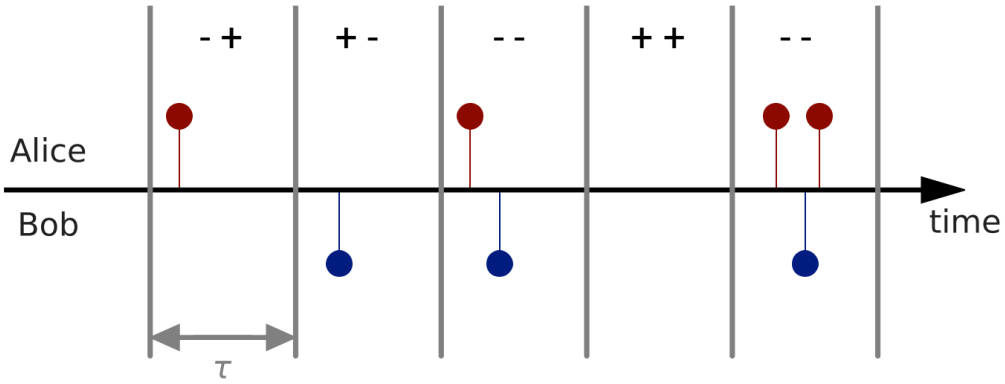


Figure 2.5: Time binning scheme. A stream of photodetection events at Alice (red) and Bob (blue) are organized into measurement rounds using uniform time bins of duration τ. Detection of one or more events is labeled "-", while not detecting any photons is assigned "+". The labels are used to evaluate the CHSH expression with Eqns. 2.21 and 2.6. Evidently, the labels for each measurement round changes as τ is varied. Optimizing τ allows us to obtain a maximal CHSH violation or randomness generation rate for a given photon detection rate (Section 3.4). Image Credit: Ref. [3].

We now describe the model used to predict the maximal CHSH violation. The source presented in Chapter 3 generates photon pairs using a spontaneous parametric down-conversion

process (SPDC). For a continuously-pumped SPDC process, the emission of independent pairs can be described with Poissonian statistics of average μ, given that the coherence time of each photon is much shorter than the length of a measurement round τ. We first consider the probability $P_Q(\alpha,\beta)$ of obtaining the classical information $\alpha,\beta \in \{+,-\}$, assuming perfect detector efficiencies, with a single photon pair:

$$P_Q(\alpha,\beta|x,y) = \mathrm{Tr}(\rho \Pi_\alpha^x \otimes \Pi_\beta^y), \tag{2.22}$$

where Π's are measurement operators.

We now consider the realistic scenario where Alice's and Bob's detector efficiencies are η_A and η_B, respectively. In a single round consisting of multiple photon pairs, if some of the pairs result in $\alpha = -$ ($\beta = -$), Alice's (Bob's) detector may be triggered, leading to the observed outcome $a = -1$ ($b = -1$).

Since each correlation term may be expressed as

$$E_{xy} = 1 - 2P(-1,+1|x,y) - 2P(+1,-1|x,y), \tag{2.23}$$

we need only calculate $P(-1,+1|x,y)$ and $P(+1,-1|x,y)$.

For each pair generated by the source, the probability $P(\alpha,+|x,y)$ is contributed by cases (i) Bob's detector did not fire even though the detector was ideal ($\beta = +$) and (ii) Bob's detector fails to fire due to finite detector efficiency (occurring with probability 1-η_B for every photon). Thus, the probability of event α is

$$D(\alpha) := P_Q(\alpha,+|x,y) + (1-\eta_B) P_Q(\alpha,-|x,y). \tag{2.24}$$

For v generated pairs, $P(-1,+1|x,y)$ is contributed by cases where at least one of the α's is $-$. Suppose that there are k instances $\alpha = -1$: the result $a = -1$ can be obtained with probability $1-(1-\eta_A)^k$, corresponding to at least one successful detection by Alice's imperfect detector. There are exactly $\binom{v}{k}$ such configurations since it does not matter which k of the v photons arriving at Alice result in $\alpha = -1$. The probability of obtaining $a = -1$ given that v photon pairs were generated in a single round is then

$$D_v = \sum_{k=1}^{v} \binom{v}{k} [1-(1-\eta_A)^k] D(-)^k D(+)^{v-k}. \tag{2.25}$$

Taking into account the Poissonian statistics of the source, this results in

$$P(-1,+1|x,y) = \sum_{v=0}^{\infty} P_{\mu}(v) D_v \,. \tag{2.26}$$

The model is slightly modified taking into account the Poissonian probability $P_{\mu_b}(0)$ that Bob's detector does not fire due to background events, corresponding to $b = +1$ in Eq. 2.26. The mean number of background events per round is represented by μ_b. Following a similar procedure, we obtain $P(+1,-1|x,y)$, which finally allows us to evaluate E_{xy} (Eq. 2.23) and the CHSH parameter S (Eq. 2.6).

The maximal S value is predicted by optimizing the state $\rho = |\Psi\rangle\langle\Psi|$ described by Eq. 2.18, and the polarization-state projection operators Π's in Eq. 2.22. The detection efficiencies, generated photon pair rate, and background count rate, are fixed during the optimization process by characterizing our experimental setup (Chapter 3). The resulting S evaluated over several values of τ is presented in Fig. 3.17.

2.4 Randomness Extraction Protocol

To extract random numbers from the output generated by a sequence of Bell measurements, we use the randomness expansion protocol described in [70] with a randomness extractor [57]. Compared the previous protocols [71, 72], the protocol in [70] does *not* assume that each measurement round is identical (e.g. the generated entangled state does not fluctuate) and independent (e.g. measurement devices have no memory) from each other (i.i.d.), and is therefore more general and relevant to real-world applications.

Implementing the extraction protocol and the extractor was performed by my colleagues Jean-Daniel Bancal, Le Phuc Thinh, and Alessandro Cerè. For completeness, the protocol is briefly outlined in this section, along with the predicted randomness generation rate. Their contribution is fully described in [30].

We first adopt the notations and labels used in [70]. The measurement outcomes are now labeled as $a,b \in \{0,1\}$, while the measurement settings are labeled the same as before with $x,y \in \{0,1\}$. The Bell test is thought of as a game which is won when $a \oplus b = x \cdot y$, where each measurement round is assigned a a score

$$w_{\text{CHSH}}(a,b,x,y) = \begin{cases} 1 & \text{if } a \oplus b = x \cdot y \,, \\ 0 & \text{otherwise} \,. \end{cases} \tag{2.27}$$

For this "CHSH-game", the winning probability is $w = 1/2 + S/8$ in terms of the CHSH value.

A randomness expansion protocol consumes a r-bit random "seed" R, and generates an m-bit string Z of almost uniform randomness. Device-independent security for the protocol in [70] is achieved as follows: Alice and Bob play the CHSH game with their devices in order to test if they are faulty or malicious. A fraction of all the measurement rounds are committed to this test. When a sufficient number of rounds wins the CHSH game, the remaining rounds are consumed to extract randomness. Otherwise, they abort.

Protocol Security

The desired level of security is bounded by the user, who specifies the "soundness" ε_s and "completeness" ε_c parameters:

1. **Completeness**
   The protocol aborts with probability

   $$\Pr[\text{abort}] \leq \varepsilon_c, \tag{2.28}$$

   when Alice and Bob "honestly" implement the protocol with their devices. An upper bound ensures that users do not arbitrarily abort the protocol, but do so for a valid reason, e.g. due to statistical fluctuations (Eqns. 2.31 and 2.32).

2. **Soundness**
   For any implementation of the device the protocol either aborts or returns a random string Z with probability

   $$(1 - \Pr[\text{abort}]) \left\| \rho_{ZRE} - \rho_{U_m} \otimes \rho_{U_r} \otimes \rho_E \right\|_1 \leq \varepsilon_s \,, \tag{2.29}$$

   where E is the adversary's system, and ρ_{U_r} and ρ_{U_m} are completely mixed states describing systems R and Z.

   This upper bound ensures that when the protocol returns a random string, the overall system, described by ρ_{ZRE}, does not deviate too much from the ideal situation where systems Z and R are completely uncorrelated with E, so that a perfectly random and secret string is produced for the user.

Protocol Implementation

The protocol takes parameters γ, the expected number of test rounds, ω_{exp}, the expected winning probability for an honest (perhaps noisy) implementation and δ_{est}, the width of its statistical interval; values used to define the abort criteria (Eq. 2.31). In an execution, for every measurement round $i \in \{1,...,n\}$:

1. Bob chooses a random bit $T_i \in \{0,1\}$ such that $\Pr(T_i = 1) = \gamma$ using the interval algorithm [73].

2. If $T_i = 0$ (randomness generation), Alice and Bob choose deterministically $(X_i, Y_i) = (0,0)$, otherwise $T_i = 1$ (test round) they choose uniformly random inputs (X_i, Y_i).

3. Alice and Bob use the physical devices with the said inputs (X_i, Y_i) and record their outputs (A_i, B_i).

4. If $T_i = 1$ (test), they compute

$$C_i = w_{\text{CHSH}}(A_i, B_i, X_i, Y_i)\,. \tag{2.30}$$

They abort the protocol if

$$\sum_j C_j < (\omega_{\text{exp}}\gamma - \delta_{\text{est}})n, \tag{2.31}$$

where j is the index of test rounds, otherwise they return $\text{Ext}(\mathbf{AB}, \mathbf{Z_s})$ where Ext is a randomness extractor, $\mathbf{AB} = A_1B_1...A_nB_n$ and $\mathbf{Z_s}$ is a uniformly random seed.

Ensuring an honest implementation

The winning probability from the CHSH-test rounds is expected to be concentrated around ω_{exp} within an error tolerance limit δ_{est}. Thus, when Alice and Bob implement the protocol honestly [70], they should not be aborting too often;

$$\Pr[\text{abort}] \leq \exp(-2n\delta_{\text{est}}^2) =: \varepsilon_{\text{est}}\,. \tag{2.32}$$

The parameter ε_{est} is related to the completeness security parameter ε_{c}, and is set by the user. Similarly, it is necessary to consider the error tolerance ε_{SA} that characterizes the abort probability for the interval algorithm generating n bits $T_1, \ldots, T_n$ [3]. This raises the total completeness and soundness by ε_{SA}, with the total completeness $\varepsilon_{\text{c}} = \varepsilon_{\text{SA}} + \varepsilon_{\text{est}}$.

[3] For the interval algorithm [73], $\varepsilon_{\text{SA}} = \exp(-18h(\gamma)^3 n/\max\{\log\gamma^{-1}, \log(1-\gamma)^{-1}\})$ where $h(p) := -p\log_2 p - (1-p)\log_2(1-p)$ is the binary entropy function [70].

Randomness extraction rate with a Trevisan extractor

The results from a set of Bell measurements are not *a priori* uniformly distributed. To extract uniformly-random bits from the results, a widely-used technique involves multiplying with a Toeplitz matrix whose elements are defined by a uniformly-random bit sequence (a random "seed"). However, this technique requires a seed linear in the length of the output and results in consuming more random seeds that it produces [74].

In this work, we use a Trevisan extractor instead, as it requires only a seed polylogarithmic in the length of the output [57]. The extractor uses the seed more efficiently since it generates every bit using a one-bit extractor whose output is approximately independent of the seed – this allows reusing portions of the seed for generating each bit [74, 75].

The performance of the Trevisan extractor is defined by the completeness and security parameters ε_c and ε_s. We apply the extractor to generate m bits of randomness from n measurement rounds

$$m = n \cdot \eta_{\text{opt}}(\varepsilon', \varepsilon_{\text{EA}}) - 4\log n + 4\log \varepsilon_{\text{EX}} - 10\,, \tag{2.33}$$

where $(\varepsilon', \varepsilon_{\text{EA}}, \varepsilon_{\text{EX}})$ are auxiliary security parameters selected to achieve the prerequisite completeness and soundness ($\varepsilon_c = \varepsilon_s = 10^{-10}$), and the entropy rate η_{opt} depends on ω_{exp} and γ [30, 70]. The quantity $n \cdot \eta_{\text{opt}}$ lower bounds the amount of private randomness belonging to Alice and Bob consistent with their experimental output **AB** when the user does not abort the protocol. Deriving this quantity was the main effort in [70].

The extractable random bit per round is then given by

$$r_n = \left(\eta_{\text{opt}}(\varepsilon', \varepsilon_{\text{EA}}) - 4\frac{\log n}{n} + 4\frac{\log \varepsilon_{\text{EX}}}{n} - \frac{10}{n} \right). \tag{2.34}$$

The expected fraction of test rounds is fixed at $\gamma = 0$ to examine the randomness extracted from all n rounds. In the limit $n \to \infty$, the asymptotic number of random bits is given by

$$r_\infty = 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{\frac{S^2}{4} - 1} \right). \tag{2.35}$$

From this, the randomness rate r_n/τ, where τ is the duration per measurement round, can be estimated by using ω_{exp} observed from several Bell measurement rounds as input. The randomness rate changes as a function of τ, and is discussed in Section 3.4.3 alongside details pertaining to the experimental setup.

Chapter 3

Randomness extraction from a detection loophole-free Bell experiment

This chapter describes the experimental implementation of a detection loophole-free Bell test, and the extraction of randomness from its measurement results. Sections 3.1 and 3.2 describe the high-efficiency single-photon detectors and polarization-entangled pair source used to close the detection loophole. The entangled state of photons emitted by the source and measurement bases are optimized for maximal Bell violation using the model described previously, before measuring polarization correlations in Section 3.3. For the binning strategy used to organize the stream of measurement outcomes from our CW source, there exists also an optimal bin width that maximizes the violation (Section 3.4.1). Interestingly, we observe a different optimum bin width for measuring a maximal violation and for obtaining the maximal randomness generation rate (Section 3.4.2). To extract uniformly random bits, we chose to optimize the randomness generate rate. In Section 3.4.3, we report on the quantum random number expansion protocol and extractor described in the previous chapter, leading to a random bit generation rate of ≈ 240 bits/s.

3.1 High-efficiency detectors

To close the detection loophole, we used[1] tungsten-based transition-edge sensors (W-TES) provided by Sae Woo Nam's group at NIST, which has a highest measured detection efficiency of more than 99 % and very low detector noise [28]. Absorption efficiency is enhanced around

[1] Although Superconducting Nanowire Single-Photon Detectors (SNSPD) (efficiency ≈ 93 %) have timing jitters smaller than the TES by two orders of magnitude, and loophole-free Bell tests have indeed been demonstrated with these devices [76], we chose the TES due to its higher efficiency and availability.

810 nm by embedding the W-TES within a multilayered optical structure which includes an anti-reflective coating on top, and a highly reflective mirror below the device [28]. Each TES is mounted on top of a sapphire rod centered inside a standard telecommunications fiber ferrule sleeve designed to hold an anti-reflection coated, SMF-28e FC/UPC fiber connector 50 μm from the detector. This ensures optimal alignment of the fiber output and the detector surface (25 μm $\times$ 25 μm) [77].

3.1.1 Operating principle

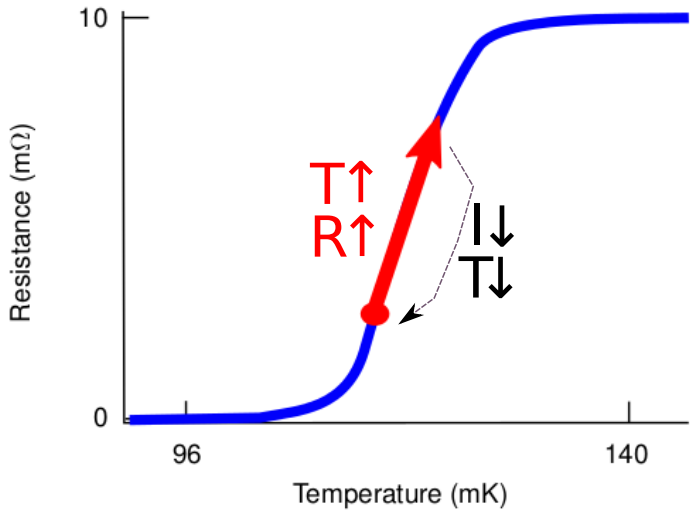


Figure 3.1: Conceptual representation of the resistance (R) dependence on temperature (T) of a TES. The steep phase transition suggests its use as a sensitive calorimeter. When a single photon is absorbed, the TES temperature increases, resulting in an increase is resistance (red arrow). As the TES is voltage-biased, its current subsequently decreases, resulting in decreased Joule heating of the device, returning it to its original operating point (red dot). Image credit: Ref [1].

A TES is a microcalorimeter that measures the heat deposited by impinging photons. It consists of an absorber for incident energy, a thermometer that measures the change in temperature and a weak thermal link to a heat sink that resets the device. Electrons in tungsten perform the role of the absorber and the thermometer. Anomalously low thermal coupling between the electrons and phonons in tungsten provides the weak thermal link [78].

The device derives its photon-number-resolving sensitivity by operating in the narrow temperature region (about 1 mK wide) between its normal and superconducting state, where its electrical resistance (R) varies sharply with temperature (T).

During operation, the TES is cooled to below its superconducting transition temperature ($T_c = 140\,\text{mK}$). By applying a voltage bias, Joule heating of the electrons raises their temperature to T_c. This temperature is stabilized within the transition edge through negative electro-thermal feedback (ETF): when T increases above T_c, R increases and causes a decrease in Joule heating ($\propto V^2/R$). Consequently, the device cools back to T_c. Similarly, when T decreases, Joule heating increases and the device heats back to T_c. In this way, temperature is self-regulated [78].

When a photon is absorbed by the TES, it produces a photoelectron which heats up the surrounding electrons. Due to weak electron-phonon thermal coupling, energy is not immediately dissipated away: the device heats up and its resistance increases partway along the transition-edge. The corresponding drop in current (I) is then read out inductively through a Superconducting Quantum Interference Device (SQUID).

When additional photons impinge the detector, its resistance continues to increase along the transition edge in proportion to the number of photons detected (for a monochromatic source); the device is photon-number-resolving and has no intrinsic deadtime.

The rise time of the combined TES-SQUID output signal is typically tens of nanoseconds and is limited by the SQUID input inductance (L_{in}) and the shape of the transition-edge [79]. The thermal relaxation time of the signal is typically a few microseconds, and depends on the strength of the negative ETF which in turn depends on voltage bias of the TES: a strong reduction of Joule heating proportional to this voltage results in faster re-thermalization. However, a too high voltage causes the temperature to overshoot its operating point, resulting in undesirable electro-thermal oscillations [1, 80]. A large enough bias voltage is thus sought to heat the TES to its transition edge, but it has to be small enough to ensure stable operation.

3.1.2 Implementation

Cryogenics

Our TES is kept at an ambient temperature of 75 mK using an adiabatic demagnetization refrigerator cryostat (ADR) built by Entropy[2]. We briefly describe the magnetocaloric effect used to achieve this temperature [81]. A pulse-tube cooler first provides a base temperature of $\approx 3\,\text{K}$ at the "4 K-stage" for the TES and a collection of paramagnetic salts (Ferric Ammonium Alum, FAA) that have been pre-aligned with a magnetic field. Fig. 3.3 shows four TES in a copper housing on top of a copper rod (cold finger) that is thermally connected to the FAA salts. A heat switch providing thermal contact between the TES and the 4 K stage is then

[2]Entropy GmbH Gmunder Str. 37a, D-81379 München

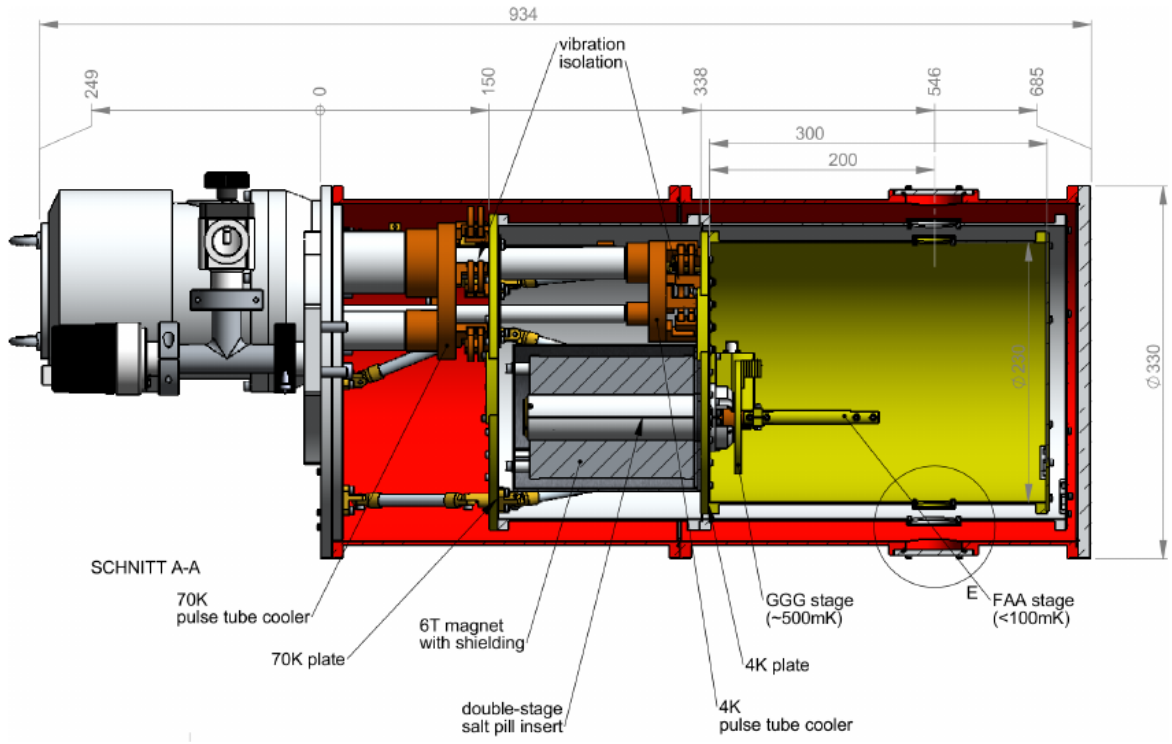


Figure 3.2: Sketch of cross section of the ADR: The inner structure of the ADR with the various temperature stages is depicted: The top flange (left) with red shielding is called the 300 K-stage as it is at room temperature. Enclosed are the 70 K-stage (light grey), the 4 K-stage (light green), the GGG stage (~ 500 mK) and the FAA-stage (< 100 mK). Not depicted are the transition-edge sensors (TES) and Superconducting Quantum Interference Device (SQUID) mounted on the FAA-stage. Image credit: Entropy GmbH.

switched off, so that the detectors are only in thermal contact with the FAA salts. Then, the magnetic field is ramped down slowly, causing the magnetic dipoles of the salts to misalign. The increased entropy of the salts results in a corresponding reduction in temperature of the detectors to as low as 30 mK for our system. A PID control loop stabilizes the temperature at 75 ± 0.03 mK by controlling a current in the superconducting electromagnet applying the magnetic field. The PID lock stops working when the current has reached 0 A. The temperature hold time is approximately 8 hours.

Signal Amplification

A schematic of the TES biasing and readout electronics is shown in Fig. 3.5. Voltage biasing of the TES was provided by a current source ($I_{\mathrm{TES}} \approx 40\,\mu$A) through a shunt resistor ($R_{\mathrm{shunt}} = 20\,\mathrm{m}\Omega$) connected in parallel to the TES (R_{TES} is typically a few ohms or less [80]). Current

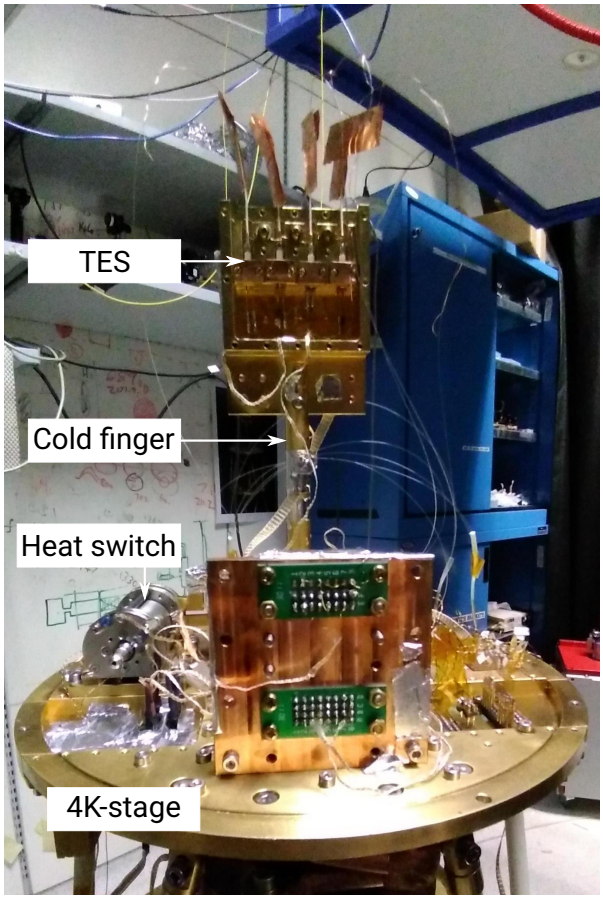


Figure 3.3: Four transition-edge sensors (TES) mounted on top of a copper "cold finger". The cold finger has a base temperature of about 3 K due to thermal contact to the 4 K-stage. After disconnecting the thermal contact with a heat switch, adiabatic demagnetization (see main text) of a collection of magnetic salts at the base of the cold finger lowers its temperature to the TES operating point (75 mK). Copper wires on the mount provide structural support to the optical fibers (SMF-28e) connected to the TES, reducing bend loss. The wires also thermalize the fibers to the mount temperature.

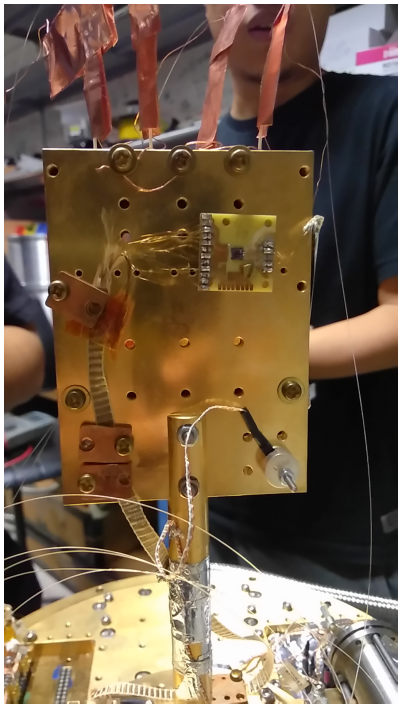


Figure 3.4: An integrated chip containing two Magnicon SQUID Arrays mounted on the reversed side of the mount supporting the TES (Fig.3.3). Superconducting niobium-titanium wires (chip left) connect the SQUIDs to room temperature electronics, reducing thermal conductivity between the 4 K-stage and the SQUIDs. Similar wires (chip right) are used to connect each SQUID to a TES, reducing Joule heating along the wire.

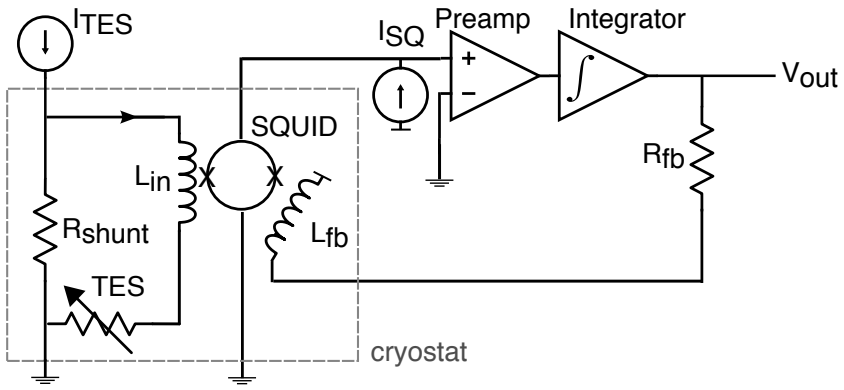


Figure 3.5: Schematic of the TES biasing and readout electronics. The TES is voltage-biased by a constant current source I_{TES} through shunt resistor $R_{\mathrm{shunt}} \ll R_{\mathrm{TES}}$. The SQUID array amplifier picks up changes in TES resistance from L_{in}. The signal is further amplified outside of the cryostat. Signal feedback via R_{fb} and coil L_{fb} linearizes the SQUID response.

changes in the TES is inductively picked up and amplified by a SQUID series array (Magnicon C7), followed by further signal conditioning (Magnicon XXF-1 electronics and Stanford Research Systems SR560 Preamplifiers) at room temperature with an overall amplification bandwidth of ≈2 MHz. The SQUIDs were mounted as close to the TES as possible to reduce parasitic inductance and kept at the same ambient temperature (Fig. 3.4).

We operate the SQUID in a flux-locked loop (FLL) [82] to linearize its response and also minimize low frequency components of the noise. Operating the SQUID in FLL mode greatly eases the optimization of the TES bias voltage: FLL ensures that the dc magnetic field environment around the SQUID is locked at a pre-determined level where the SQUID is most sensitive to magnetic field changes. This allows us to adjust I_{TES} without inadvertently disturbing the optimal operating point of the SQUID through corresponding current changes in the input inductance L_{in}.

Heat conduction and unintended Joule heating in the wiring were minimized – both electrical wiring and optical fibers were heat sunk at the various cooling stages of the ADR to minimize heat conduction to the detectors. The TES and SQUIDs were electrically connected with superconducting niobium-titanium wires, reducing Joule heating. The same type of wire was used for connecting the SQUIDs to room-temperature electronics; superconducting materials have low thermal conductivity, which minimizes heat conduction from the '4 K-stage' to the TES. To reduce pickup noise, we used these wires in a twisted pair geometry.

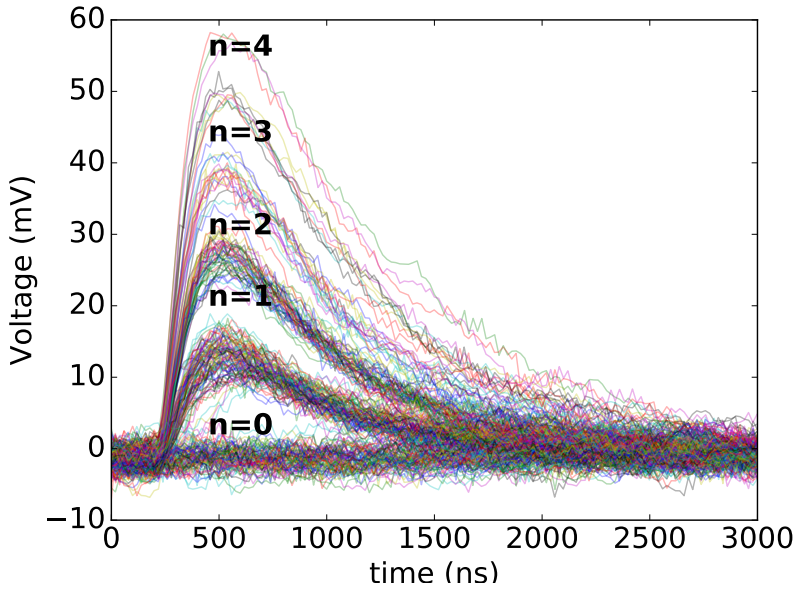


Figure 3.6: Detector response to 810 nm photons from a pulsed laser diode. The photon number n contained in each pulse follows a Poissonian distribution.

3.1.3 Device optimization and characterization

TES Voltage Bias

To observe the TES response for various I_{TES}, we use a laser diode centered at 810 nm as a light source, operated in pulsed mode. We control the average photon flux with a variable attenuator, then launch the light into a fiber (SMF-28e) that directs it to the TES.

Fig. 3.6 shows a persistence plot of TES voltage traces demonstrating its photon-number-resolving capability. To improve signal-to-noise ratio, we histogram the maximal height of the traces (Fig. 3.7) and adjust I_{TES} to increase the separation between the height distributions corresponding to $n = 0$ and $n > 0$ photodetection events.

Signal Discrimination

To distinguish a photodetection event from background noise, we pre-process the signal using a Schmitt trigger implemented via discriminators at two levels [83]: a qualifier flag is raised when the signal passes threshold V_{high} (Fig. 3.8(a), point A) and lowered by the first subsequent crossing of threshold $V_{\mathrm{low}} = 0\,\mathrm{mV}$ (point B). Using two threshold levels creates a discriminator that is inherently robust against false-triggering – this is evident in Fig. 3.8(a), which shows the

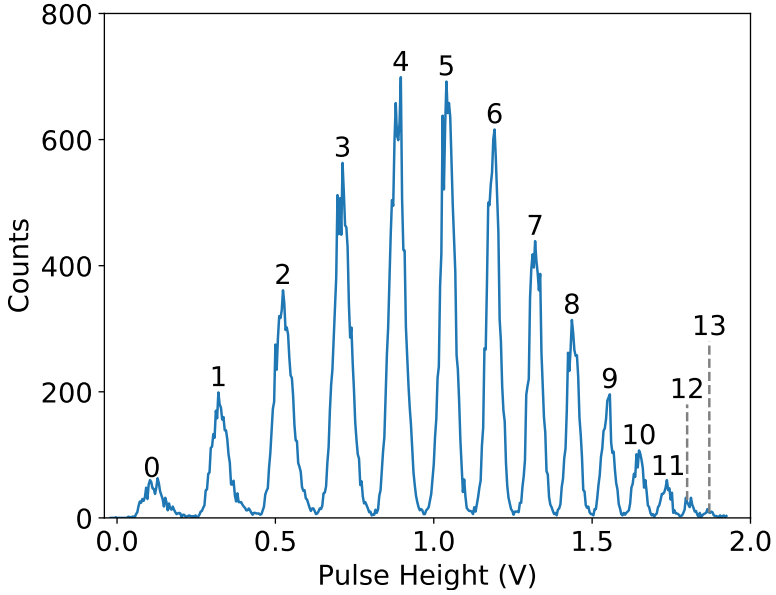


Figure 3.7: Pulse-height distribution from our TES photon counter in response to a 810 nm pulsed laser. The photon number peaks for 0, 1, ..., 13 are clearly resolved. High signal-to-noise ratios reduce dark counts to less than 20 Hz. The average photon number per pulse is about 5 for this acquisition.

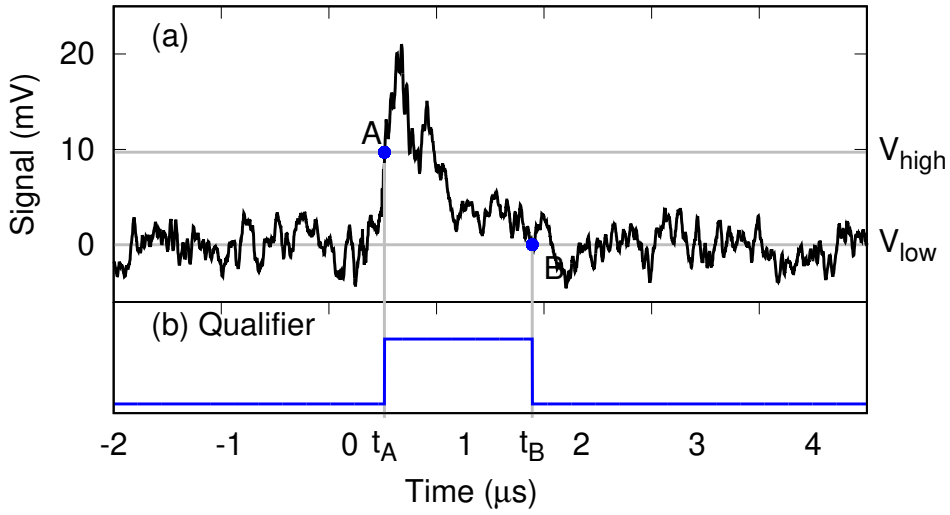
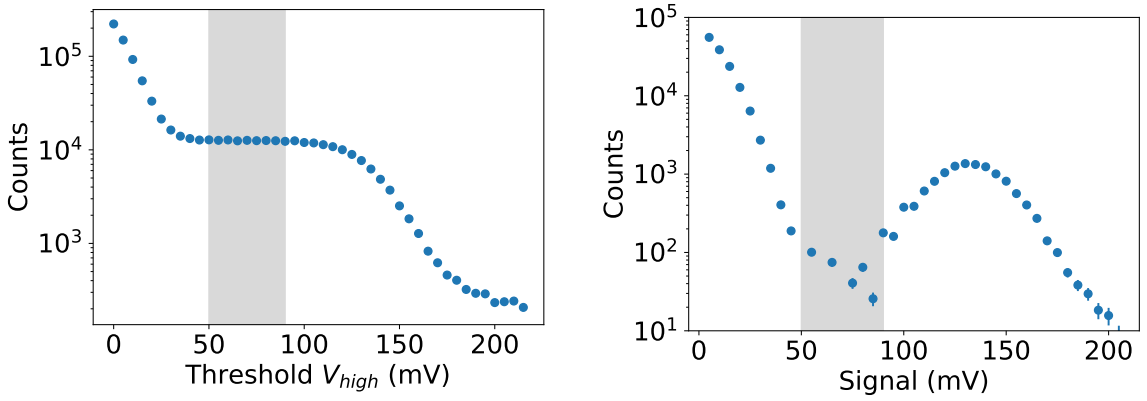


Figure 3.8: (a) Typical TES signal trace with a single 810 nm photon after magnification by Magnicon SQUIDs and XXF-1 readout electronics. The horizontal lines show the high and low threshold settings of the Schmitt trigger mechanism. (b) Qualifying interval AB identified by the Schmitt trigger.



(a) **(b)**

Figure 3.9: (a) Measured photon counts over 1 s as a function of the threshold V_{high} of the Schmitt trigger. For this acquisition, 810 nm photons distributed to Alice, generated from our continuously-pumped SPDC-based entangled photon source, was measured. (b) Pulse-height distribution corresponding to the measured counts in (a). Grey area: region separating $n = 0$ and $n = 1$ photon detection events. We fine-tune the value of V_{high} within this region to maximize signal-to-noise ratio.

Schmitt trigger activating only once due to a single-photon detection event even though the TES signal fluctuates about V_{high} due to detector noise.

We record t_A as the detection time of the photon with a time-stamp card at a resolution of 2 ns. One disadvantage of this method is that it will not register additional photons arriving between t_A and t_B: an artificial dead time which varies with the two threshold levels is introduced, resulting in a flux-rate dependent detection efficiency. A solution to this problem is presented in Chapter 4 but was not implemented in the Bell test presented in this chapter due to the additional computational resources required. The improvement to the overall detection efficiency and the corresponding increase in randomness generation rate from the Bell experiment, are estimated in Section 4.6.

The optimal value for V_{high} is chosen by measuring the count rate as V_{high} is increased. The count rate drops rapidly when V_{high} is increased from a low value, corresponding to the gradual rejection of electronic noise. The first plateau (Fig. 3.9a grey area) encountered in this measurement corresponds to the region separating events triggered by electronic noise and photodetection events with $n > 0$. The best value of V_{high} for each TES corresponds to the value which maximizes its heralding efficiency while keeping its dark-count rate to a minimum.

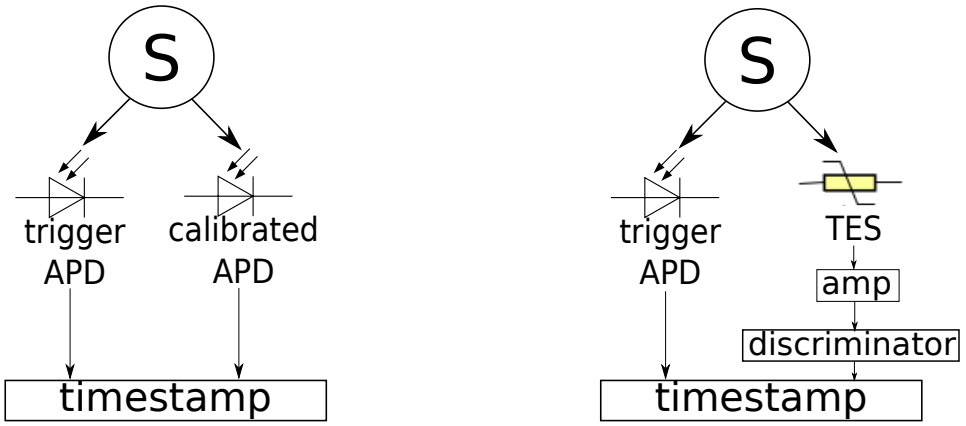


Figure 3.10: (a) Photon collection efficiency along the arm leading to a calibrated APD serves as a reference measurement for the TES detection efficiency measured in (b). S: time-correlated pair source of 810 nm photons.

Detector efficiency

Once the Schmitt trigger for each TES is set, we proceed to select two detectors with the best efficiencies. An efficiency measurement consists of comparing the TES with a calibrated Si-APD using time-correlated photon pairs produced by SPDC (Fig. 3.10). The comparison allows the detection efficiency of the TES to be estimated independently of the transmission efficiencies of the rest of the system (e.g. arising from imperfect optical coupling in the source). Although comparing the ratio of the detected photon flux from a calibrated photon source is a straightforward alternative to measuring detector efficiency, the method presented here is more robust to intensity fluctuations of the source [84].

Using a time-stamp unit, the time series collected by two APDs (Fig. 3.10a) is used to compute a cross-correlation function $g^{(2)}(\Delta t)$. Due to the tight time-correlation (about few hundred femtoseconds) of the photon pairs generated by SPDC, $g^{(2)}(\Delta t)$ will show a coincidence signature with a FWHM corresponding to the combined time jitter of both detectors (about 1 ns). From this coincidence signature, we can calculate the observed pair rate p. The background coincidences (acc) are due to accidental coincidences of the singles detected.

Consider the scenario where a detector with efficiency $\eta^{(a)}$ ($\eta^{(b)}$) and dark count rate $d^{(a)}$ ($d^{(b)}$) resides with Alice (Bob). Due to imperfect optical mode-matching and imperfect transmission of the optical elements used in the source, the pair collection efficiency (η_{source}) is already less than unity without taking into account the finite detection efficiency of each detector. Suppose that each detector reports a singles rate of $s^{(a)}$ ($s^{(b)}$) consisting of dark counts

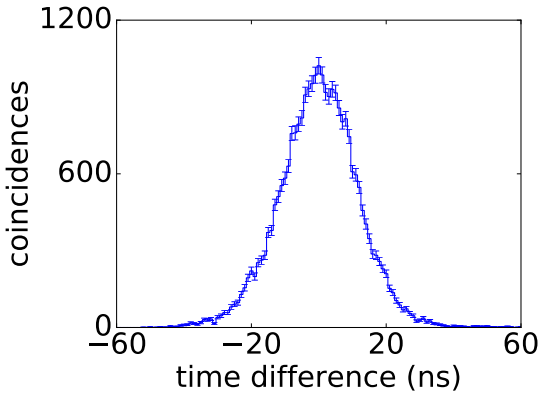


Figure 3.11: Cross correlation measurement of a time-correlated photon pair source measured with an APD and TES arranged according to Fig. 3.10b. The coincidence signature has a FWHM (26 ns) that is contributed mainly by the jitter of the TES.

and photon counts. The measured heralding efficiency

$$\eta = \frac{p - \text{acc}}{\sqrt{\left(s^{(a)} - d^{(a)}\right)\left(s^{(b)} - d^{(b)}\right)}} \tag{3.1}$$

can be expressed as

$$\eta_{\text{APD}} = \sqrt{\eta^{(a)}_{\text{trigger APD}}\,\eta^{(b)}_{\text{calibrated APD}}}\,\eta_{\text{source}} \quad \text{and} \quad \eta_{\text{TES}} = \sqrt{\eta^{(a)}_{\text{trigger APD}}\,\eta^{(b)}_{\text{TES}}}\,\eta_{\text{source}} \tag{3.2}$$

for the setup using a calibrated APD (Fig. 3.10a) and the TES (Fig. 3.10b), respectively. Thus, the TES efficiency can be inferred from APD efficiency values $\eta^{(b)}_{\text{calibrated APD}}$ and the measured heralding efficiencies using

$$\eta^{(b)}_{\text{TES}} = \left(\frac{\eta_{\text{TES}}}{\eta_{\text{APD}}}\right)^2 \times \eta^{(b)}_{\text{calibrated APD}}. \tag{3.3}$$

With this method, we characterize five TES samples and selected detectors with the highest detection efficiencies ($\approx 89.4\%, 87.3\%$).

Detector jitter

To characterize the timing jitter of each TES, we detect time-correlated photon pairs using the setup shown in Fig. 3.10b and measure the FWHM of the resultant coincidence signature (Fig. 3.11). In view of closing the locality loophole (Section 2.2.2) in future experiments, we explored techniques to reduce detector jitter in order to reduce the space-like separation between parties performing the Bell test.

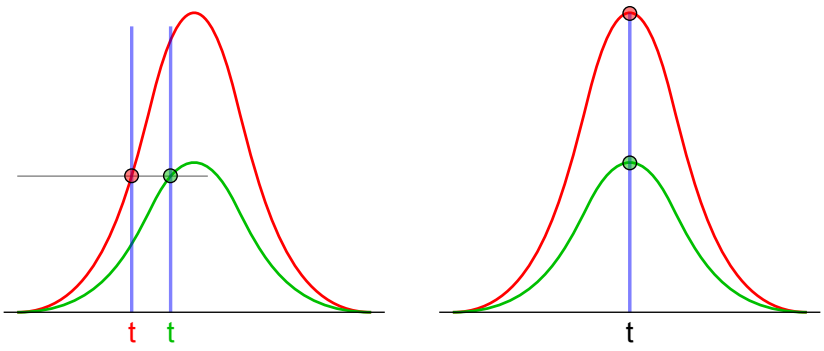


Figure 3.12: Comparison of threshold triggering characteristic of a Schmitt trigger (left) with peak triggering used by a constant-fraction-discriminator (CFD) (right). Peak triggering allows voltage pulses (red and green) of varying heights to be triggered without imposing a height-dependent delay. Image credit: Ref. [4].

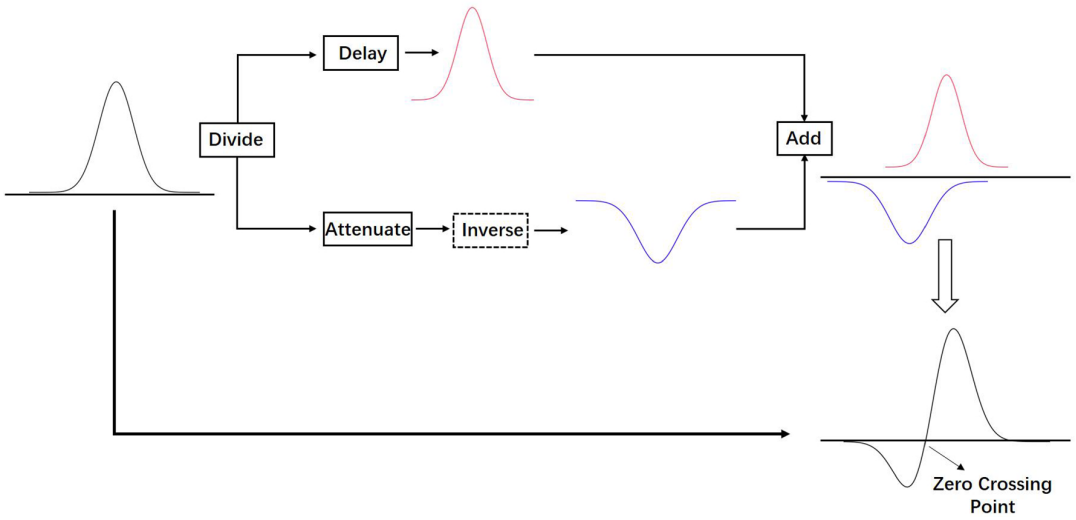


Figure 3.13: Principle of the constant-fraction-discriminator (CFD). The CFD is designed to trigger at the peak of a signal by emulating its time-differential and identifying its zero-crossing. The incoming signal is split into two components: one component is delayed, while the second component is attenuated and inverted. When both components have equal magnitude and are added together, they produce an output with a zero-crossing point that corresponds to the peak of the signal. For signals with the same pulse shape, the zero-crossing point is independent of amplitude. The amount of attenuation sets the triggering point to be on the leading or trailing edge of the signal. Image credit: Ref. [5].

First, we improved our signal discrimination method. Beforehand, we used a constant-fraction-discriminator (CFD) for pulse discrimination instead of a threshold trigger, such as the Schmitt trigger in Section 3.1.3 [1]. The CFD is designed to mimic triggering at the peak of the pulse (Fig. 3.13), and was thought to be more suitable for a photon-number-resolving detector such as the TES, compared to a threshold trigger that imposes a height-dependent triggering time (Fig. 3.12). However, the rate-of-change of the signal at its peak vanishes, resulting in an increased timing jitter when peak triggering is used to register photodetection times (Fig. 3.14). A similar observation was made by Lamas-Linares *et al.*, who reported that a threshold trigger provides a smaller jitter time when the threshold is set as low as possible, where the rate-of-change of the signal is maximum [79]. A second improvement was made

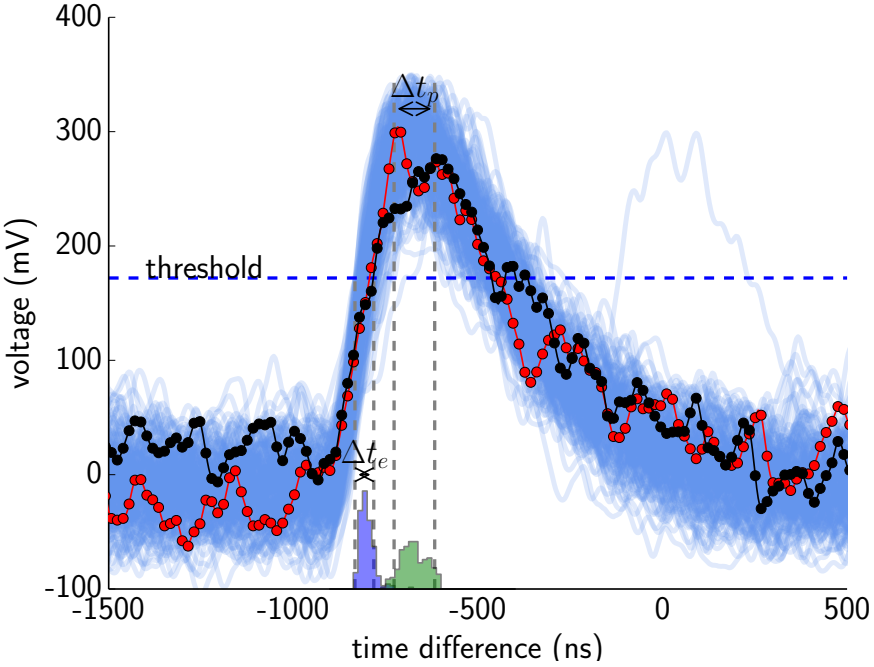


Figure 3.14: Comparison of two discrimination methods. (Sky Blue) Persistence plot of multiple TES pulses. (Red and Black) Individual TES pulses showing different peak positions. (Blue and Green) Histograms of threshold crossing times and peak times respectively. Threshold discrimination at the leading-edge of TES pulses yielded smaller jitter times (Δt_e) compared to peak discrimination (Δt_p). Fast leading-edge provides the best noise-rejection for triggering, compared to the slower varying peak.

through the use of Magnicon SQUIDs (6 MHz in FLL mode) with a higher bandwidth than the SQUIDs initially provided by NIST (2 MHz bandwidth). The lowest recorded jitter after upgrading our system was about 26 ns. Unfortunately, an increased SQUID bandwidth also admitted more noise, reducing the photon-number distinguishably observed in our pulse-height

distributions. For just closing the detection loophole, we chose to filter the signal from the new SQUIDs to about 2 MHz, measuring a final dark-count rate of about 20 Hz and a jitter of about 120 ns for each TES.

3.2 High-efficiency source of entangled photons

The source was the main focus of my colleague Shen Lijiong. This section describes the source in sufficient detail for completeness – further details of its characterization can be found in his thesis [3].

3.2.1 Source implementation

A sketch of the experimental setup is shown in Fig. 3.15. The source generates polarization-entangled photon pairs by coherently combining two collinear, type-II spontaneous parametric down conversion (SPDC) processes [85], and has proven suitable for high heralding efficiencies [19]. An Ondax 405 nm grating-stabilized laser diode (bandwidth = 160 MHz) continuously pumps a periodically poled potassium titanyl phosphate (ppKTP, $1 \times 2 \times 10$ mm) crystal, located within a Sagnac interferometer, from two opposite directions. A polarization-maintaining (PM) fiber filters the spatial mode and stabilizes the polarization. A telescope (Thorlabs BE052-A) adjusts the waist of the pump and focuses it at the centre of the crystal located 1.2 m away from it. A half-wave plate (HWP) rotates the pump polarization, while a polarizing beam splitter PBS_{405} splits the pump beam with a splitting ratio set by the orientation of the pump polarization. The two outputs of PBS_{405} are independently aligned so that a single pump photon is in a superposition of two spatial modes that counter-propagate through the crystal at the base of the interferometer. Both pump beams have the same Gaussian waists of $\approx 350\,\mu$m located at the centre of the crystal.

At the crystal, pump photons are down-converted with a small probability into pairs of degenerate, orthogonally polarized 810 nm photons. Each photon pair traverses the interferometer in the direction set by one of the two pump modes. Photon pairs traversing the interferometer in the clockwise (CW) direction reach the polarizing beam-splitter (PBS_{810}) at input port 1 and produce the bi-photon state $|\psi_{AB}\rangle = |HV\rangle$ at the output ports 3 and 4. Photon pairs traversing in the anticlockwise (ACW) direction arrive at input port 2 and produce instead $|\psi_{AB}\rangle = |VH\rangle$. A coherent combination of these outputs at PBS_{810} produces the polarization-entangled state

$$|\psi_{AB}(\theta,\phi)\rangle = \cos\theta|HV\rangle - e^{i\phi}\sin\theta|VH\rangle\,, \tag{3.4}$$

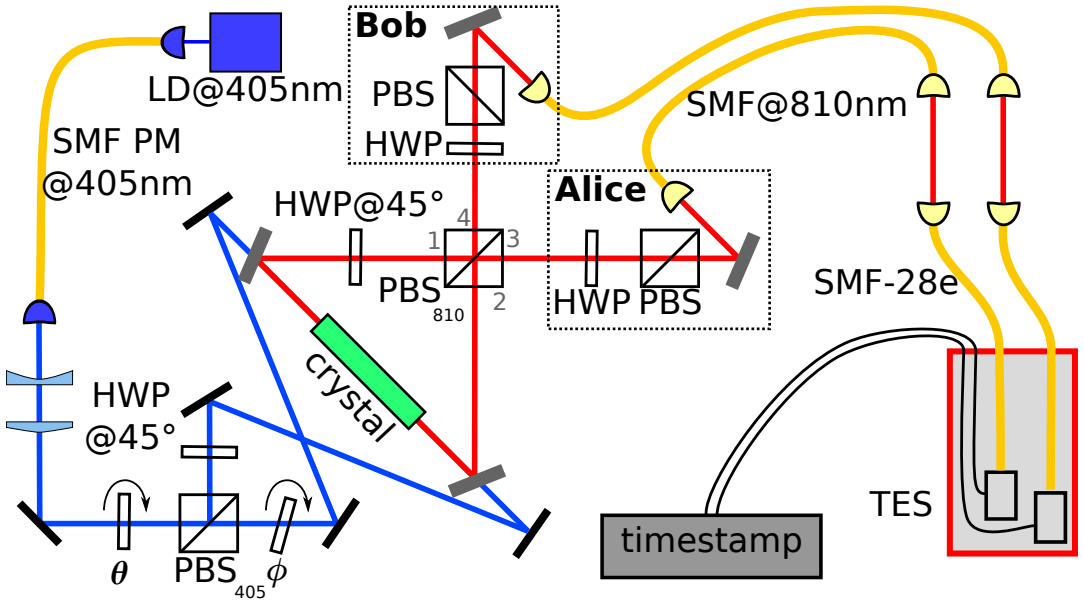


Figure 3.15: Schematic of the experimental setup, including the source of the non-maximally entangled photon pairs. A PPKTP crystal, cut and poled for type II spontaneous parametric down conversion from 405 nm to 810 nm, is placed at the waist of a Sagnac-style interferometer and pumped from both sides. Light at 810 nm from the two SPDC process is overlapped in a polarizing beam splitter (PBS_{810}), generating the non-maximally entangled state described by Eq. (3.4) when considering a single photon pair. A laser diode (LD) provides the continuous wave UV pump light. The combination of a half wave plate and polarization beam splitter (PBS_{405}) sets θ by controlling the relative intensity of the two pump beams, while a thin glass plate controls their relative phase ϕ. The pump beams enter the interferometer through dichroic mirrors. At each output of PBS_{810}, the combination of a HWP and PBS projects the mode polarization before coupling into a fiber single mode for light at 810 nm (SMF@810). A free space link is used to transfer light from SMF@810 to single mode fibers designed for 1550 nm (SMF-28e). Eventually the light is detected with high efficiency superconducting Transition Edge Sensors (TES), and timestamped with a resolution of 2 ns.

where θ and ϕ are determined by the relative intensity and phase of the two pump beams, set by rotating a half-wave plate (HWP) before the PBS_{405}, and the tilt of a glass plate in one of the pump beams.

The visibility of the interferometer relies on a high degree of overlap between the spatial modes of H and V-polarized photons. To achieve this, we considered the wedge error between the two prisms used to construct PBS_{810}. A wedge error slightly refracts H-polarized photons from their intended path, while producing a much larger beam deviation on reflected V-polarized photons. To ensure spatial mode symmetry between the two polarization modes, we used a PBS_{810} with very wedge small error (< 30”).

The collection mode for the down-converted light was defined by the single mode optical fibers (SMF@810 nm) and incoupling optics (Thorlabs C220, $f = 11$ mm). To maximize collection efficiency, the mode was chosen to have a Gaussian beam waist of ≈ 130 μm centered in the crystal located 65 cm away from the incoupling optics [86, 87].

Interference bandpass filters (transmission wavelength 810 ± 10 nm) and SMF@810 nm filter wide-band fluorescence generated by the interaction between the pump and crystal defects [88]. The unpolarized fluorescence photons contribute to uncorrelated detection events, raising the efficiency requirements for a Bell violation. To further suppress detected fluorescence, we operate the crystal at a higher temperature, which shifts the florescence spectrum away from the transmission wavelength of our bandpass filters [20, 89]. We used ppKTP with a poling period (9.55 μm) by Raicol designed for degenerate, collinear SPDC at 165 °C.

The combination of a zero-order half-wave plate (HWP) and another PBS (extinction rate 1:1000 in transmission) sets the measurement bases for light entering the single mode fibers. All optical elements are anti-reflection coated for 810 nm.

3.2.2 Source characterization

Pair collection efficiency was first characterized with calibrated Si-APDs using the setup shown in Fig. 3.10a. Setting the measurement bases to measure HV and VH, we estimate heralding efficiencies of $\approx 94.07\,\%$ and $\approx 93.56\,\%$, respectively; these values have been corrected for the APD detection efficiencies and dark counts (Eq. 3.1).

After pre-selecting two TES with the highest efficiencies, we deliver photons collected by the SMF@810 nm fibers from the pair source to the SMF-28e fibers of the TES by matching their optical modes efficiently ($\approx 95\%$) in free-space[3].

The TES output signal is amplified (pulse height $\approx$150 mV) using the techniques described in Section. 3.1.2, translated into photodetection event arrival times using our Schmitt trigger with an overall timing jitter ≈ 170 ns, and recorded with a timestamp unit with a resolution of 2 ns.

Using cross-correlation measurements to identify and count photon pairs (Section. 3.1.3), we estimate the overall heralding efficiency of the source together with the TES to be 82.42 ± 0.31 % (HV) and 82.24 ± 0.30 % (VH). With the source turned off, we measured intrinsic detector and background events of $6.7 \pm 0.58\,\mathrm{s}^{-1}$ for Alice and $11.9 \pm 0.77\,\mathrm{s}^{-1}$ for Bob, respectively.

[3] As our TES show the highest efficiency with SMF-28e fibers (Section. 3.1), the light collected in to single mode fibers from the parametric conversion source is transferred to these fibers via a free-space link

To estimate the fluorescence level, we measure the amount of unpolarized photons back-scattered from the crystal as it is being pumped. This is performed by setting the measurement basis to measure VH while generating the state $|HV\rangle$, and measuring the detection rate $F_{A,B}$ at Alice's (A) and Bob's (B) detectors. We then set the measurement basis to HV to measure the detection rate $S_{A,B}$ at each detector due to down-converted photons and forward-scattered fluorescence. Assuming that the fluorescence in both the forward and backward directions are the same, we calculate F_A/S_A at Alice, obtaining a fluorescence-to-signal ratio of $0.135 \pm 0.08\%$. A similar ratio is observed for Bob. With a total pump power at the crystal of 5.8 mW we estimate a pair generation rate $\approx 2.4 \times 10^4\,\mathrm{s}^{-1}$ (detected $\approx 20 \times 10^3\,\mathrm{s}^{-1}$) and background rates[4] of $45.7\,\mathrm{s}^{-1}$ at Alice and $41.5\,\mathrm{s}^{-1}$ at Bob.

We verify the quality of the source by measuring a high visibility ($\approx 99.1\%$) in the $+45^\circ/-45^\circ$ basis when generating the singlet state

$$|\psi_{AB}^-\rangle = |\psi_{AB}(\theta = \pi/4, \phi = 0)\rangle = (|HV\rangle - |VH\rangle)/\sqrt{2}.$$

3.3 Experimental procedure

To achieve the highest Bell violation with the measured system efficiencies and background rates, a numerical optimization (Section 2.3) of the state and measurement parameters suggested: $\theta = 25.9^\circ$, $\phi = 0$, $\alpha_0 = -7.2^\circ$, $\alpha_1 = 28.7^\circ$, $\beta_0 = 82.7^\circ$, and $\beta_1 = -61.5^\circ$, corresponding to the state

$$|\psi_{AB}\rangle = 0.900|HV\rangle + 0.437|VH\rangle. \tag{3.5}$$

The required state corresponds to the ratio of $|HV\rangle$ to $|VH\rangle$ pairs to be equal to 4.246. We ensure this ratio by comparing the source pair rates at measurement settings HV and VH, and fine-tuning the pump power splitting ratio.

Thermal drift in the source affects the path-length between the two pump modes. We periodically (every 6 mins) lock the phase at $\phi \approx 0$ by generating the singlet state $|\psi_{AB}^-\rangle$ and rotating the phase plate until the visibility in the $+45^\circ/-45^\circ$ basis is larger than 0.985.

To ensure that the source generates the prerequisite state, we perform a state-tomography by measuring photon pairs cycling through basis measurements (H,V,D,A) at Alice and Bob [90]. We do not consider elliptical states in this measurement as space constraints in the source prevents us from inserting an additional quarter-wave plate. Comparing the generated state to the required state, we obtain a fidelity of $99.15 \pm 0.18\%$.

[4] Comprising of intrinsic detector, background, and fluorescence events.

To perform the Bell measurement, we change the measurement basis every 2 minutes, cycling through the four possible basis combinations and recorded detection events for approximately 42.8 minutes, The sequence of the four settings is determined for every cycle using a pseudo-random number generator. Excluding the time taken to implement the phase lock and the measurement settings, the effective data acquisition time is approximately 34 minutes.

3.4 Results

3.4.1 Bell violation

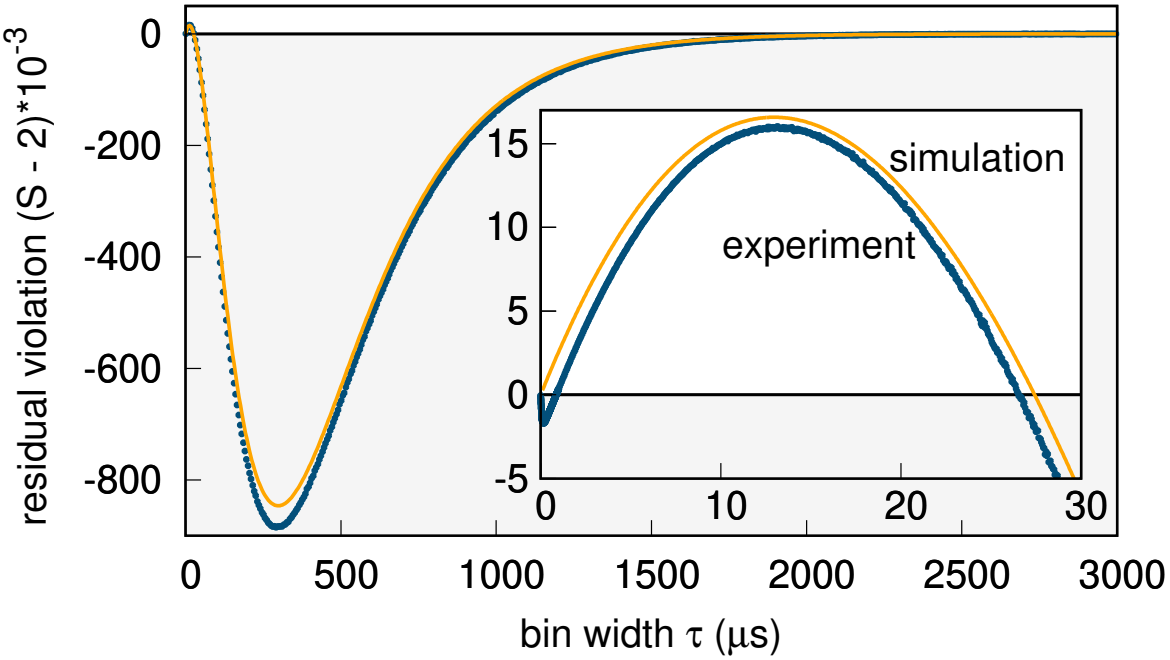


Figure 3.16: Measured CHSH violation as function of bin width τ (blue circles). Orange continuous line: numerical simulation (Chapter 2). Both the simulation and the experimental data show a violation for short τ (zoom in inset). The uncertainty on the measured value, calculated assuming i.i.d., corresponding to one standard deviation due to a Poissonian distribution of the events, is smaller than the symbols. For $\tau \lesssim 1$ μs the detection jitter ($\approx$ 170 ns) is comparable with the time bin, resulting in a loss of observable correlation and a fast drop of the value of S.

Fig. 3.16 shows the result of processing the timestamped events for different bin widths τ. The largest violation $S = 2.01602(32)$ is observed for $\tau = 13.150$ μs, which, with the cited pair generation rate of $24 \times 10^3\,\mathrm{s}^{-1}$, corresponds to a mean photon number per bin $\mu \approx 0.32$. This number is very close to the value $\mu \approx 0.322$ predicted from our model (Section 2.3). The

uncertainty is calculated assuming that measurement results are independent and identically distributed (i.i.d.).

The slight discrepancy between the experimental violation and the simulation is attributed to the non-ideal visibility of the state generated by the photon pair source. When τ is comparable to the detection jitter, detection events due to a single pair may be assigned to different rounds, decreasing correlation. This explains the drop of S below 2 (which our simulation does not capture because we have not included the jitter as a parameter).

3.4.2 Extractable randomness from observed violation

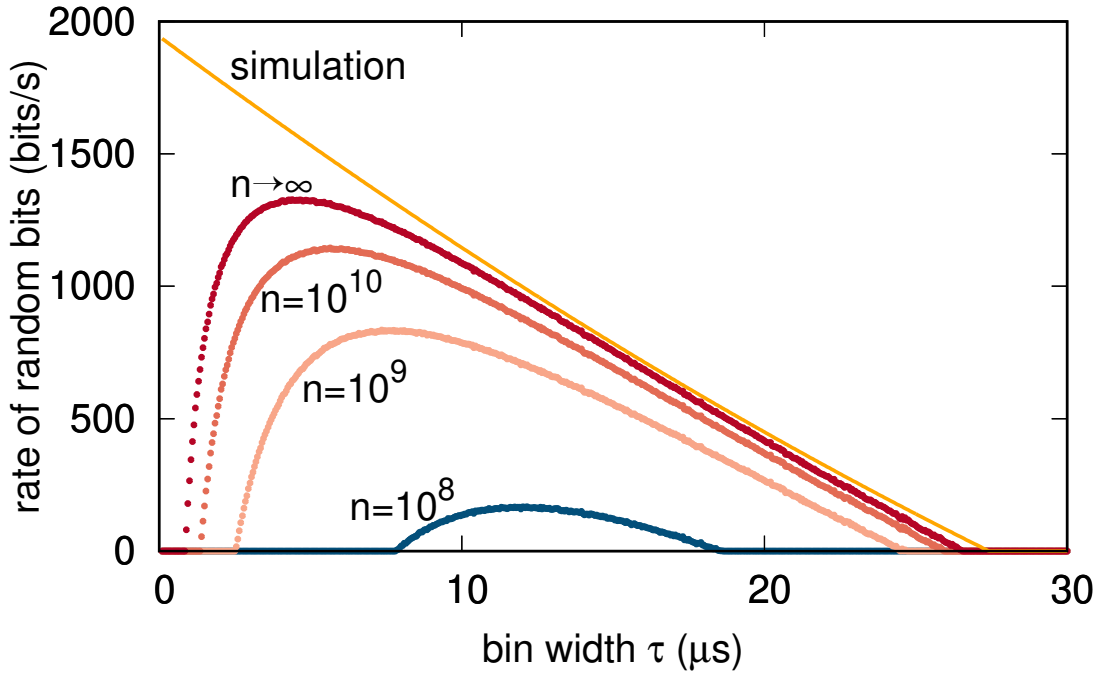


Figure 3.17: Randomness generation rate r_n/τ as a function of τ for different block sizes n. The points are calculated via Eq. 2.34 for finite n (Eq. 2.35 for $n \to \infty$) and the violation measured in the experiment, assuming $\gamma = 0$ (no testing rounds) and $\varepsilon_c = \varepsilon_s = 10^{-10}$. The continuous line is the asymptotic rate Eq. 2.35 evaluated on the values of S of the simulation shown in Fig. 3.16, for the same security assumptions.

Fig. 3.17 shows the randomness extraction rate r_n/τ for various block sizes n for the observed S values shown in Fig. 3.16. For comparison, we include the asymptotic rate r_∞/τ, computed with S values given by a simulation that takes the source efficiency and dark-counts as inputs.

The most obvious feature is that the highest randomness rate does not occur at the maximum S value, where the highest randomness per round occurs. Rather, it is more advantageous to sacrifice the randomness per round for more rounds per unit time. This optimization will be required for calibrating a random number generator with an active switching of the measurement bases.

Similar to the S value, the randomness extraction rate falls when the bin width τ is comparable to the detector jitter. For fixed detector efficiencies, we expect that the randomness rates to increase with higher photon pair generation rates [3]. This could be implemented with higher pump powers and will be ultimately limited by the detector jitter. Here, the use of superconducting nanowire detectors, with jitter times at tens of picoseconds, will be a significant advantage.

3.4.3 Randomness Extraction

To determine the number of certified random bits that can be generated by applying a Trevisan extractor to our experimental data (Eq. 2.33), we apply the randomness extraction protocol described in Section 2.4, which requires the expected winning probability of the nonlocal game, ω_{exp}, as an input parameter.

To estimate ω_{exp} directly from our data, we first dedicate a "calibration fraction" γ_{calib} of the data to determine a reference winning probability ω_{calib}. From this value, we define an honest implementation of the protocol as an implementation which reproduces the CHSH violation during the calibration stage with probability

$$P(\omega_{\text{exp}} \geq \omega_{\text{calib}}) \leq \varepsilon_{\text{calib}},$$

where $\varepsilon_{\text{calib}} = 10^{-10}$ guarantees that the Bell violation will not be overestimated.

This definition allows us obtain

$$\omega_{\text{exp}} = \omega_{\text{calib}} - \delta_{\text{calib}}, \tag{3.6}$$

where an upper bound

$$\delta_{\text{calib}} \leq \sqrt{\frac{\log(1/\varepsilon_{\text{calib}})}{2n}} \tag{3.7}$$

leads to a conservative estimate [30]. We then optimize the calibration fraction γ_{calib} and bin width τ to maximize the extractable randomness, obtaining $\gamma_{\text{calib}} = 22\,\%$ and $\tau = 8.9\,\mu$s. The corresponding value of ω_{exp}, and security parameters ($\varepsilon_{\text{s}}, \varepsilon_{\text{c}}$ set *a priori* to 10^{-10}), are then

used to define the number of certified bits that the Trevisan extractor should extract from the remaining $(1-\gamma_{\text{calib}})$ fraction of the data (Eq. 2.33). We confirm an honest implementation by verifying that the data used to extract random bits also exceeds the threshold Bell violation set by $\omega_{\text{exp}} - \delta_{\text{est}}$ (Eqs. 2.31, 2.32). The extractor also requires an initial random seed which we generate from Ref. [91]. From the remaining 175288156 measurement rounds, the extractor generated 617920 random bits. The rate of extracted random bits is ≈ 240 bits/s over a total measurement time (≈ 42.8 mins), which includes the time for acquiring the calibration data, optimizing the phase of the source, and implementing the measurement settings with the motorized waveplates. Further details on the extraction procedure can be found in Ref. [30].

We used the NIST Statistical Test Suite to check that the uniformity of the generated strings is at least on par with acceptable pseudo-randomness. The result of the individual tests are summarized in Table 3.1.

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 3.1: Result of the NIST Statistical Test Suite for the extracted bits. We split the random bits into 97 sequences of 6300 bits each.

3.5 Conclusion

We experimentally observed a detection loophole-free Bell violation with a continuous wave photon entangled pair source. A high collection efficiency source and high detection efficiency superconducting detectors resulted in an overall detection efficiency of $> 82\,\%$, and a low background count rate ($< 0.2\,\%$).

The photon pair source and measurement bases were optimized for the highest Bell violation, based on the overall efficiency and background counts [2]. Bell tests were carried out by measuring detection events at the optimal measurement settings. To define a measurement round, the continuous stream of detection events were organized into uniform time bins, each of width τ. We observe that for τ approaching the detector jitter (≈ 170 ns), the violation drops dramatically as photon pairs that should be detected within the same time bin are

detected in other bins. At the optimal bin width, we recorded the largest detected violation of $S = 2.01602(32)$ with an average number of photon pairs per round ≈ 0.32.

The flexible definition of an experimental round permitted by the CW nature of our setup allowed us to study the dependence of the observable violation as 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 this kind of experiments: an increase in the pair generation rate is accompanied by a reduction of the round duration τ. This approach shifts the experimental repetition rate limitation from the photon statistics to the other elements of the setup, e.g. detectors time response or active polarization basis switching speed.

The observation of a Bell violation certifies the generation of private randomness. When considering the largest attainable rate of random bit generation, the optimal round duration is the result of the trade-off between observed violation $S(\tau)$ and number of rounds per unit time $(1/\tau)$. While for an ideal realization the optimal round duration would be infinitesimally short, it is limited in our system by the detection time jitter.

To extract uniformly random bits from the Bell experiment, we apply a randomness expansion protocol [92]. We first reserve a fraction ($\approx 22\,\%$) of the data to determine the optimal bin width ($\tau = 8.9\,\mu$s) that maximizes the randomness rate and its corresponding Bell violation. The remaining data is then binned accordingly and verified to see if they possess a Bell violation consistent with the calibration data. Subsequently, a Trevisan extractor is applied to extract random bits [57].

From the total measurement time of 42.8 min, we calculate a rate of ≈ 240 random bit/s. Due to a lack of an intrinsic dead time of our CW source, the randomness rate is competitive with experiments using pulsed sources that required acquisition times in the order of tens of hours [93, 94]. The acquisition time reduction represents a significant advancement towards a practical source of certified randomness. This work was published in Ref. [30].

Our proof of principle demonstration can be extended into a complete, loophole-free random number source. This requires closing the locality and freedom-of-choice loopholes, with techniques not different from pulsed photonic-sources, with the only addition of a periodic calibration necessary for determining the optimal time-bin.

Chapter 4

Multi-pulse Fitting of Transition-Edge Sensor Signals from a near-infrared continuous-wave source

In the previous chapter, we demonstrated a time binning method that allows the time duration of each Bell measurement round to be flexibly defined. The duration can be optimized to obtain a maximal random bit generation rate (Fig. 3.17). As the number of measurement rounds containing entangled photon pairs increases per unit time with higher photon flux rates, the associated randomness generation rate tends to increase accordingly [91]. However, the maximum photon flux rate that can be detected with our transition-edge sensors (TESs) is limited by the duration of each pulse; photodetection events with time separation shorter than the pulse duration overlap and cannot be reliably identified by our discriminator since it registers only the leading event (Fig. 4.1). Consequently, this limits the randomness generation rate with TESs[1]. This problem is not confined only to our Bell experiment: TESs are often used with pulsed light sources with a repetition rate lower than few tens of kHz in order to avoid overlapping signal pulses [95], excluding the use of TESs with otherwise superb detection efficiencies from some applications. Therefore, we investigate the time discrimination for overlapping TES pulses using a continuous-wave (CW) light source.

Techniques to extract timing information from overlapping signals have been explored for high-energy physics experiments [96–100]. Fowler *et al.* [100] improved time discrimination by considering the time derivative of the signal to locate the steep rising edge of individual

[1]The maximum detectable photon flux rate is not the only factor limiting the randomness generation rate; the TES jitter contributes as well since it results in the wrong assignment of photodetection events to time bins with duration of a similar time scale.

photodetection events. In cases with high signal-to-noise ratio, such as in the detection of high-energy photons γ and X-rays (SNR ≈260, estimated from Ref. 100), this approach is effective also when signals overlap. However, for near-infrared (NIR) photodetection with a TES, it is necessary to filter high frequency noise components to improve the signal-to-noise ratio (SNR ≈2.4, estimated from Ref. 101) at the expense of a reduced timing accuracy.

We approach the problem by separating it into two distinct phases: an initial event identification, followed by a more accurate timing discrimination. We identify photodetection events using a two-level discriminator [2]. Its resilience to noise allows us to coarsely locate both isolated and overlapping pulses with a moderate use of filtering, thus retaining some of the high frequency components of the signal, useful to improve the time accuracy of subsequent operations. For monochromatic sources, every detection event has the same energy. We can then estimate the number of photons for every detection region from the total pulse area, identifying the cases of overlapping events. From the number of photons, we calculate a heuristic model function and fit it to the signal to recover the detection-times.

4.1 Electronics and photon detection pulse

The TES is biased and readout according to the description in Section. 3.1.2. To characterize the TES response, we use a laser diode centered at 810 nm as a light source, operated in CW mode. We control the average photon flux with a variable attenuator, then launch the light into a fiber (type SMF28e) that directs it to the sensitive surface of the TES.

We record 10 μs long traces with a sampling rate of 5×10^8 s^{-1} and a 12 bit voltage resolution. For light at 810 nm, the signal generated by discrete absorption processes for each photon after the amplifier chain exhibits a rise time for a single photon pulse of about 100 ns, and an overall pulse duration of about 2 μs.

We collected a total of 4×10^5 traces with the TES continuously illuminated by an attenuated laser diode. Despite the flux-locked loop, we observe a residual voltage offset variation from trace to trace. Therefore, for every recorded pulse trace $v_{\mathrm{rec}}(t)$, we remove the residual baseline,

$$v(t) = v_{\mathrm{rec}}(t) - V_M\,, \tag{4.1}$$

where V_M is the most frequently occurring value of the discretized signal $v_{\mathrm{rec}}(t)$ over the sampling interval.

[2] The discriminator used in this chapter is based on the Schmitt trigger mechanism introduced in Section, but has additional features which will be elaborated further in Section 4.2.

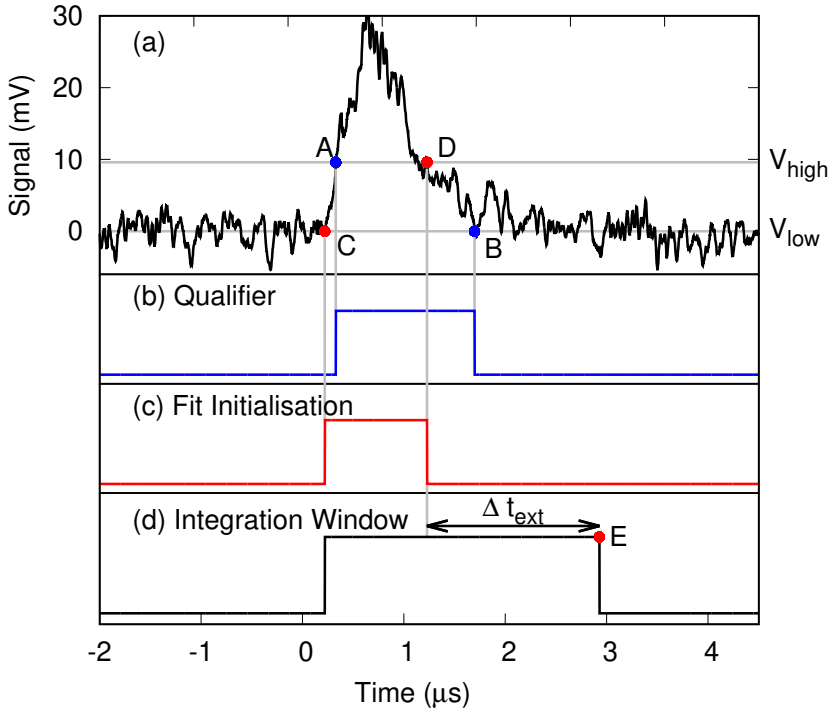


Figure 4.1: (a) Typical TES response with overlapping pulses. The horizontal lines show the high and low threshold settings of the Schmitt trigger mechanism. (b) Qualifying interval AB identified by the Schmitt trigger. (c) The interval CD includes the rising edges of the overlapping pulses, and is used to initialize a least-square fit. (d) The wider interval CE that includes the rising edge and decaying tail is used to estimate the number of photons associated with the event. We empirically found a reasonable energy resolution with Point E obtained by extending interval CD by $\Delta t_{ext} = 1700\,\text{ns}$.

4.2 Pulse Identification

In a first step, we identify the presence of an absorption process from one or more photons in a trace, and distinguish it from background noise. This is done by a traditional Schmitt trigger mechanism [102], implemented via discriminators at two levels: a qualifier flag is raised when the signal passes threshold V_{high} (Fig. 4.1(a), point A) and lowered by the first subsequent crossing of threshold V_{low} (point B).

In order to minimize the number of false events, we estimate V_{high} using a histogram of maximum pulse heights for 4×10^4 traces, shown in Fig. 4.2. The distribution has two distinct peaks, with one around 5 mV corresponding to traces without any detection event ($n = 0$), and another one starting from 9.5 mV onwards corresponding to traces with at least one detection event ($n > 0$). We choose V_{high} to the minimum between the two peaks (9.5 mV), and V_{low} to 0 mV.

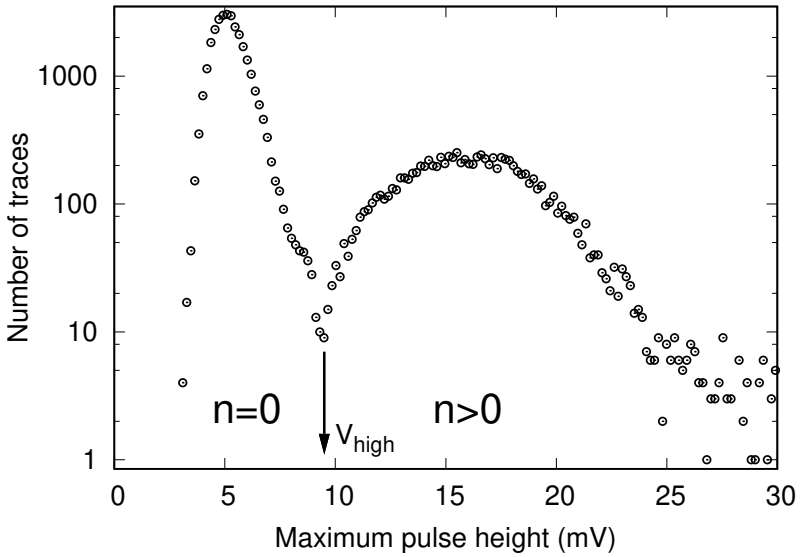


Figure 4.2: Histogram of maximum pulse heights for 4×10^5 traces. The two distributions correspond to traces with ($n > 0$) and without ($n = 0$) photodetection events. We use the minimum between the two distributions to set the threshold V_{high} of the discriminator.

We estimate a timing accuracy for single photon events [101] of $\sigma/(dv/dt) \approx 16\,\text{ns}$, from the RMS noise $\sigma = 1.75\,\text{mV}$, and the steepest slope of the response $dv/dt = 0.11(9)\,\text{mV/ns}$ (from the average of the 10%-90% transitions of an ensemble of pulses). However, a simple threshold detection of the leading edge does not work if pulses start to overlap.

More precise timing information of a photodetection event is obtained from a least square fit to the signal using a displaced standard pulse. To efficiently initialize this fit, we do not directly use the qualifier window AB for two reasons: first, it contains only a fraction of the leading edge belonging to the earlier pulse that contains most of the timing information, and second, it includes a large portion of the decaying tail unassociated with the onset of photodetection. The time window CD derived from the same discriminator levels ensures the inclusion of the first leading edge, and is also shorter.

Similarly, we derive an integration time window from the qualifier window to determine the pulse integral, from which we extract the photon number of a quasi-monochromatic light source. As a starting point, we choose point C for the integration to capture the rising slope of a pulse, and extend the time D by a fixed amount Δt_{ext} to point E to capture the tail of the response signal (Fig. 4.1(d)). We found that it is more reliable to extend point D by a fixed time to capture the tail of the signal rather than to reference the end of the integration window to point B. This is because the signal-to-noise ratio around B is low, leading to a large variation of integration times. We empirically find that $\Delta t_{ext} = 1700\,\text{ns}$ gives a good signal-to-noise ratio of the pulse integral.

4.3 Photon Number Discrimination

To determine the number of photons in each trace, we assume that the detection and subsequent amplification have a linear response, so that the integral of each signal is proportional to the absorbed energy [103], resulting in a discrete distribution of the areas of the signals. This distribution is spread out by noise, and we have to use an algorithm to extract the photon number in presence of this noise.

For this, we first compute the pulse area $a = \int_{t_C}^{t_E} |v(t)|$ for every qualified trace within region CE. Fig. 4.3 shows a histogram of pulse areas from the qualified traces out of all the 4×10^5 acquired. The distribution shows three resolved peaks that suggest having been caused by $n = 1, 2, 3$ photons being absorbed by the TES.

One can fit the histogram in Fig. 4.3 to a sum of three normalized Gaussian peaks $g_n(a; a_n, \sigma_n)$,

$$H(a) = \sum_{n=1}^{3} h_n \, g_n(a|a_n, \sigma_n) \,, \tag{4.2}$$

where each Gaussian peak is characterized by an average area a_n and width σ_n. The ratio $a_2/a_1 = 1.95$ indicates that the TES response to photon energies of 1 and 2 photons is approximately linear.

We identify thresholds $a_{n-1,n}$ as the values that minimize the overlap between distributions $g_{n-1}(a|a_{n-1}, \sigma_{n-1})$ and $g_n(a|a_n, \sigma_n)$. With this, we assign a number of detected photons n by comparing the area of every trace to thresholds $a_{n-1,n}$ and $a_{n,n+1}$.

The continuous nature of the light source with a fixed power level makes it difficult to assign a number of photons per qualified signal, as the integration window varies from pulse to pulse, and detection events may occur at random times in the respective integration windows. Heuristically, however, one could even replace the individual event numbers h_n in Eq. 4.2 by a Poisson distribution,

$$h_n = N p(n|\bar{n}) \,, \tag{4.3}$$

where $\bar{n}$ is an average photon number, $p(n|\bar{n})$ the Poisson coefficient, and N is the total number of traces. For the data shown in Fig. 4.3, this would lead to an average photon number of $\bar{n} \approx 0.3$ per integration time interval.

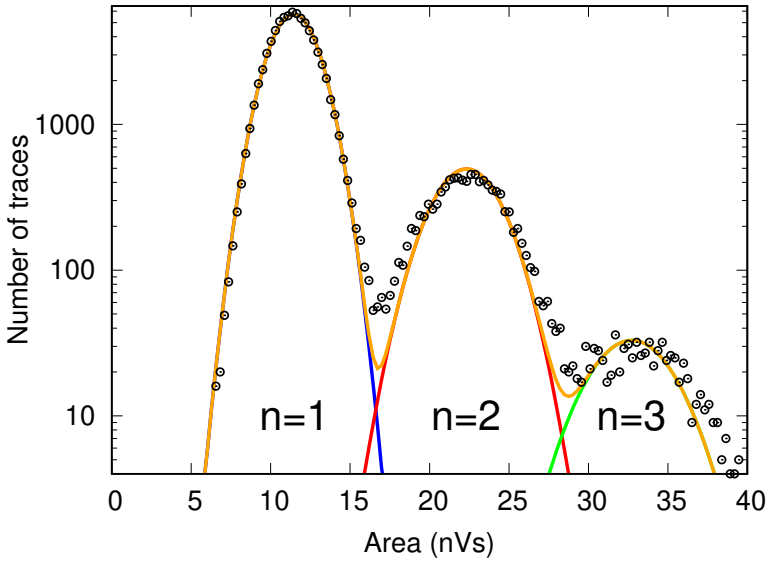


Figure 4.3: Distribution of pulse areas $H(a)$. For every trace that triggers the two-levels discriminator, the area is calculated within the region CE. The continuous lines are Gaussian fits for the $n = 1$ (blue), $n = 2$ (red), and $n = 3$ (green) area distributions, and their sum (orange).

4.4 Determining the detection-times of overlapping pulses

The difficulty of assigning a photon number to light detected from a CW source can be resolved if one treats the first detection process of light following the paradigm of wideband photodetectors in quantum optics [104]. As TES are sensitive over a relatively wide optical bandwidth, the corresponding time scale of the absorption process is much shorter than the few microseconds of the TES thermal recovery [105]. Then, the signal would correspond to a superposition of responses to individual absorption processes, which may happen at times closer than the characteristic pulse time.

To recover absorption times of individual absorption events in a trace of N overlapping pulses, where N is determined with the pulse area method outlined in the previous section, we fit the TES response signal $v(t)$ to a heuristic model $v_N(t)$ of a linear combination of single-photon responses $v_1(t)$,

$$v_N(t|\{t_i,A_i\}) = \sum_{i=1}^{N} A_i\, v_1(t-t_i)\,, \tag{4.4}$$

where A_i is the amplitude and t_i the detection time of the i-th pulse. While the TES response to multi-photon events is not strictly linear, this model will give a reasonably good estimation of the timing for single photon absorption events.

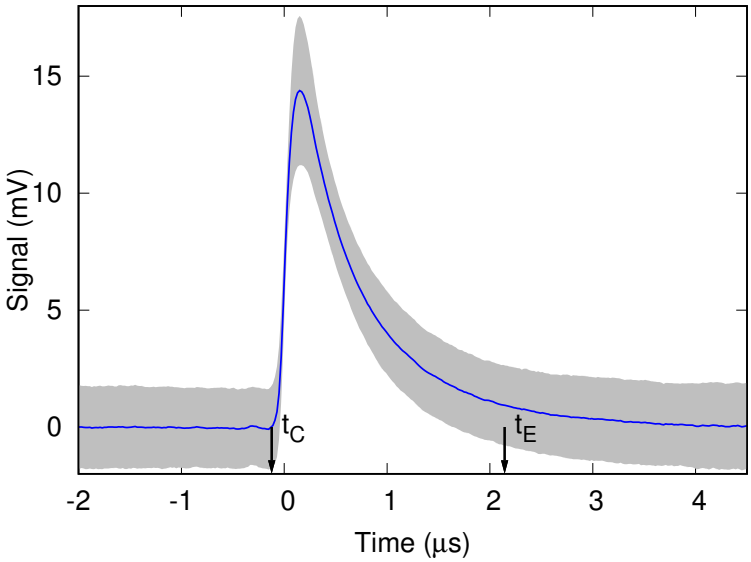


Figure 4.4: Solid line: average response of the TES and amplification to a single absorption. We use a Schmitt trigger to identify the region between t_C and t_E. Grey region: one standard deviation in the observed ensemble of $n = 1$ traces.

4.4.1 Single photon pulse model

We obtain a model for the single photon response $v_1(t)$ of the TES and its signal amplification chain for the fit in Eq. 4.4 by selecting $N_1 = 10^4$ single photon traces from the measurement shown in Fig. 4.3, and averaging over them. The averaging process eliminates the noise from individual traces, and retains the detector response.

Signal photon events can happen at any time within the sampling window. It is necessary to align these detection events to average the traces. We assign a detection time to the i-th trace $v_1^{(i)}(t)$ by recording the time t_i corresponding to the maximum of $dv_1^{(i)}(t)/dt$. We use a Savitzky-Golay filter (SGF) to reduce the high frequency components [106]; the SGF replaces every point with the result of a linear fit to the subset of adjacent 41 points.

We also reject clear outlier traces by limiting the search for t_i to the time interval CD. The remaining N_1 traces are then averaged by synchronizing them according to their respective t_i and to obtain the single-photon response $v_1(t)$,

$$v_1(t) = \frac{1}{N_1} \sum_{i=1}^{N_1} v_1^{(i)}(t + t_i)\,. \tag{4.5}$$

The result is shown in Fig. 4.4, together with a noise interval derived from the standard deviation of N_1 single photon traces. The model demonstrates an average rise time of 116 ns from 10% to 90% of its maximum height. The relaxation time ($1/e$) of 635 ns corresponds to detector thermalization [28].

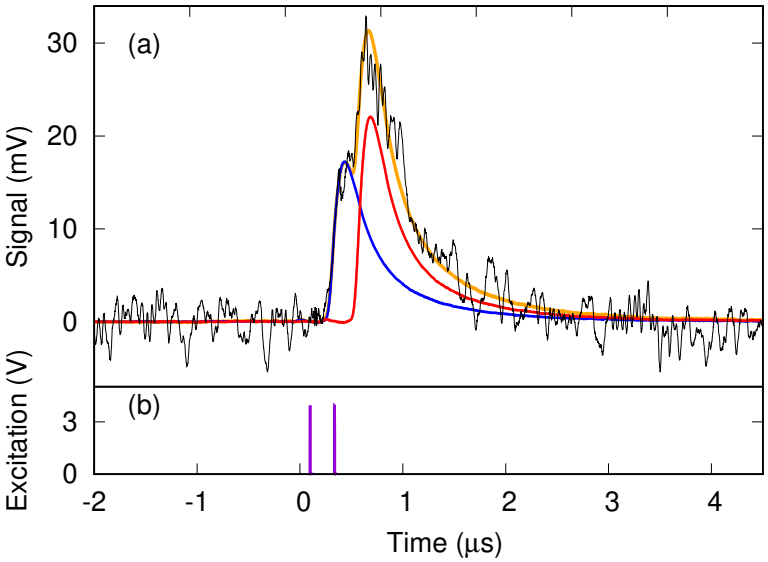


Figure 4.5: (a) Fit of a two-photon signal with the heuristic function described in the main text. Black line: measured TES response after removing the vertical offset. Orange line: fit to Eq. (4.4), with two single photon components separated in time (blue and red line). (b) Electrical pulse pair separated by 239 ns sent to the LD illuminating the TES.

4.4.2 Time-tagging via least-square fitting

For every qualified trace, we assign a number of photons N according to the calculated area, and fit it using Eq. (4.4). The fit has $2N$ free parameters: detection times t_i and amplitudes A_i, with $i = 1 \ldots N$. We bound t_i to the range CD (Fig. 4.1(c)), and restrict the sum of A_i to be consistent with the thresholds obtained from the area distribution

$$\frac{a_{N-1,N}}{\int_{t_C}^{t_E} |v_1(\tau)|\, d\tau} \leq \sum_{i=1}^{N} A_i \leq \frac{a_{N,N+1}}{\int_{t_C}^{t_E} |v_1(\tau)|\, d\tau}\,. \tag{4.6}$$

The accuracy of the fit depends on the choice of minimization algorithm. We used Powell's derivative-free method [107] because the presence of noise tends to corrupt gradient estimation [108].

To verify the accuracy of the fitting algorithm for $N = 2$, we expose the TES to pairs of short (4 ns) laser pulses with a controlled delay Δt_p. The 100 kHz repetition rate is low enough to isolate the TES response between consecutive laser pulse pairs. Selecting only the traces with two photons, we have two possible cases: (i) a two-photon event generated within one of the 4 ns pulses or (ii) one photon in each pulse. We compared the TES response for five different delays Δt_p: 92 ns, 170 ns, 239 ns, 493 ns, and 950 ns. Fig. 4.5 shows an example of a measured trace where the fitting algorithm was able to distinguish between separate photodetection events at $\Delta t_p = 239$ ns even though it appears to be a single event because of the detector noise. For each delay we collected $\approx 3.5 \times 10^5$ traces, and for each trace we estimate the

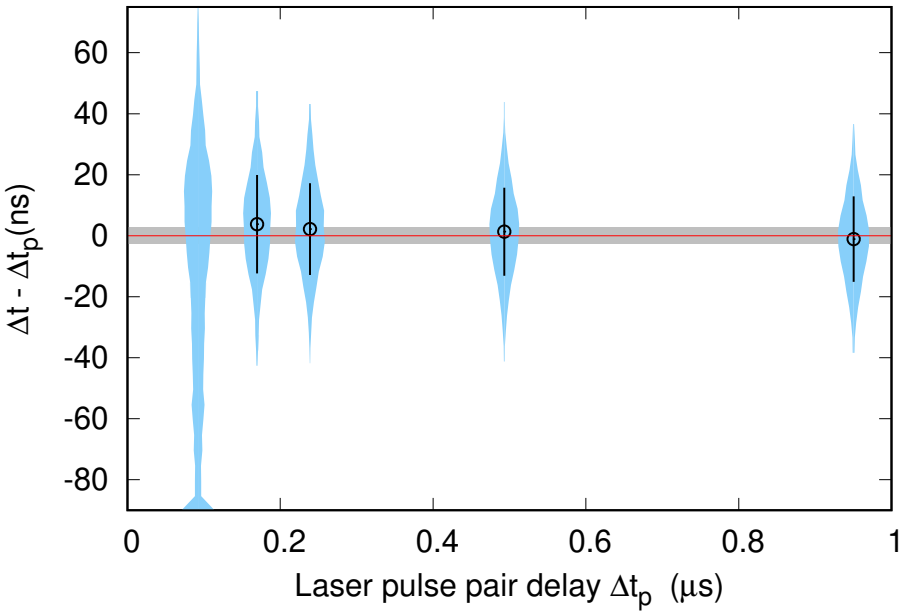


Figure 4.6: Difference between the detection-time separation estimated with the fitting technique (Δt) and the delay of laser pulse pairs (Δt_p) for five different delays: 92 ns, 170 ns, 239 ns, 493 ns, and 950 ns. Blue regions: distribution of $\Delta t - \Delta t_p$. Grey region: expected range of separation for 90% of single photon detections for 4 ns long laser pulse pairs. Black circles: mean of the distributions with error bars corresponding to one standard deviation.

photodetection times using the least-square method. In Fig. 4.6 we summarize the distribution of time differences $\Delta t = |t_2 - t_1|$ for each delay.

Except for the shortest pulse separation, the time differences have Gaussian distributions with standard deviations of about 16 ns. This matches the time accuracy expected from the simple noise/slope estimation for the leading edge of the single photon pulse (Section 4.2), despite the overlapping pulses. The average separation between the center of the distribution and the expected result, $\Delta t - \Delta t_p$, is 2(2) ns. For $\Delta t_p = 92$ ns, the distribution is clearly skewed toward 0 ns. This multi-modal distribution indicates that the fit procedure is unable to distinguish two single-photon events generated by the two separated diode pulses from two-photon events generated within the same diode pulse.

4.5 Detection-Time Separation from coherent source

To examine the accuracy of the fitting technique over a continuous range of time differences Δt, we extract the normalized second order correlation function $g^{(2)}(\Delta t)$ for detection events

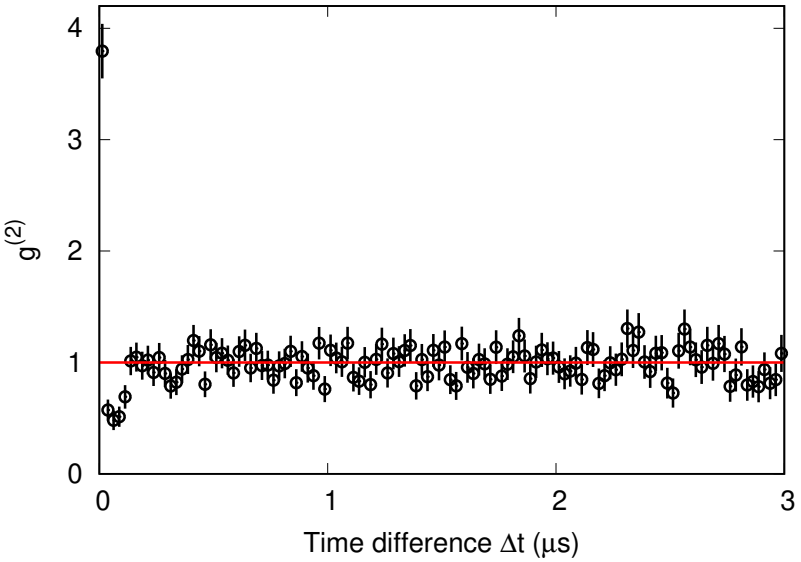


Figure 4.7: Normalized second order correlation function $g^{(2)}(\Delta t)$ for events recorded with a single TES from a coherent light field. Error bars indicate one standard deviation assuming Poissonian statistics, the bin size is 25 ns. Solid line: expected correlation for a coherent field.

recorded with a single TES from a coherent light field. This correlation function should be exactly 1 for all time differences Δt [104].

For this, the TES is exposed to light from a continuously running laser diode, with an average photon number of about 0.3 per integration interval of around 3 μs. Again, we select only two-photon traces using the methods described in Section 4.3, and fit the traces to the model described by Eq. 4.4 with $N = 2$.

Each fitted trace leads to two time values t_1 and t_2, which we sort into a frequency distribution $G^{(2)}(\Delta t)$ of time differences $\Delta t = t_2 - t_1$. We normalize this distribution with the distribution expected for a Poissonian source, taking into account the finite time of our acquisition windows. We remove single-photon traces mis-identified as two-photon traces by filtering out traces that have a minimum estimated amplitude smaller than one half of a single photon pulse.

The resulting normalized distribution $g^{(2)}(\Delta t)$ is shown in Fig. 4.7. For $\Delta t > 150$ ns, the correlation function is compatible with the expected value of 1. For shorter time differences, the fit algorithm occasionally locks on the same detection times t_1 and t_2, redistributing pair events to $\Delta t = 0$, resulting in a calculated correlation then deviates from the expected behavior, including the unphysical value $g^{(2)}(\Delta t = 0) > 2$. This instability region ($\Delta t < 150$ ns) is comparable with the rise time of the average single-photon pulse, and is consistent with the precision indicated in Fig. 4.6.

4.6 Conclusion

We demonstrated a signal processing method based on a Schmitt-trigger based data acquisition and a linear algorithm that can reliably extract both a photon number and photodetection times from the signal provided by an optical Transition Edge Sensor (TES) with an accuracy that is mostly limited by the detector time jitter.

Using this method, we successfully resolved between $n = 1, 2$ and 3 photons from a CW NIR source, using the signal integral evaluated in the time interval identified by the discriminator. The time interval includes a greater fraction of the photodetection signal than that considered by a single-threshold discriminator. By considering an optimal fraction of the pulse profile, we obtained pulse integral distributions that sufficiently resolve between photon numbers. We note that the maximum pulse height is unsuitable for photon number discrimination of a CW source since the maximum height depends on the photodetection times when pulses are overlapped. This is evident in Fig. 4.2. In contrast, Fig. 4.3 shows that $n = 1, 2$ and 3 photon events are well resolved using the pulse integral, which does not depend on photodetection times. Although we do not demonstrate photon number resolution for $n > 3$, transition edge sensors can resolve $n > 10$ photons from pulsed sources [109]. We expect a similar extension to be possible for CW sources.

This technique provides an alternative to photon counting using edge detection on the differentiated signal [100] when signal-to-noise ratio is low.

The discriminated region is then used to initialize a least-squares fit of a signal containing two overlapping pulses to a two-photon model, returning the amplitudes and detection-times of the individual photons.

With the available TES, we can distinguish two photodetection events within about 150 ns using this method. The highest detection rate that can be processed is thus estimated to be about 6.7×10^6 s^{-1}, compared to about 4.0×10^5 s^{-1} if we were to discard overlapping pulses, corresponding to more than an order of magnitude improvement.

The timing extraction algorithm presented here could be applied to future Bell experiments performed with TESs, registering photodetection events which were previously neglected using threshold discrimination methods, resulting in an increase in Bell violation and randomness generation rate. For the photon flux generated in our Bell experiment (Chapter 3), we estimate that $\approx 0.4\,\%$ of the detection events can be recovered with the algorithm, which increases the randomness generation rate by $\approx 8\,\%$[3]. For higher photon fluxes, the probability of signals

[3]This result was obtained by using the simulation in Section 2.3 to estimate the new S value due to a higher effective detection efficiency, and using it to estimate the new asymptotic randomness generation rate, which is described in Section 2.4.

overlapping is higher, and the randomness generation rate that results from the use of the timing extraction algorithm increases correspondingly.

Other potential applications include the measurement of time-resolved correlation functions using the TES without the need for the spatial multiplexing of several single-photon non-photon-number resolving detectors, provided that the coherence time of the light source is larger than the timing resolution of this technique. The order of the correlation function measured is limited only by the maximum number of photons resolvable by the TES. The algorithm is published in Ref. [110] and is freely available on Github[4].

[4] https://github.com/hoopernikaho/TESPulseFitCode.git

Chapter 5

Symmetrical clock synchronization with time-correlated photon pairs

In this chapter, we describe a distance-independent protocol using counter-propagating single photons originating from photon pairs [39]. Tight time correlations of photon pairs generated from spontaneous parametric down-conversion (SPDC) enable precise synchronization. The single-photon regime allows, in principle, an additional security layer by testing a Bell inequality with entangled photons to verify the origin of the timing signal [42]. While clock synchronization based on SPDC has been demonstrated, previous works require knowing *a priori* the signal propagation times [43–45], controlling them with a balanced interferometer [46], or were performed with clocks sharing a common frequency reference [47, 48]. Here, we synchronize remote clocks referenced to independent frequency standards using two separate SPDC pair sources. We obtain a synchronization precision consistent with the intrinsic frequency instabilities of our clocks, while changing their relative separation [49]. Protocol vulnerability to attacks which evade the Bell inequality check is examined in Chapter 6.

5.1 Time synchronization protocol

The protocol involves two parties, Alice and Bob, connected by a single mode optical channel. Each party has an SPDC source producing photons pairs, one photon is detected locally, while the other is sent and detected on the remote side (see Fig. 5.1). Every photodetection event is time tagged according to a local clock which assigns time stamps t and t'.

For a propagation time Δt_{AB} from Alice to Bob, and Δt_{BA} in the other direction, the detection time differences are

$$t' - t = \Delta t_{AB} + \delta \quad \text{and} \quad t - t' = \Delta t_{BA} - \delta \tag{5.1}$$

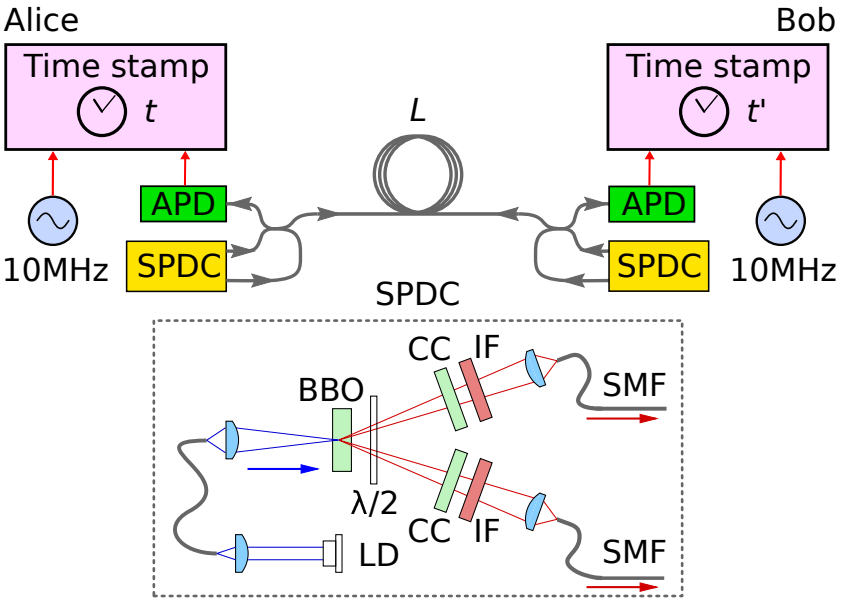


Figure 5.1: Clock synchronization setup. Alice and Bob each have a source of time-correlated photon pairs based on spontaneous parametric down-conversion (SPDC), and an avalanche photodetector (APD). One photon of the pair is detected locally, while the other photon is sent through a single mode fiber of length L to be detected on the remote side. Times of arrival for all detected photons are recorded at each side with respect to the local clock, each locked to a rubidium frequency reference. The inset shows the optical setup of a SPDC source [6]. LD: laser diode, BBO: β-Barium Borate, CC: compensation crystals, SMF: single mode fiber, $\lambda/2$: half-wave plate.

for the photon pairs originating from Alice and Bob, respectively. The sequence of photodetection events on each side are described by

$$a(t) = \sum_i \delta\left(t - t_i\right) \quad \text{and} \quad b(t') = \sum_j \delta\left(t' - t'_j\right) . \tag{5.2}$$

Due to tight time correlations present during pair generation, the cross-correlation

$$c_{AB}(\tau) = (a \star b)(\tau) = \int a(t) b(t+\tau) \mathrm{d}t \tag{5.3}$$

will show two peaks at

$$\tau_{AB} = \delta + \Delta t_{AB} \quad \text{and} \quad \tau_{BA} = \delta - \Delta t_{BA} \tag{5.4}$$

for the pairs created by Alice and Bob.

A round-trip time ΔT for photons can be calculated using the inter-peak separation,

$$\Delta T = \Delta t_{AB} + \Delta t_{BA} = \tau_{AB} - \tau_{BA}. \tag{5.5}$$

If the propagation times in the two directions are the same, $\Delta t_{AB} = \Delta t_{BA}$, they do not contribute to the clock offset

$$\delta = \frac{1}{2}\left(\tau_{AB} + \tau_{BA}\right), \tag{5.6}$$

which is calculated directly from the midpoint of the two peaks. In this way, the protocol is inherently robust against symmetric changes in channel propagation times.

As is the norm in quantum key distribution (QKD) [111], the time stamps are transmitted through a classical public authenticated channel, while the quantum channel is supposed to be under the control of a malicious adversary.

5.2 Experiment

Time-correlated photon pairs are generated by two identical SPDC sources (Fig. 5.1). The output of a laser diode (power ≈10 mW, central wavelength 405 nm) is coupled into a single mode optical fiber for spatial mode filtering and focused to a beam waist of 80 μm into a 2 mm thick β-Barium Borate crystal cut for non-collinear type-II phase matching [6]. Down-converted photons at 810 nm are coupled into two single mode fibers; with an overall detected pair rate of about 200 s^{-1}.

Fiber beam splitters separate the photon pairs so that one photon is detected locally with an avalanche photodetector (APD), while the other photon is transmitted to the remote party. Time-stamping units with nominal resolution ≈ 4 ps assign detection times t and t' to the events detected at Alice and Bob, respectively.

To resolve the coincidence peaks (FWHM ≈ 500 ps), we obtain $c_{AB}(\tau = t' - t)$ with coarse (≈ 2 μs) and fine (≈ 16 ps) resolutions separately [44].

To extract the peak positions τ_{AB} and τ_{BA}, we fit $c_{AB}(\tau)$ to a linear combination of two peak profiles $V(\tau)$,

$$c_{AB}(\tau) = a_0 + a_1 V(\tau - \tau_{AB}) + a_2 V(\tau - \tau_{BA}), \tag{5.7}$$

where a_0 denotes background coincidences, $a_{1,2}$ detected pairs, and $V(\tau)$ is a pseudo-Voigt distribution [112]

$$V(\tau) = (1-f)\,G\left(\tau, \frac{\sigma}{\sqrt{2\ln 2}}\right) + f\,L(\tau,\sigma). \tag{5.8}$$

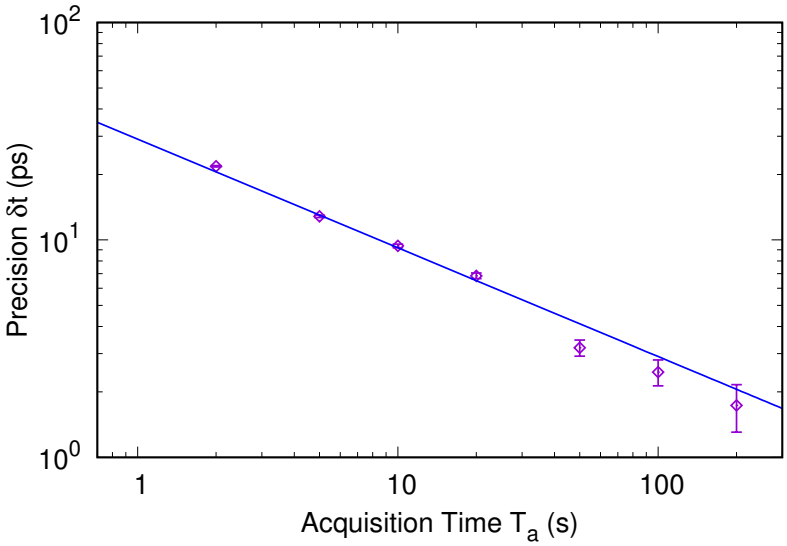


Figure 5.2: Standard deviation (precision δt) of the measured offset between two clocks. Both clocks are locked to the same frequency reference. Solid line: Least-squares fit to a model where δt follows Poisson statistics and improves with acquisition time T_a. Error bars: precision uncertainty due to errors from fitting c_{AB} to our model in Eq. 5.7.

The functions

$$G(\tau,\sigma) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\tau^2/2\sigma^2} \quad \text{and} \quad L(\tau,\gamma) = \frac{\gamma}{\pi(\tau^2+\gamma^2)}$$

represent Gaussian and Lorentzian distributions, respectively.

Values of $f = 0.2$ and $\sigma = 290\,\text{ps}$ best characterize the timing jitter (FWHM$= 2\sigma = 580\,\text{ps}$) of the combined photodetection and time-stamping system, and τ_{AB}, τ_{BA} from the fit fix δ and ΔT through equations 5.5 and 5.6.

5.3 Results

5.3.1 Synchronization precision

To demonstrate the independence of the protocol from the clock separation, we first determine the minimum resolvable separation ($v\,\delta t/2$), where v is the propagation speed of light in the fiber, and δt is the precision (1 standard deviation) of measuring a fixed offset.

To characterize the precision δt, we accumulate offset measurements between two clocks locked to a common frequency reference (Stanford Research Systems FS725), separated by a constant fiber length $L = 1.7\,\text{m}$. The standard deviation of the measured offset depends on the detector timing response $V(\tau = 0)$, pair rate $R = 227\,\text{s}^{-1}$ and acquisition time T_a according to [113]

$$\delta t = \frac{1}{\sqrt{2}} \frac{1}{2V(\tau=0)} \frac{1}{\sqrt{RT_a}}. \tag{5.9}$$

Fig. 5.2 shows the precision of the measured offset for various T_a, extracted from time stamps recorded over 1 hour. Fitting the data to the model in Eq. 5.9, we obtain $\delta t = 2.91(9) \times 10^{-11} / \sqrt{T_a}$ and infer $V(\tau = 0) = 0.81(4)$ ns^{-1}. The inferred detector timing response is approximately twice the value (1.5 ns^{-1}) expected using Eq. 5.8. Faster detectors, such as superconducting nanowire single photon detectors (SNSPDs), improves precision by an order-of-magnitude [47].

For an acquisition lasting several seconds, a precision of a few picoseconds limits the minimum resolvable clock separation to the millimeter scale. To demonstrate that the protocol is secure against symmetric channel delay attacks, we change the propagation length over several meters during synchronization – three orders of magnitude larger than the minimum resolvable length-scale.

5.3.2 Distance-independent clock synchronization

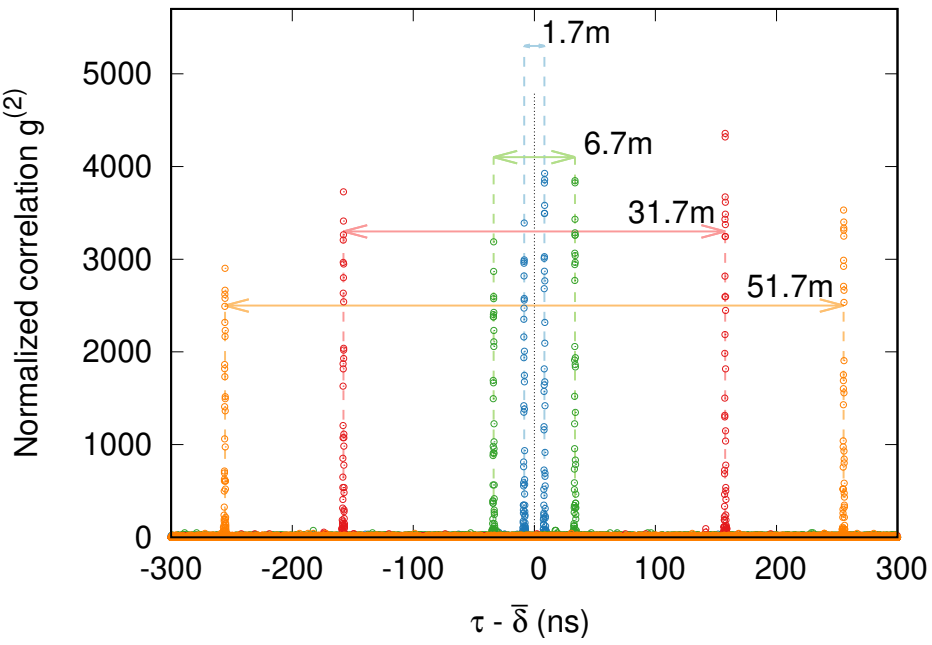


Figure 5.3: Timing correlations of Alice and Bob's detection events normalized to background coincidences. During the measurement, four fibers of lengths L were used to change the separation between Alice and Bob. For every L, the correlation measurement yields two coincidence peaks, one for each source. The time separation between peaks corresponds to the round-trip time ΔT, and the midpoint is the offset between the clocks δ. The time axis is shifted by $\overline{\delta}$,the average value of the four δ calculated for four different L.

To simulate a symmetric channel delay attack, we impose different propagation distances using different fibers of length $L = 1.7\,\text{m}$, $6.7\,\text{m}$, $31.7\,\text{m}$, and $51.7\,\text{m}$. Fig. 5.3 shows $g^{(2)}(\tau)$, the cross-correlation $c_{AB}(\tau)$ normalized to background coincidences, acquired from the time stamps recorded over 20 mins. To detect changes in the clock offset throughout the acquisition, we split the time-stamped events into blocks of 20 s. Fig. 5.4 shows the clock offset δ and round-trip time ΔT for every block. Throughout the acquisition, the offset was measured to within 7 ps, comparable to the precision obtained with a constant round-trip time (Fig. 5.2). With no significant correlation between the measured clock offset and the propagation distance ($\lesssim 0.12\,\text{ps}\,\text{m}^{-1}$), we conclude that for measuring a fixed offset, the protocol is robust against symmetric channel delay attacks.

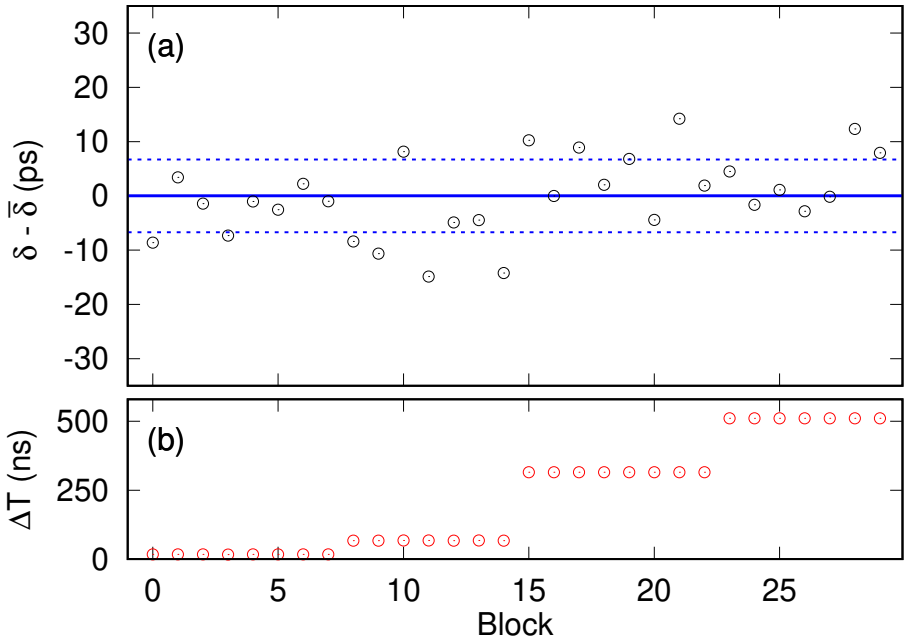


Figure 5.4: (a) Measured offset δ between two clocks, both locked on the same frequency reference. Each value of δ was evaluated from measuring photon pair timing correlations from a block of photodetection times recorded by Alice and Bob. Each block is 20 s long. The continuous line indicates the average offset $\overline{\delta}$. Dashed lines: one standard deviation. (b) The round-trip time ΔT was changed using different fiber lengths.

5.3.3 Distance-independent clock synchronization with independent clocks

To examine a more realistic scenario, we provide each time-stamping unit with an independent frequency reference (both Stanford Research Systems FS725), resulting in a clock offset that drifts with time $\delta \to \delta(t)$.

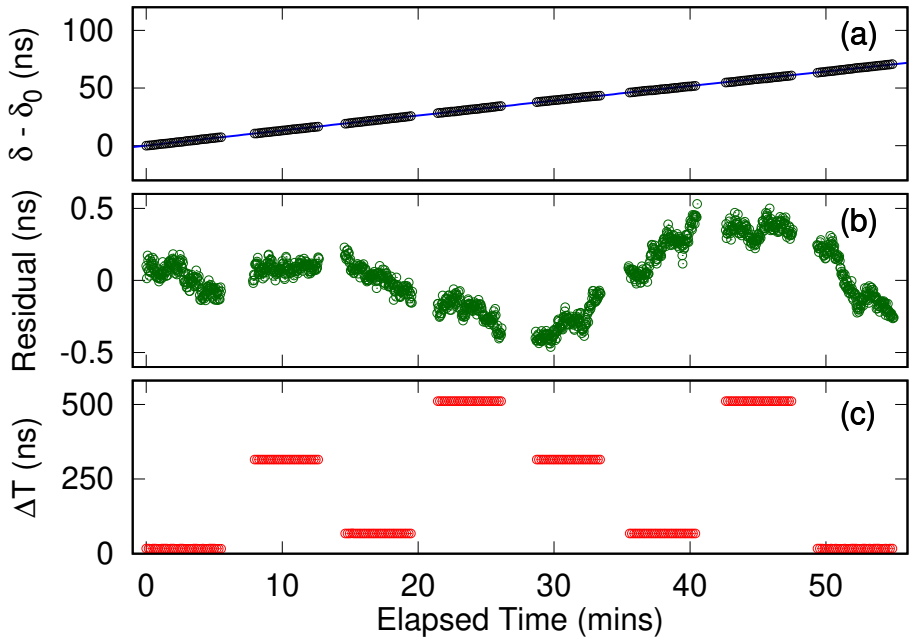


Figure 5.5: (a) Measured offset δ between two clocks with different frequency references. Each value of δ was evaluated from measuring photon pair timing correlations for 2 s. The offset measured at the beginning is δ_0. Continuous blue line: fit used to extract the relative frequency accuracy ($\approx 4 \times 10^{-11}$) between the clocks. (b) Residual of the fit fluctuates due to the intrinsic instability of the individual frequency references. (c) The round-trip time ΔT was changed using four different fiber lengths.

The frequency references have a nominal relative frequency accuracy $d_0 < 5 \times 10^{-11}$. We evaluate the offset from the time stamps every $T_a = 2\,\mathrm{s}$ so that the drift ($\approx 100\,\mathrm{ps}$) is much smaller than the FWHM of each coincidence peak. This allows extracting the peak positions from c_{AB} with the model in Eq. 5.7.

We again simulate a symmetric channel delay attack by changing L every 5 mins. Fig. 5.5 shows the measured $\delta(t)$ which appears to follow a continuous trend over different round-trip times, indicating that the delay attacks were ineffective. Discontinuities in $\delta(t)$ correspond to periods when fibers were changed.

To verify that meaningful clock parameters can be extracted from $\delta(t)$ despite the attack, we fit the data to a parabola $at^2 + dt + b$, where a, d and b represent the relative aging, frequency accuracy and bias of the frequency references, respectively [114]. The resulting relative frequency accuracy between the clocks, $d = 4.05(7) \times 10^{-11}$, agrees with the nominal relative frequency accuracy d_0 of our frequency references. The residual of the fit, $r(t)$, fluctuates (Allan deviation $= 1.1 \times 10^{-12}$, time deviation TDEV = 45 ps, in 100 s) mainly due to the intrinsic

instabilities of our frequency references ($< 2 \times 10^{-12}$). Negligible correlation between $r(t)$ and propagation distance ($\lesssim 0.78\,\mathrm{ps\,m^{-1}}$) demonstrates the distance-independence of this protocol.

The standard deviation ($\delta t \approx 51\,\mathrm{ps}$) of the fast fluctuating component of $r(t)$ suggests that the clocks can be synchronized to a precision comparable to the time deviation of our frequency references in 100 s. This integration time improves with detectors with a lower timing jitter, higher efficiency, a higher path transmission, and with brighter pair sources (Eq. 5.9).

5.4 Protocol Security

Although not demonstrated in this work, Alice and Bob can verify the origin of each photon by synchronizing with polarization-entangled photon pairs and performing a Bell measurement to check for correspondence between the local and transmitted photons. As is the case in QKD scenarios [11], if the signal is copied (cloned) or the entangled degree of freedom is otherwise disturbed, the extent of the interference can be bounded via a Bell inequality. For this measurement, the setup in Fig. 5.1 should be modified such that the detectors are preceded by a polarization measurement in the appropriate basis and that measurement result is added to the time stamp information transmitted through the classical channel. This modification addresses the issue of spoofing in current classical synchronization protocols.

In addition, we made the strong assumption that the photon propagation times in both directions were equal ($\Delta t_{AB} = \Delta t_{BA}$). Without this assumption, the offset derived from Eq. 5.6 becomes

$$\delta = \frac{1}{2}\left[(\tau_{AB} + \tau_{BA}) - (\Delta t_{AB} - \Delta t_{BA})\right]. \tag{5.10}$$

Therefore, the offset can no longer be obtained from the midpoint between τ_{AB} and τ_{BA}.

We note that while creating an asymmetric channel for a classical signal is routine given the ability to split and amplify the signal at will; in the case of entangled photons produced at random times, making an asymmetric channel implies breaking the reciprocity of the channel. This is possible, via for example magneto-optical effects such as found in optical circulators, and is explored in the following chapter.

5.5 Conclusion

We have demonstrated a protocol for synchronizing two remote clocks with time-correlated photon pairs generated from SPDC. By assuming symmetry in the synchronization channel, the protocol does not require *a priori* knowledge of the relative distance or propagation times

between two parties, providing security against symmetric channel delay attacks. Although we do not perform an experimental demonstration, synchronizing with entangled photon pairs should allow, in principle, timing signal verification via the measurement of a Bell inequality (Section. 5.4).

We observe a synchronization precision of 51 ps within 100 s between two clocks with independent frequency references. The achieved precision is comparable to the time deviation arising from the intrinsic instability of our frequency references, even with relatively low pair rates ($\approx 200\ s^{-1}$), and improves with faster detectors or more stable frequency references [47].

The protocol lends itself particularly well to synchronization tasks performed between mobile stations (e.g., between satellites and ground stations) where photon rates are typically low, and propagation times are constantly changing. Since the protocol is based on existing quantum communication techniques, it provides a natural complement to Global Navigation Satellite Systems (GNSS) and would be a natural fit to future quantum networks with the ability to distribute entanglement.

Chapter 6

Asymmetric delay attack on an entanglement-based bidirectional clock synchronization protocol

In Chapter 5, we demonstrated an absolute clock synchronization protocol performed with time-correlated photon pairs, and described its vulnerability to an attack that introduces a direction-dependent delay in the synchronization channel. This attack is based on the fact that the protocol, similar to existing bidirectional protocols, e.g., the Network Time Protocol (NTP) or the two-way satellite time transfer (TWSTFT), relies on a symmetrical channel for deducing the correct offset between remote clocks [31, 115]. Although security against spoofing attacks can be enhanced by using a Bell inequality check with entangled photons (Section. 5.4), vulnerability to an asymmetric delay attack remains – photons traveling in opposite directions can be passively rerouted with a circulator (Fig. 6.1), which uses the Faraday effect to break the reciprocity of the channel.

Recently, a proposal suggests that even polarization-insensitive circulators, which rotate input polarizations back to the same state, impose a measurable change in the phase of the joint state [50]. The proposal was based on the fact that the phase change after a cyclic quantum evolution is measurable under certain conditions [7]. Previous experiments with entangled photons [51–54] seemed to support this proposed protection.

In this chapter, we examine the circulator-based asymmetric delay attack [50] on the protocol introduced in Chapter 5. We experimentally show that the attack *cannot* be detected by the proposed mechanism and demonstrate an induced error in synchronization of over 25 ns between two rubidium clocks.

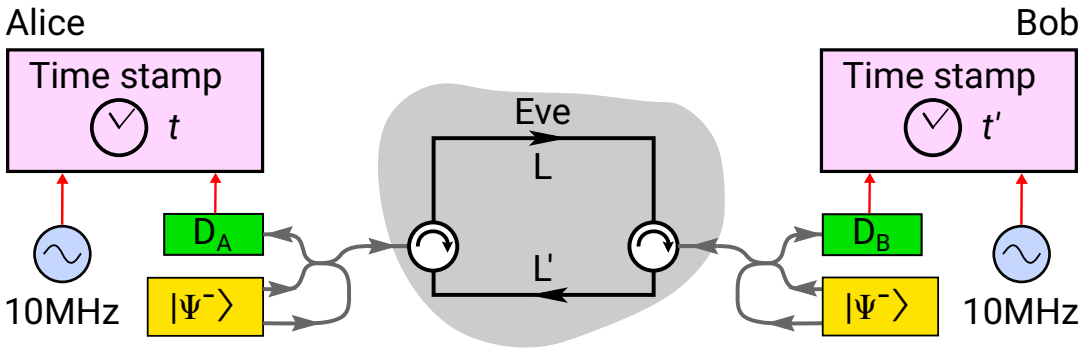


Figure 6.1: Clock synchronization scheme. Alice and Bob each have a source of polarization-entangled photon pairs $|\Psi^-\rangle$, and avalanche photodetectors at $D_{A,B}$. One photon of the pair is detected locally, while the other photon is sent through a fiber to be detected on the remote side. Arrival times for all detected photons are recorded at each side with respect to local clocks, each locked to a rubidium frequency reference. Grey region: asymmetric delay attack. An adversary (Eve) uses a pair of circulators to introduce a direction-dependent propagation delay:photons originating at Bob's site will always take the bottom path, while photons originating at Alice's side will take the top path.

6.1 Attacking an Entanglement-Based Clock Synchronization Protocol

In Chapter 5, we described how Alice and Bob, each having a source of correlated photon pairs, generate two coincidence peaks in the cross-correlation of the detection times recorded on each side (Fig. 5.3), and use them to deduce the offset between their clocks. For two peaks located at τ_{AB} and τ_{BA}, and a propagation time delay Δt_{AB} from Alice to Bob and Δt_{BA} in the other direction, the offset between two clocks

$$\delta = \frac{1}{2}\left[(\tau_{AB} + \tau_{BA}) - (\Delta t_{AB} - \Delta t_{BA})\right] \tag{6.1}$$

is given by the midpoint between the two peaks, $(\tau_{AB} + \tau_{BA})/2$, and the propagation delay asymmetry, $(\Delta t_{AB} - \Delta t_{BA})$, respectively.

When parties assume a symmetrical channel, $\Delta t_{AB} = \Delta t_{BA}$, they may determine the offset directly from the midpoint from the two peaks

$$\delta = \frac{1}{2}(\tau_{AB} + \tau_{BA}) \tag{6.2}$$

but expose themselves to the following attack: an adversary, Eve, may now may exploit this assumption by separating the two propagation directions with a pair of circulators (Fig. 6.1 grey region), introducing a direction-dependent delay

$$\Delta t_{AB} - \Delta t_{BA} = \frac{L - L'}{v}, \tag{6.3}$$

where L is the additional propagation length from Alice to Bob, and L' in the other direction, and v is the speed of light in the fiber. If Alice and Bob continue to rely on the midpoint between the peaks to estimate δ, they will obtain instead $\delta + (L - L')/2v$.

In an attempt to detect the circulators, Ref. [50] suggests that Alice and Bob monitor polarization correlations using avalanche photodiode preceded by a polarization measurement in the appropriate bases ($D_{A,B}$). The detection scheme is based on the fact that circulators use Faraday Rotation to separate photons propagating in opposite directions – Faraday Rotation is a time-reversal symmetry breaking mechanism that rotates polarization, potentially changing the input state.

For each individual polarization state to be preserved, the circulators must rotate the state by an integer multiple of 180° so that for a Bell state $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle)$ distributed by Alice, the rotation of Bob's state ($|\psi\rangle_B \rightarrow \pm|\psi\rangle_B$) does not result in any measurable change

$$|\Psi^-\rangle \rightarrow \pm\frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle) = \pm|\Psi^-\rangle. \tag{6.4}$$

However, as the evolution of Bob's state follows a closed trajectory on the Poincaré sphere, Ref. [50] predicted that a geometric phase – the phase determined by the geometry of the trajectory on the sphere [7] – is imposed on the Bell state, and can be detected in a non-local measurement. We show in Appendix A that when other phase contributions are taken into account, the net effect of the circulators nonetheless produce no measurable change to the Bell state (Eq. 6.4). We use this result and experimentally demonstrate a successful asymmetric delay attack using the circulators in subsequent sections.

6.2 Experiment

We implement the clock synchronization protocol described in Section 5.2. For the purposes of demonstrating the asymmetric delay attack, we lock the clocks with unknown offset to a common rubidium frequency reference, thus avoiding frequency drifts that can detract from the main point of the experiment, i.e. demonstrating an induced error in offset estimation.

6.2.1 Asymmetric Delay Attack

To implement the asymmetric delay attack, we use two 3-port polarization-insensitive optical circulators of design-wavelength 810 nm and two single mode fibers of lengths L and L'.

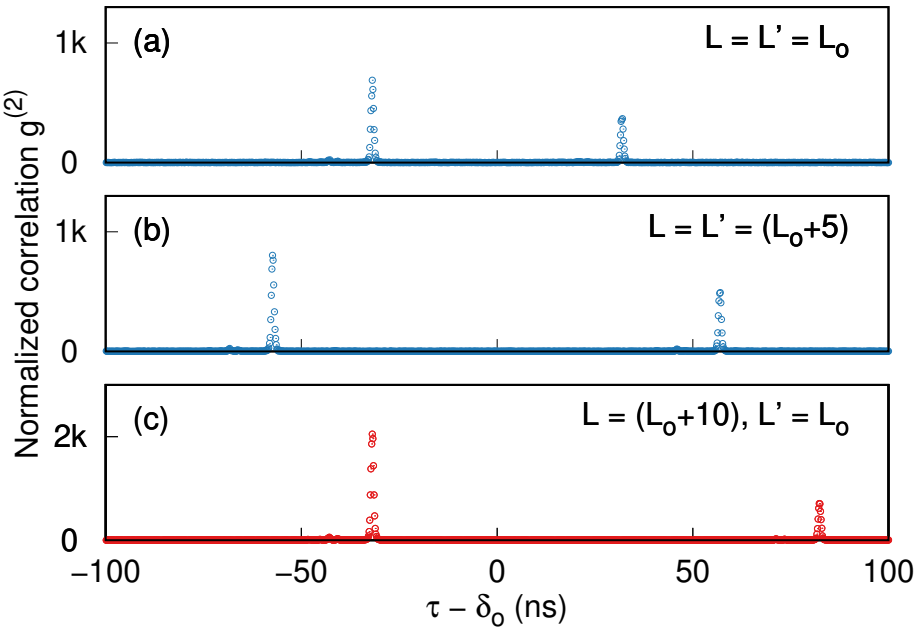


Figure 6.2: Time correlations of Alice and Bob's detection events normalized to background coincidences. The separation between peaks corresponds to the round-trip time ΔT, and the midpoint is the offset between the clocks δ. Symmetric delays with $L = L'$ show that the offset remains constant for both the (a) initial and (b) extended round-trip times. An asymmetric delay with (c) $L = L' + 10$ results in an offset shift. $L_o/2$: minimum length of the fiber belonging to each circulator port. δ_o: the offset estimated in (a).

We first estimate the initial offset δ_o between the two clocks with a symmetric channel delay $L = L' = L_o$. Fig. 6.2(a) shows $g^{(2)}(\tau = t' - t)$, the cross correlation function normalized to background coincidences, acquired from the time stamps recorded for about 5 min. In Fig. 6.3 we plot the offset and round-trip times estimated every 40 s.

To illustrate the difference in the cross-correlation measured between a symmetric and an asymmetric delay attack, we use two 5 m fibers to impose an additional round-trip of 10 m, but distribute them differently during each attack. For the symmetric delay attack, we extend L and L' equally by 5 m. We observe in Fig. 6.2(b) that although the peak separation increases, the midpoint of the peaks used for estimating the offset remains unchanged. For the asymmetric delay attack, both fibers are used to extend L by 10 m, while L' remains unchanged. We observe

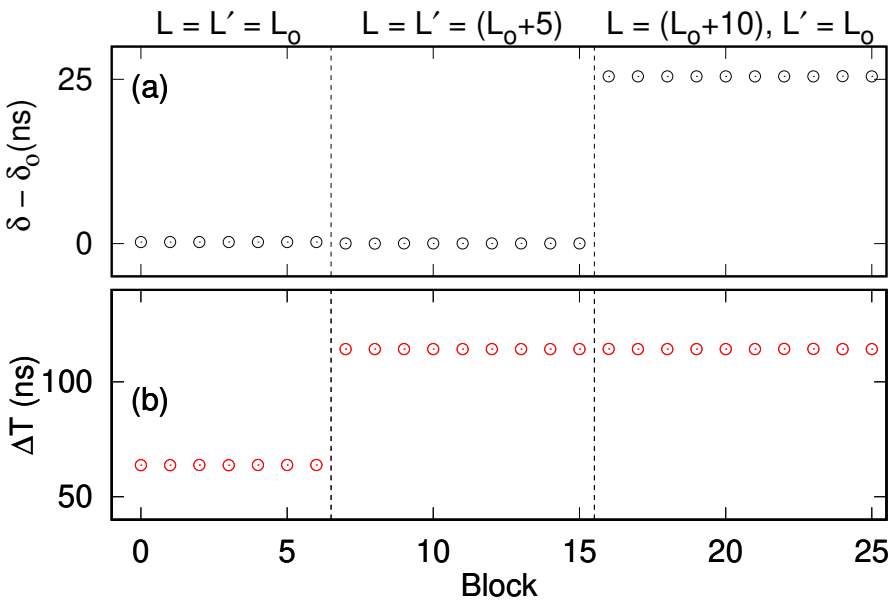


Figure 6.3: (a) Measured offset δ between two clocks, both locked on the same frequency reference. Each value of δ was evaluated from measuring photon pair timing correlations from a block of photodetection times recorded by Alice and Bob. Each block is 40 s long. (b) The round-trip time ΔT. Block 6 to 7: increasing the symmetric delay ($L = L'$) does not change δ. Block 15 to 16: introducing an asymmetric delay ($L \neq L'$) creates an offset error. δ_0: offset measured in the first block.

in Fig. 6.2(c) that the peak separation remains the same as in Fig. 6.2(b), but the midpoint of the peaks has shifted by $25.24(2)$ ns corresponding to half the additional round-trip time incurred. This indicates a successful attack.

6.2.2 Asymmetric Delay Attack Detection

As a proof-of-principle demonstration of how the circulators influence the distributed entanglement, we measure polarization correlations of Alice's pair source before and after the circulators are inserted in one of its output modes with the setup shown in Fig. 6.4. For each output mode, a quarter-wave plate (QWP), half-wave plate (HWP) and polarizing beamsplitter (PBS) projects the polarization mode into either $|H\rangle, |V\rangle, |D\rangle, |A\rangle, |L\rangle$ or $|R\rangle$. Fiber polarization controllers (FPCs) correct for the polarization errors introduced by the fibers. We note that since FPCs do not break time-reversal symmetry, they cannot invert the polarization transformation induced by

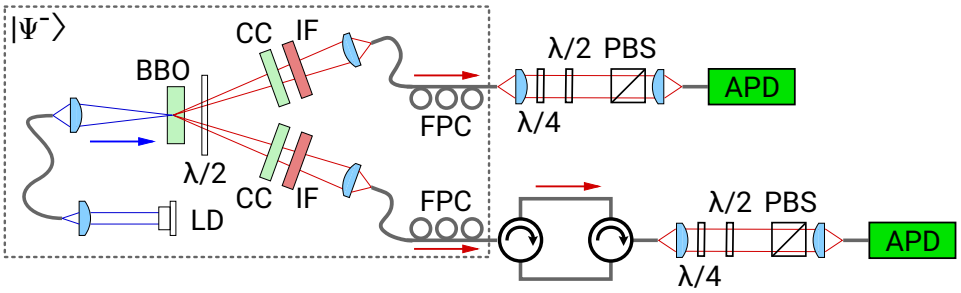


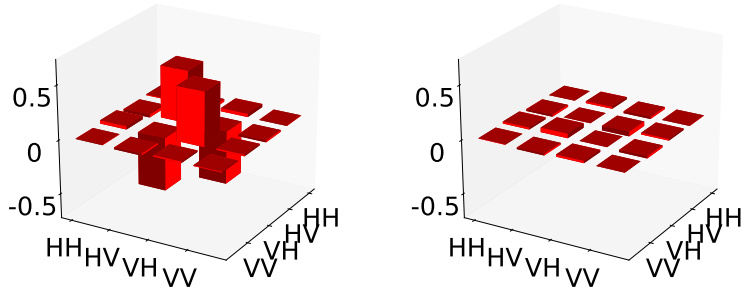
Figure 6.4: Setup for quantum state tomography on a polarization-entangled photon pair state, with one photon passing through a pair of circulators. Dashed box: optical setup of our polarization-entangled photon source [6]. LD: laser diode, BBO: β-Barium Borate, CC: compensation crystals, FPC: fiber polarization controller, SMF: single mode fiber, $\lambda/4$: quarter-wave plate, $\lambda/2$: half-wave plate, PBS: polarizing beam splitter, APD: avalanche photodiode.

the circulators. We detect photon pairs with APDs for 36 wave plate settings and numerically search for the density matrix most likely to have returned the observed pair rates [116].

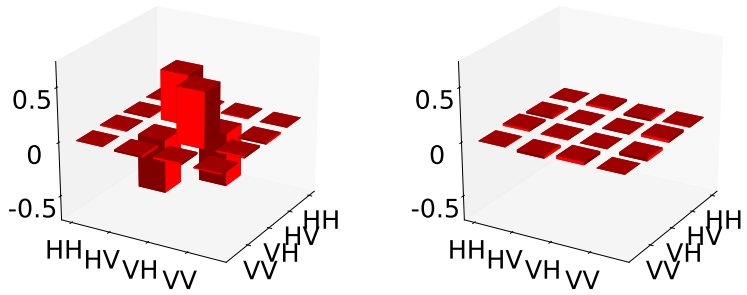
Fig. 6.5 shows the reconstructed density matrices of Alice's state before (ρ_o) and after (ρ) the introduction of the circulators into the path of Bob's photons. We compare ρ_o and ρ by computing the fidelity $F(\rho,\rho_o) = \left(\mathrm{Tr}\sqrt{\sqrt{\rho}\rho_o\sqrt{\rho}}\right)^2$. The uncertainty in F due to errors in counting statistics was obtained by Monte Carlo simulation, where 36 new measurement results are numerically generated, each drawn randomly from a Poissonian distribution with a mean equal to the original number of counts [116]. From these numerically generated results, a new density matrix can be calculated and consequently, a new value of F. Repeating this process 100 times, we obtain the fidelity distribution shown in Fig. 6.6 from which we compute a 95% confidence interval $98.7\% < F < 98.9\%$. The distribution of F does not include 100%, which we attribute to imperfect control of the polarization state in the optical fiber. From the near-unity value of F, we conclude that the circulators do not affect the distributed Bell state.

6.3 Conclusion

We have successfully demonstrated an attack of a clock synchronization protocol that tries to achieve security by detecting changes in polarization-entanglement distributed across a synchronization channel. The attack was implemented by rerouting photons with polarization-insensitive circulators, and imposing a direction-dependent propagation delay. The observed shift in the estimated clock offset is equal to half the propagation delay asymmetry, as expected for a protocol which assumes a symmetric channel [34]. Although circulators reroute photons using a polarization-rotation mechanism, we experimentally verify that they produce no mea-



(a) Before insertion of circulators, fidelity with $|\Psi^-\rangle$: 98.2%.



(b) After insertion of circulators, fidelity with $|\Psi^-\rangle$: 98.4%.

Figure 6.5: Real and imaginary part of the reconstructed density matrix for the target Bell state $|\Psi^-\rangle$ originating from Alice's source. Bob receives one photon of the pair through the synchronization channel. The density matrices obtained (a) before and (b) after polarization-insensitive circulators are inserted (Fig. 6.4) do not deviate significantly from $|\Psi^-\rangle$.

surable change in the distributed entangled state, indicating that they cannot be detected with the protocol.

In this thesis, we focused on detecting its underlying mechanism – Faraday Rotation (FR), which must be performed in any circulator. Methods based on characterizing light intensities, e.g. identifying additional reflections, may still allow the detection of circulators, but they rely on the specific characteristics of the device (e.g. reflectivity). We also note that when Alice and Bob exchange photons that are identical in every other degree-of-freedom apart from propagation direction, there are few technologies besides a FR-based circulator capable of discreetly separating their photons. Alternatives such as advanced photonic structures [117–121] and quantum non-demolition measurements [122] still pose a significant technological barrier for any adversary, so entanglement-based clock synchronization still may provide a significant security advantage compared to traditional methods.

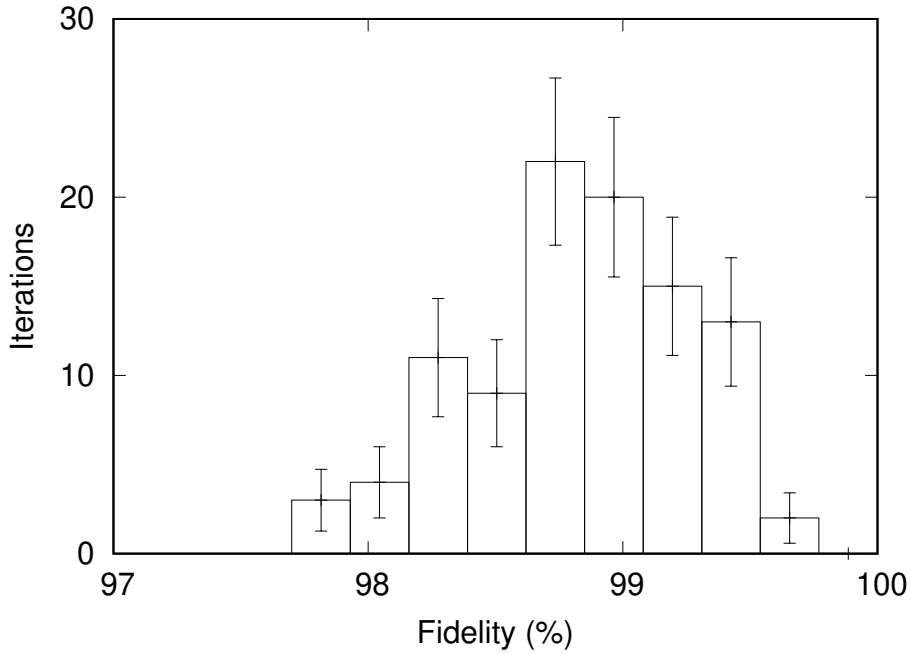


Figure 6.6: Fidelity distribution comparing the Bell state originating from Alice's source before and after introducing the circulators. The distribution is generated by numerically propagating errors due to counting statistics. A high mean fidelity suggests that the state remains unchanged and cannot be used to detect the attack. Error bars: Poissonian standard deviation.

In Appendix A, we also examine the geometric phase associated with polarization state rotation in the circulators, previously thought to be observable [50], as an additional phase associated with photon dynamics in the Faraday Rotator neutralizes this geometric phase. We note that when geometric phases were observed in other entangled systems, an interferometric arrangement was necessary to eliminate the influence of this "dynamic" phase [51–54]. Whether or not a similar technique can be used to secure the present synchronization protocol remains an open question.

Chapter 7

Conclusion

We have demonstrated two protocols related to secure communication enhanced with entangled photons. The photons were generated from continuous spontaneous parametric down-conversion (SPDC), whose features were exploited in the respective protocols.

The first protocol improves on the extraction of private random numbers from quantum entanglement. Entangled systems can be certified to generate randomness uncorrelated with any outside process or variable by violating a Bell inequality. The amount of violation, and the repetition rate of the Bell test, determine the randomness extraction rate.

In this thesis, we demonstrated a dramatic reduction in acquisition time for generating certified randomness at rates competitive with earlier state of the art experiments (Chapter 3). This was achieved through a framework capable of encoding a stream of detection events from a continuous source of entangled photons, which eliminated the intrinsic dead time found in current experiments performed with pulsed sources. We violated the Bell inequality closing the detection loophole, and maximized the randomness generation rate by an optimal choice of the entangled state, measurement basis, and the duration of the time bins used to organize the detection events. Using an extractor secure against a quantum adversary with quantum side information, we calculated an asymptotic rate of ≈ 1300 random bits/s. With an experimental run of 43 minutes, the extractor generated 617920 random bits, corresponding to ≈ 240 random bits/s [30].

As the randomness generation rate increases with higher detected photon pair rates, we pursued a novel timing extraction algorithm that increased the maximum detectable photon flux rate by the our high-efficiency detectors (Chapter 4). When our detector, a transition-edge sensor (TES), absorbs a single photon, it generates an electric pulse response with a fast (tens of nanoseconds) rising edge, and a relaxation with a time constant of a few microseconds. Consequently, photodetection events with time separation shorter than the pulse duration

overlap and cannot be reliably identified by threshold crossing – the method used previously during our Bell experiment. However, by coarsely identifying photodetection events in time with a two-level discriminator, and fitting to a heuristic model, we were able resolve detection times of overlapping TES pulses down to about 150 ns. This algorithm increases the maximum detectable flux rate by about an order of magnitude [110].

The second protocol introduced in this thesis synchronizes remote clocks using entangled photon pairs (Chapter 5). Tight time-correlation between two photons in a pair produced from SPDC provides a coincidence signature useful for synchronization, while a Bell inequality check allows remote parties to verify the origin of the photons. By exchanging counter-propagating photons, the protocol is also secure against a symmetric delay attack where the propagation delay is changed without the users' knowledge, but remains equal in both propagation directions. We demonstrated the timing aspect of this protocol using time-correlated photon pairs and showed that two independent rubidium clocks can be synchronized independently of their separation distance, to a precision of 51 ps in 100 s, using a pair rate of order 200 s^{-1} [49].

Next, we tested the security aspect of the protocol by investigating its vulnerability against an asymmetric delay attack, where a direction-dependent delay is deliberately inserted into the synchronization channel (Chapter 6). As the protocol assumes a symmetric channel delay, this attack creates an error in time synchronization. We used polarization-independent circulators to implement the attack, and showed, despite the polarization transformation induced within the circulators, that the attack cannot be detected by monitoring polarization-entanglement distributed across the synchronization channel. In our demonstration, we showed that the attack creates a synchronization error of 25 ns while evading detection [55].

Outlook

Randomness Generation

Randomness generation rate can be improved in two ways. First, by using detectors with smaller jitter and comparable efficiencies with the TES, e.g. superconducting nanowire single-photon detectors (SNSPDs), as is apparent from the simulation results in Fig. 3.17 that illustrate the generate rates for zero detector jitter. Second, we can increase the pump power of our source, thereby increasing the number of measurement rounds containing entangled photon pairs per unit time [3]. The multi-pulse fitting technique introduced in Chapter 4 can be used to manage overlapping signal events at higher photon flux rates.

To improve protocol security, the locality loophole can be closed in future experiments by introducing the appropriate space-like separation between Alice, Bob and the source consistent

with the choice of time bin duration, and the speed of choosing and implementing the measurement settings (Fig. 2.4). To reduce this distance and the associated optical channel losses, a fast polarization rotation switch was developed to reduce the time taken for implementing the measurement setting choice [1].

Clock synchronization

Synchronization precision can be improved with the use of detectors with smaller jitter or higher efficiencies, or with higher photon pair generation rates[1] (Eq. 5.9). Regarding protocol vulnerability to a circulator-based asymmetric delay attack, we note that although the circulators induce a geometric phase on the photons in the synchronization channel, this phase is neutralized by an additional phase associated with photon dynamics due to Faraday Rotation in the circulator. Consequently, this attack evades detection by testing a Bell inequality with the existing scheme. A proof of this result is given in Appendix A, and clarifies the prediction in a previous work [50]. We note that when geometric phases were observed in other entangled systems, an interferometric arrangement was necessary to eliminate the influence of this "dynamic" phase [51–54]. Whether or not a similar technique can be used to secure the present synchronization protocol remains an open question.

[1] With higher pump powers, or with collinear SPDC when producing entangled photons (Section 3.2).

Appendix A

Geometric and dynamic phases imposed by a circulator on a singlet state

In this appendix, we show that when circulators rotate the polarization state of one of the photons in an entangled pair by 180°, the geometric phase imposed on the rotated photon does not produce a measurable change in polarization entanglement.

We first introduce the formalism to deal with the fact that points on the Poincaré sphere carry no phase information; the beginning and end points of a cyclic evolution correspond on the same point on the sphere.

To reflect this property, we define a "basis vector field" $|\tilde{\psi}(t)\rangle$, such that

$$|\tilde{\psi}(t)\rangle = e^{-if(t)}|\psi(t)\rangle \quad \text{and} \quad |\tilde{\psi}(\tau)\rangle = |\tilde{\psi}(0)\rangle, \tag{A.1}$$

where $f(t)$ is the phase of $|\psi(t)\rangle$ expressed in terms of its basis state $|\tilde{\psi}(t)\rangle$ on the Poincaré sphere, and τ the time taken to complete the cycle [123].

To derive the evolution of the function $f(t)$ as the circulator rotates the polarization qubit, we write Schrödinger's equation for the state:

$$i\hbar\frac{\mathrm{d}}{\mathrm{d}t}|\tilde{\psi}(t)\rangle = i\hbar\left(-i\frac{\mathrm{d}f}{\mathrm{d}t}e^{-if(t)}|\psi(t)\rangle + e^{-if(t)}\frac{\mathrm{d}}{\mathrm{d}t}|\psi(t)\rangle\right).$$

From this, we can see that

$$\langle\tilde{\psi}(t)|i\frac{\mathrm{d}}{\mathrm{d}t}|\tilde{\psi}(t)\rangle = \frac{\mathrm{d}f}{\mathrm{d}t} + i\langle\tilde{\psi}|e^{-if(t)}\frac{\mathrm{d}}{\mathrm{d}t}|\psi(t)\rangle.$$

And so,

$$\begin{aligned}\frac{\mathrm{d}f}{\mathrm{d}t} &= \langle\tilde{\psi}(t)|i\frac{\mathrm{d}}{\mathrm{d}t}|\tilde{\psi}(t)\rangle - \langle\psi|i\frac{\mathrm{d}}{\mathrm{d}t}|\psi(t)\rangle \\ &= \langle\tilde{\psi}(t)|i\frac{\mathrm{d}}{\mathrm{d}t}|\tilde{\psi}(t)\rangle - \frac{1}{\hbar}\langle\psi|\hat{H}|\psi(t)\rangle.\end{aligned}$$

Integrating this over the path taken by the qubit from $t = 0$ to $t = \tau$, we have a total phase change Δf given by

$$\Delta f = \beta + \gamma, \tag{A.2}$$

where the geometric phase

$$\beta = \int_0^\tau \langle\tilde{\psi}(t)|i\frac{\mathrm{d}}{\mathrm{d}t}|\tilde{\psi}(t)\rangle \tag{A.3}$$

is due to the evolution of the basis state along a curved geometry, and the dynamic phase

$$\gamma = -\int_0^\tau \langle\psi(t)|i\frac{\mathrm{d}}{\mathrm{d}t}|\psi(t)\rangle \mathrm{d}t \tag{A.4}$$

is due to the photon's dynamics through the rotation medium [50].

Geometric Phase

Berry showed that the geometric phase is proportional only to the solid angle Ω subtended by the cyclic trajectory on the Poincaré sphere [7],

$$\beta = -\frac{1}{2}\Omega. \tag{A.5}$$

Consider a qubit in the initial state[1]

$$|\psi(t=0)\rangle = e^{-i\phi}\cos(\theta/2)|R\rangle + \sin(\theta/2)|L\rangle \tag{A.6}$$

[1]The right and left polarizations are represented by $|R\rangle = \frac{1}{\sqrt{2}}(1,-i)^T$ and $|L\rangle = \frac{1}{\sqrt{2}}(1,i)^T$, respectively.

that underwent a 180° rotation in the plane of polarization ($\phi \to \phi + 2\pi$). On the Poincaré sphere, the state evolves along the trajectory shown in Fig. A.1, subtending a solid angle[2]

$$\begin{aligned}\Omega &= 2\pi \int_0^{\theta} d\theta' \sin\theta' \\ &= 2\pi\,(1-\cos\theta)\,,\end{aligned}$$

corresponding to a geometric phase $\beta = -\pi(1-\cos\theta)$ [50].

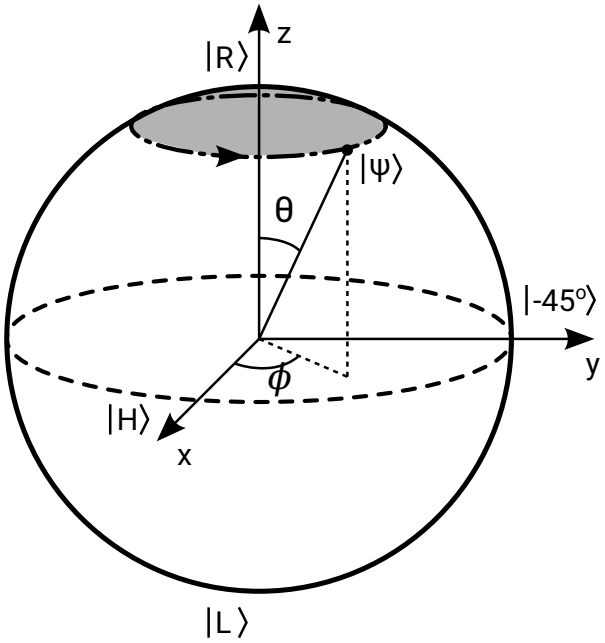


Figure A.1: Rotation of a polarization qubit (Eq. A.6), represented on a Poincaré sphere. For a 180° rotation in the plane of polarization of a single photon, the corresponding trajectory on the Poincaré sphere is a full cycle. Grey region: solid angle subtended by the closed trajectory; this was determined by Berry to be proportional to the geometric phase accumulated by the qubit during its evolution [7]. Image adapted from Ref. [8].

[2]The integrand is obtained by considering an area element $2\pi(r\sin\theta')rd\theta'$ subtended by a small angle $d\theta'$ at a radial distance $r = 1$ from the centre of the Poincaré sphere.

Dynamic Phase

To evaluate the dynamic phase γ accumulated by the photon at end of a Faraday Rotator of length d, we parameterize its expression in Eq. A.4 in terms of the penetration depth z

$$\gamma = -\int_0^d \langle\psi(z)|i\frac{\mathrm{d}}{\mathrm{d}z}|\psi(z)\rangle dz \qquad = -\int_0^d \langle\psi(z)|\hat{N}|\psi(z)\rangle dz, \tag{A.7}$$

where

$$\hat{N} = k\begin{pmatrix} n_R & 0 \\ 0 & n_L \end{pmatrix} \quad \text{and} \quad |\psi(z)\rangle = \begin{pmatrix} e^{ikn_Rz}e^{-i\phi}\cos(\theta/2) \\ e^{ikn_Lz}sin(\theta/2) \end{pmatrix} \tag{A.8}$$

are expressed in the $\{|R\rangle, |L\rangle\}$ basis, and $k = \frac{2\pi}{\lambda}$ is the wave number of the photon mode in free space.

The Faraday Rotator is a birefringent medium whose refractive indices $n_{R,L}$ depend on the magnitude of an applied magnetic field B in the direction of light propagation,

$$n_{R,L} = n_0\left(1 \pm \frac{VB}{kn_0}\right), \tag{A.9}$$

where V is the Verdet constant and n_0 is the index of refraction in the absence of a magnetic field.

Substituting A.8 into A.7, we obtain

$$\gamma = kn_0d + VBd\cos\theta, \tag{A.10}$$

where the product VBd can be shown to be the anti-clockwise rotation angle for a linearly polarized input [124].

Consider an initial input state $|\psi(\phi = 0, \theta = 0)\rangle = |H\rangle$. For the evolution cycle ($\phi = 0 \rightarrow 2\pi$) considered earlier, $|H\rangle \rightarrow |-45\rangle \rightarrow |V\rangle \rightarrow |+45\rangle \rightarrow |H\rangle$ corresponds to a *clockwise* 180° in the plane-of-polarization. Thus, the the rotation must be realized by a medium whose product $VBd = -\pi$. Consequently, the dynamic phase $\gamma = kn_0d - \pi\cos\theta$ for the state considered in Eq. A.6.

Overall Phase & the Circulator Attack

We have already shown that an initial state

$$|\psi\rangle = \cos(\theta/2)|R\rangle + \sin(\theta/2)|L\rangle, \tag{A.11}$$

will accumulate a geometric phase $\beta = -\pi(1-\cos\theta)$ and a dynamic phase $\gamma = kn_0d - \pi\cos\theta$, resulting in an overall phase $\phi = kn_0d - \pi$. Repeating this procedure for the orthogonal state

$$|\psi_\perp\rangle = -\sin(\theta/2)|R\rangle + \cos(\theta/2)|L\rangle, \tag{A.12}$$

we obtain a geometric phase of $\beta' = -\beta = +\pi(1-\cos\theta)$ and a dynamic phase $\gamma' = kn_0d + \pi\cos\theta$, resulting in an overall phase $\phi' = kn_0d + \pi = \phi + 2\pi$.

Let the entangled pair initially be in the Bell state $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle)$. With the first qubit Alice's photon and the second one Bob's photon. We can re-write the Bell state in the basis defined by Equations A.11 and A.12,

$$\begin{aligned} |\Psi^-\rangle &= \frac{1}{\sqrt{2}}\Big(|HV\rangle - |VH\rangle\Big) \\ &= \frac{i}{\sqrt{2}}\Big(|\psi_\perp\rangle_A|\psi\rangle_B - |\psi\rangle_A|\psi_\perp\rangle_B\Big). \end{aligned} \tag{A.13}$$

The state of the Bell pair after Bob's photon goes through Eve's circulator based attack, $\hat{U}_{Attack}$, is given by

$$\begin{aligned} |\Psi^-\rangle &\to \hat{U}_{Attack}\frac{i}{\sqrt{2}}\Big(|\psi_\perp\rangle_A|\psi\rangle_B - |\psi\rangle_A|\psi_\perp\rangle_B\Big) \\ &= \frac{i}{\sqrt{2}}\Big(e^{i\phi}|\psi_\perp\rangle_A|\psi\rangle_B - e^{i\phi'}|\psi\rangle_A|\psi_\perp\rangle_B\Big) \qquad \text{(A.14)} \\ &= \frac{ie^{i\phi}}{\sqrt{2}}\Big(|\psi_\perp\rangle_A|\psi\rangle_B - e^{i2\pi}|\psi\rangle_A|\psi_\perp\rangle_B\Big) \\ &= e^{i\phi}|\Psi^-\rangle = -e^{ikn_0d}|\Psi^-\rangle \\ &\equiv -|\Psi^-\rangle. \qquad \text{(A.15)} \end{aligned}$$

We can see from this expression, that the initial Bell state remains unchanged from the introduction of the circulators, and is equivalent to the result obtained by direct calculation in Eq. 5 in the main text.

Recent work assumed that the contribution from the dynamic phase was "zero, or is known and compensated for" and predicted instead that the circulators imparted a non-local geometric

phase to produce a dramatic change [50]

$$\begin{aligned} |\Psi^-\rangle &\rightarrow \hat{U}_{Attack}\frac{i}{\sqrt{2}}\Big(|\psi_\perp\rangle_A|\psi\rangle_B - |\psi\rangle_A|\psi_\perp\rangle_B\Big) \\ &= \frac{i}{\sqrt{2}}\Big(e^{i\beta}|\psi_\perp\rangle_A|\psi\rangle_B - e^{-i\beta}|\psi\rangle_A|\psi_\perp\rangle_B\Big). \end{aligned} \tag{A.16}$$

However, we note that the dynamic phase (Eq. A.10) is likewise non-local (due to its dependence on θ) and combines with the geometric phase to produce no measurable net change in the state.

References

[1] Siddarth Koduru Joshi. *Entangled photon pairs: Efficient generation and detection, and bit commitment*. PhD thesis, 2014.

[2] Philippe H Eberhard. Background level and counter efficiencies required for a loophole-free einstein-podolsky-rosen experiment. *Physical Review A*, 47(2):R747, 1993.

[3] Shen Lijiong. *Randomness Extraction from Detection Loophole-Free Bell Violation with Continuous Parametric Down-Conversion*. PhD thesis, 2019.

[4] Wikipedia contributors. Constant fraction discriminator — Wikipedia, the free encyclopedia, 2014. [Online; accessed 16-April-2019].

[5] Jiale Cai, Daowu Li, Yingjie Wang, Zhiming Zhang, Peilin Wang, Haohui Tang, Baoyi Wang, Xingzhong Cao, Fuyan Liu, and Long Wei. Design of a high-sampling-rate electronic module for array-detector positron annihilation lifetime measurements. *Radiation Detection Technology and Methods*, 3(3):33, Apr 2019.

[6] Paul G Kwiat, Klaus Mattle, Harald Weinfurter, Anton Zeilinger, Alexander V Sergienko, and Yanhua Shih. New high-intensity source of polarization-entangled photon pairs. *Phys. Rev. Lett.*, 75(24):4337–4341, 1995.

[7] Michael V. Berry. The adiabatic phase and pancharatnam's phase for polarized light. *Journal of Modern Optics*, 34:1401, 1987.

[8] Ermes Toninelli, Bienvenu Ndagano, Adam Vallés, Bereneice Sephton, Isaac Nape, Antonio Ambrosio, Federico Capasso, Miles J Padgett, and Andrew Forbes. Concepts in quantum state tomography and classical implementation with intense light: a tutorial. *Advances in Optics and Photonics*, 11(1):67–134, 2019.

[9] Dirk P Kroese, Tim Brereton, Thomas Taimre, and Zdravko I Botev. Why the monte carlo method is so important today. *Wiley Interdisciplinary Reviews: Computational Statistics*, 6(6):386–392, 2014.

[10] Severino Collier Coutinho. *The mathematics of ciphers: number theory and RSA cryptography*. AK Peters/CRC Press, 1999.

[11] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991.

[12] Stefano Pironio, Antonio Acín, Serge Massar, A Boyer de La Giroday, Dzmitry N Matsukevich, Peter Maunz, Steven Olmschenk, David Hayes, Le Luo, T Andrew Manning, et al. Random numbers certified by bell's theorem. *Nature*, 464(7291):1021, 2010.

[13] Valerio Scarani. *Bell Nonlocality*. 2018.

[14] Bruce Schneier. *Applied cryptography: protocols, algorithms, and source code in C*. john wiley & sons, 2007.

[15] Davide G Marangon, Giuseppe Vallone, and Paolo Villoresi. Random bits, true and unbiased, from atmospheric turbulence. *Scientific reports*, 4:5490, 2014.

[16] Antonio Acín and Lluis Masanes. Certified randomness in quantum physics. *Nature*, 540(7632):213, 2016.

[17] Alain Aspect, Philippe Grangier, and Gérard Roger. Experimental realization of einstein-podolsky-rosen-bohm gedankenexperiment: a new violation of bell's inequalities. *Physical review letters*, 49(2):91, 1982.

[18] Mary A Rowe, David Kielpinski, Volker Meyer, Charles A Sackett, Wayne M Itano, Christopher Monroe, and David J Wineland. Experimental violation of a bell's inequality with efficient detection. *Nature*, 409(6822):791, 2001.

[19] Marissa Giustina, Alexandra Mech, Sven Ramelow, Bernhard Wittmann, Johannes Kofler, Jörn Beyer, Adriana Lita, Brice Calkins, Thomas Gerrits, Sae Woo Nam, et al. Bell violation using entangled photons without the fair-sampling assumption. *Nature*, 497(7448):227, 2013.

[20] Marissa Giustina, Marijn A M Versteegh, Soeren Wengerowsky, Johannes Handsteiner, Armin Hochrainer, Kevin Phelan, Fabian Steinlechner, Johannes Kofler, Jan-Ake Larsson, Carlos Abellán, Waldimar Amaya, Valerio Pruneri, Morgan W Mitchell, Jörn Beyer, Thomas Gerrits, Adriana E Lita, Lynden K Shalm, Sae Woo Nam, Thomas Scheidl, Rupert Ursin, Bernhard Wittmann, and Anton Zeilinger. Significant-loophole-free test of bell's theorem with entangled photons. *Phys. Rev. Lett.*, 115(25):250401, December 2015.

[21] Bas Hensen, Hannes Bernien, Anaïs E Dréau, Andreas Reiserer, Norbert Kalb, Machiel S Blok, Just Ruitenberg, Raymond FL Vermeulen, Raymond N Schouten, Carlos Abellán, et al. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682, 2015.

[22] Lynden K Shalm, Evan Meyer-Scott, Bradley G Christensen, Peter Bierhorst, Michael A Wayne, Martin J Stevens, Thomas Gerrits, Scott Glancy, Deny R Hamel, Michael S Allman, et al. Strong loophole-free test of local realism. *Physical review letters*, 115(25):250402, 2015.

[23] Adriana E Lita, Aaron J Miller, and Sae Woo Nam. Counting near-infrared single-photons with 95% efficiency. *Optics express*, 16(5):3032–3040, 2008.

[24] F Marsili, Varun B Verma, Jeffrey A Stern, S Harrington, Adriana E Lita, Thomas Gerrits, Igor Vayshenker, Burm Baek, Matthew D Shaw, Richard P Mirin, et al. Detecting single infrared photons with 93% system efficiency. *Nature Photonics*, 7(3):210, 2013.

[25] Philip M Pearle. Hidden-variable example based upon data rejection. *Physical Review D*, 2(8):1418, 1970.

[26] Anupam Garg and N David Mermin. Detector inefficiencies in the einstein-podolsky-rosen experiment. *Physical Review D*, 35(12):3831, 1987.

[27] Peter Bierhorst, Emanuel Knill, Scott Glancy, Yanbao Zhang, Alan Mink, Stephen Jordan, Andrea Rommal, Yi-Kai Liu, Bradley Christensen, Sae Woo Nam, et al. Experimentally generated randomness certified by the impossibility of superluminal signals. *Nature*, 556(7700):223, 2018.

[28] Adriana E Lita, Brice Calkins, L A Pellouchoud, Aaron Joseph Miller, and S Nam. Superconducting transition-edge sensors optimized for high-efficiency photon-number resolving detectors. *SPIE Defense, Security, and Sensing*, 7681:76810D–76810D–10, April 2010.

[29] Marco Fiorentino, Gaetan Messin, Christopher E Kuklewicz, Franco NC Wong, and Jeffrey H Shapiro. Ultrabright tunable photon-pair source with total-flux polarization-entanglement. In *Digest of Quantum Electronics and Laser Science Conference*, 2003.

[30] 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. *Phys. Rev. Lett.*, 121:150402, Oct 2018.

[31] D. L. Mills. Internet time synchronization: the network time protocol. *IEEE Transactions on Communications*, 39(10):1482–1493, Oct 1991.

[32] Ieee standard for a precision clock synchronization protocol for networked measurement and control systems. *IEC 61588:2009(E)*, pages C1–274, Feb 2009.

[33] P. Moreira, J. Serrano, T. Wlostowski, P. Loschmidt, and G. Gaderer. White rabbit: Sub-nanosecond timing distribution over ethernet. In *2009 International Symposium on Precision Clock Synchronization for Measurement, Control and Communication*, pages 1–5, Oct 2009.

[34] L. Narula and T. E. Humphreys. Requirements for secure clock synchronization. *IEEE Journal of Selected Topics in Signal Processing*, 12(4):749–762, Aug 2018.

[35] Tal Mizrahi. A game theoretic analysis of delay attacks against time synchronization protocols. In *2012 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication Proceedings*, pages 1–6. IEEE, 2012.

[36] Markus Ullmann and Matthias Vögeler. Delay attacks—implication on ntp and ptp time synchronization. In *2009 International Symposium on Precision Clock Synchronization for Measurement, Control and Communication*, pages 1–6. IEEE, 2009.

[37] Jeanette Tsang and Konstantin Beznosov. A security analysis of the precise time protocol (short paper). In *International Conference on Information and Communications Security*, pages 50–59. Springer, 2006.

[38] Dima Rabadi, Rui Tan, David KY Yau, and Sreejaya Viswanathan. Taming asymmetric network delays for clock synchronization using power grid voltage. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, pages 874–886. ACM, 2017.

[39] Feiyan Hou, Ruifang Dong, Tao Liu, and Shougang Zhang. Quantum-enhanced two-way time transfer. In *Quantum Information and Measurement (QIM) 2017*, page QF3A.4. Optical Society of America, 2017.

[40] Dong Yang. A simple proof of monogamy of entanglement. *Physics Letters A*, 360(2):249–250, 2006.

[41] William K Wootters and Wojciech H Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

[42] Antia Lamas-Linares and James E Troupe. Secure quantum clock synchronization. *Advances in Photonics of Quantum Computing, Memory, and Communication XI*, 10547:105470L, 2018.

[43] Alejandra Valencia, Giuliano Scarcelli, and Yanhua Shih. Distant clock synchronization using entangled photon pairs. *Applied Physics Letters*, 85:2655, 2004.

[44] Ivan Marcikic, Antía Lamas-Linares, and Christian Kurtsiefer. Free-space quantum key distribution with entangled photons. *Applied Physics Letters*, 89(10):101122, 2006.

[45] Caleb Ho, Antía Lamas-Linares, and Christian Kurtsiefer. Clock synchronization by remote detection of correlated photon pairs. *New Journal of Physics*, 11(4):045011, 2009.

[46] Runai Quan, Yiwei Zhai, Mengmeng Wang, Feiyan Hou, Shaofeng Wang, Xiao Xiang, Tao Liu, Shougang Zhang, and Ruifang Dong. Demonstration of quantum synchronization based on second-order quantum coherence of entangled photons. *Scientific reports*, 6:30453, 2016.

[47] Feiyan Hou, Ruifang Dong, Runai Quan, Xiao Xiang, Tao Liu, Xiaoyan Yang, Hao Li, Lixing You, Zhen Wang, and Shougang Zhang. Fiber-optic quantum two-way time transfer with frequency entangled pulses. *arXiv preprint arXiv:1812.10077*, 2018.

[48] Hou Feiyan, Dong Ruifang, Quan Runai, Xiang Xiao, Liu Tao, and Zhang Shougang. First demonstration of nonlocal two-way quantum clock synchronization on fiber link. In *CLEO Pacific Rim Conference 2018*, page Th4J.3. Optical Society of America, 2018.

[49] 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(10):101102, 2019.

[50] James E Troupe and Antia Lamas-Linares. Detecting optical channel non-reciprocity with non-local quantum geometric phase. *arXiv preprint arXiv:1808.09019*, 2018.

[51] Paul G. Kwiat and Raymond Y. Chiao. Observation of a nonclassical berry's phase for the photon. *Physical Review Letters*, 66:588, 1991.

[52] D. V. Strekalov and Y. H. Shih. Two-photon geometrical phase. *Physical Review A*, 56:3129, 1997.

[53] J. Brendel, W. Dultz, and W. Martinessen. Geometric phases in two-photon interference experiments. *Physical Review A*, 52:2551, 1995.

[54] Anand Kumar Jha, Mehul Malik, and Robert W. Boyd. Exploring energy-time entanglement using geometric phase. *Physical Review Letters*, 101:180405, 2009.

[55] J. Lee, L. Shen, A. Cerè, J. Troupe, A. Lamas-Linares, and C. Kurtsiefer. Asymmetric delay attack on an entanglement-based bidirectional clock synchronization protocol. *arXiv preprint arXiv:1907.09661*, 2019.

[56] John S Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1(3):195, 1964.

[57] Wolfgang Mauerer, Christopher Portmann, and Volkher B Scholz. A modular framework for randomness extraction based on trevisan's construction. *arXiv preprint arXiv:1212.0520*, 2012.

[58] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical review*, 47(10):777, 1935.

[59] Markus Ansmann, H Wang, Radoslaw C Bialczak, Max Hofheinz, Erik Lucero, M Neeley, AD O'Connell, D Sank, M Weides, J Wenner, et al. Violation of bell's inequality in josephson phase qubits. *Nature*, 461(7263):504, 2009.

[60] Gregor Weihs, Thomas Jennewein, Christoph Simon, Harald Weinfurter, and Anton Zeilinger. Violation of bell's inequality under strict einstein locality conditions. *Physical Review Letters*, 81(23):5039, 1998.

[61] JG Rarity and PR Tapster. Experimental violation of bell's inequality based on phase and momentum. *Physical Review Letters*, 64(21):2495, 1990.

[62] Wolfgang Tittel, Jürgen Brendel, Bernard Gisin, Thomas Herzog, Hugo Zbinden, and Nicolas Gisin. Experimental demonstration of quantum correlations over more than 10 km. *Physical Review A*, 57(5):3229, 1998.

[63] Johannes Handsteiner, Andrew S Friedman, Dominik Rauch, Jason Gallicchio, Bo Liu, Hannes Hosp, Johannes Kofler, David Bricher, Matthias Fink, Calvin Leung, et al. Cosmic bell test: measurement settings from milky way stars. *Physical review letters*, 118(6):060401, 2017.

[64] John F Clauser, Michael A Horne, Abner Shimony, and Richard A Holt. Proposed experiment to test local hidden-variable theories. *Physical review letters*, 23(15):880, 1969.

[65] Edward S Fry and Randall C Thompson. Experimental test of local hidden-variable theories. *Physical Review Letters*, 37(8):465, 1976.

[66] BG Christensen, KT McCusker, JB Altepeter, B Calkins, Thomas Gerrits, Adriana E Lita, A Miller, Lynden K Shalm, Y Zhang, SW Nam, et al. Detection-loophole-free test of quantum nonlocality, and applications. *Physical review letters*, 111(13):130406, 2013.

[67] Jan-Åke Larsson and Jason Semitecolos. Strict detector-efficiency bounds for n-site clauser-horne inequalities. *Physical Review A*, 63(2):022117, 2001.

[68] Augusto Garuccio. Hardy's approach, eberhard's inequality, and supplementary assumptions. *Physical Review A*, 52(4):2535, 1995.

[69] G Garbarino. Minimum detection efficiencies for a loophole-free observable-asymmetric bell-type test. *Physical Review A*, 81(3):032106, 2010.

[70] Rotem Arnon-Friedman, Frédéric Dupuis, Omar Fawzi, Renato Renner, and Thomas Vidick. Practical device-independent quantum cryptography via entropy accumulation. *Nature communications*, 9(1):459, 2018.

[71] Marco Tomamichel, Roger Colbeck, and Renato Renner. A fully quantum asymptotic equipartition property. *IEEE Transactions on information theory*, 55(12):5840–5847, 2009.

[72] Lluís Masanes, Renato Renner, Matthias Christandl, Andreas Winter, and Jonathan Barrett. Full security of quantum key distribution from no-signaling constraints. *IEEE Transactions on Information Theory*, 60(8):4973–4986, 2014.

[73] Mamoru Hoshi et al. Interval algorithm for random number generation. *IEEE Transactions on Information Theory*, 43(2):599–611, 1997.

[74] Xiongfeng Ma, Feihu Xu, He Xu, Xiaoqing Tan, Bing Qi, and Hoi-Kwong Lo. Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction. *Physical Review A*, 87(6):062327, 2013.

[75] Anindya De, Christopher Portmann, Thomas Vidick, and Renato Renner. Trevisan's extractor in the presence of quantum side information. *SIAM Journal on Computing*, 41(4):915–940, 2012.

[76] Lynden K Shalm, E Meyer-Scott, Bradley G Christensen, and Peter Bierhorst. Strong loophole-free test of local realism. *Phys. Rev.*, 115(25):250402, December 2015.

[77] Aaron J Miller, Adriana E Lita, Brice Calkins, Igor Vayshenker, Steven M Gruber, and Sae Woo Nam. Compact cryogenic self-aligning fiber-to-detector coupling with losses below one percent. *Optics express*, 19(10):9102–9110, 2011.

[78] K D Irwin. An application of electrothermal feedback for high resolution cryogenic particle detection. *Appl. Phys. Lett.*, 66(15):1998, 1995.

[79] Antia Lamas-Linares, Brice Calkins, Nathan A Tomlin, Thomas Gerrits, Adriana E Lita, Joern Beyer, Richard P Mirin, and Sae Woo Nam. Nanosecond-scale timing jitter in transition edge sensors at telecom and visible wavelengths. *arXiv preprint arXiv:1209.5721*, 2012.

[80] Kent D Irwin and Gene C Hilton. Transition-edge sensors. In *Cryogenic particle detection*, pages 63–150. Springer, 2005.

[81] Vitalij K Pecharsky and Karl A Gschneidner Jr. Magnetocaloric effect and magnetic refrigeration. *Journal of Magnetism and Magnetic Materials*, 200(1-3):44–56, 1999.

[82] D Drung, C Assmann, J Beyer, A Kirste, M Peters, F Ruede, and T Schurig. Highly sensitive and easy-to-use squid sensors. *IEEE Trans. Appl. Supercond.*, 17(2):699–704, 2007.

[83] Otto H Schmitt. A thermionic trigger. *Journal of Scientific Instruments*, 15(1):24, 1938.

[84] Aladar Czitrovszky and Alexander V Sergienko. Measurement of quantum efficiency of avalanche photodetectors based on quantum two-photon field. In *OPTIKA'98: 5th Congress on Modern Optics*, volume 3573, pages 332–335. International Society for Optics and Photonics, 1998.

[85] Alessandro Fedrizzi, Thomas Herbst, Andreas Poppe, Thomas Jennewein, and Anton Zeilinger. A wavelength-tunable fiber-coupled source of narrowband entangled photons. *Optics Express*, 15(23):15377–15386, 2007.

[86] Ryan S Bennink. Optimal collinear gaussian beams for spontaneous parametric down-conversion. *Phys. Rev. A*, 81(5):053805, May 2010.

[87] P. Ben Dixon, Danna Rosenberg, Veronika Stelmakh, Matthew E. Grein, Ryan S. Bennink, Eric A. Dauler, Andrew J. Kerman, Richard J. Molnar, and Franco N. C. Wong. Heralding efficiency and correlated-mode coupling of near-ir fiber-coupled photon pairs. *Phys. Rev. A*, 90:043804, Oct 2014.

[88] S M Hegde, K L Schepler, R D Peterson, and D E Zelmon. Room-temperature near ir fluorescence of high optical quality KTP. In Gary L Wood and Mark A Dubinskii, editors, *Defense and Security Symposium*, page 65520V. SPIE, May 2007.

[89] Alexandra Mech. *Experimental test of a Bell inequality with nonmaximally entangled states*. PhD thesis, uniwien, 2012.

[90] Andrew G White, Daniel FV James, Philippe H Eberhard, and Paul G Kwiat. Nonmaximally entangled states: Production, characterization, and utilization. *Physical review letters*, 83(16):3103, 1999.

[91] Yicheng Shi, Brenda Chng, and Christian Kurtsiefer. Random numbers from vacuum fluctuations. *Applied Physics Letters*, 109(4):041101, 2016.

[92] Dava Sobel. *Longitude: The True Story of a Lone Genius Who Solved the Greatest Scientific Problem of His Time*. Walker Publishing Company, 1995.

[93] Yang Liu, Xiao Yuan, Ming-Han Li, Weijun Zhang, Qi Zhao, Jiaqiang Zhong, Yuan Cao, Yu-Huai Li, Luo-Kan Chen, Hao Li, et al. High-speed device-independent quantum random number generation without a detection loophole. *Physical review letters*, 120(1):010503, 2018.

[94] Yang Liu, Qi Zhao, Ming-Han Li, Jian-Yu Guan, Yanbao Zhang, Bing Bai, Weijun Zhang, Wen-Zhao Liu, Cheng Wu, Xiao Yuan, et al. Device-independent quantum random-number generation. *Nature*, 562(7728):548, 2018.

[95] Zachary H Levine, Thomas Gerrits, Alan L Migdall, Daniel V Samarov, Brice Calkins, Adriana E Lita, and Sae Woo Nam. Algorithm for finding clusters with a known distribution and its application to photon-number resolution using a superconducting transition-edge sensor. *J. Opt. Soc. Am. B*, 29(8):2066–2073, August 2012.

[96] S. Marrone, E. Berthomieux, F. Becvar, D. Cano-Ott, N. Colonna, C. Domingo-Pardo, F. Gunsing, R. C. Haight, M. Heil, F. Käppeler, M. Krtička, P. Mastinu, A. Mengoni, P. M. Milazzo, J. O'Donnell, R. Plag, P. Schillebeeckx, G. Tagliente, J. L. Tain, R. Terlizzi, and J. L. Ullmann. Pulse shape analysis of signals from baf2 and cef3 scintillators for neutron capture experiments. *Nuclear Instruments and Methods in Physics Research, Section A: Accelerators, Spectrometers, Detectors and Associated Equipment*, 568(2):904–911, 2006.

[97] F. Belli, B. Esposito, D. Marocco, M. Riva, Y. Kaschuck, and G. Bonheure. A method for digital processing of pile-up events in organic scintillators. *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment*, 595(2):512 – 519, 2008.

[98] M. Vencelj, K. Bučar, R. Novak, and H. J. Wörtche. Event by event pile-up compensation in digital timestamped calorimetry. *Nuclear Instruments and Methods in Physics Research, Section A: Accelerators, Spectrometers, Detectors and Associated Equipment*, 607(3):581–586, 2009.

[99] G. Tambave, E. Guliyev, M. Kavatsyuk, F. Schreuder, and H. Löhner. Pulse pile-up recovery for the front-end electronics of the panda electromagnetic calorimeter. *IEEE Nuclear Science Symposium Conference Record*, pages 2163–2168, 2012.

[100] J W Fowler, B K Alpert, W B Doriese, D A Fischer, C Jaye, Y I Joe, G C O'Neil, D S Swetz, and J N Ullom. Microcalorimeter spectroscopy at high pulse rates: A multi-pulse fitting technique. *ApJS*, 219(2):35, August 2015.

[101] Lamas-Linares, Antía, Brice Calkins, Nathan A Tomlin, Thomas Gerrits, Adriana E Lita, Jörn Beyer, Richard P Mirin, and Sae Woo Nam. Nanosecond-scale timing jitter for single photon detection in transition edge sensors. *Appl. Phys. Lett.*, 102(23):231117, June 2013.

[102] O H Schmitt. A thermionic trigger. *J. Sci. Instrum.*, 15(1):24, 1938.

[103] Blas Cabrera, Roland Clarke, Aaron Miller, Sae Woo Nam, Roger Romani, Tarek Saab, and Betty Young. Cryogenic detectors based on superconducting transition-edge sensors for time-energy-resolved single-photon counters and for dark matter searches. *Physica B: Condensed Matter*, 280(1–4):509–514, 2000.

[104] Roy J. Glauber. The quantum theory of optical coherence. *Phys. Rev.*, 130:2529–2539, Jun 1963.

[105] Thomas Gerrits, Adriana E Lita, Brice Calkins, and Sae Woo Nam. Superconducting transition edge sensors for quantum optics. In *Superconducting Devices in Quantum Optics*, pages 31–60. Springer International Publishing, Cham, March 2016.

[106] Abraham Savitzky and MJE Golay. Smoothing and differentiation of data by simplified least squares procedures. 36:1627–1639, 07 1964.

[107] M. J. D. Powell. An efficient method for finding the minimum of a function of several variables without calculating derivatives. *The Computer Journal*, 7(2):155–162, feb 1964.

[108] Vassilis P. Plagianakos and Michael Vrahatis. *A derivative free minimization method for noisy functions*. 01 2002.

[109] Peter C Humphreys, Benjamin J Metcalf, Thomas Gerrits, Thomas Hiemstra, Adriana E Lita, Joshua Nunn, Sae Woo Nam, Animesh Datta, W Steven Kolthammer, and Ian A Walmsley. Tomography of photon-number resolving continuous-output detectors. *New Journal of Physics*, 17(10):103044, 2015.

[110] Jianwei Lee, Lijiong Shen, Alessandro Cerè, Thomas Gerrits, Adriana E Lita, 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(12):123108, 2018.

[111] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301–1350, Sep 2009.

[112] G. K. Wertheim, M. A. Butler, K. W. West, and D. N. E. Buchanan. Determination of the gaussian and lorentzian content of experimental line shapes. *Review of Scientific Instruments*, 45(11):1369–1371, 1974.

[113] Paul R. Rider. Variance of the median of small samples from several special populations. *Journal of the American Statistical Association*, 55(289):148–150, 1960.

[114] Guochang Xu and Yan Xu. *GPS*. Theory, Algorithms and Applications. Springer Berlin Heidelberg, Berlin, Heidelberg, 2016.

[115] Zhiheng Jiang, Y Huan, Victor Zhang, and P Dirk. Bipm 2017 twstft satre/sdr calibrations for utc and non-utc links. Technical report, BIPM Technical Memorandum, TM268 V2a, 2017.

[116] Joseph B Altepeter, Evan R Jeffrey, and Paul G Kwiat. Photonic state tomography. *Advances in Atomic, Molecular, and Optical Physics*, 52:105–159, 2005.

[117] Dirk Jalas, Alexander Yu Petrov, and Manfred Eich. Optical three-port circulators made with ring resonators. *Optics letters*, 39(6):1425–1428, 2014.

[118] Victor Dmitriev, Gianni Portela, and Daimam Zimmer. Possible mechanisms of switching in symmetrical two-ports based on 2d photonic crystals with magneto-optical resonators. *Optics letters*, 38(20):4040–4043, 2013.

[119] Victor Dmitriev, Marcelo N Kawakatsu, and Gianni Portela. Compact optical switch based on 2d photonic crystal and magneto-optical cavity. *Optics letters*, 38(7):1016–1018, 2013.

[120] Lei Bi, Juejun Hu, Peng Jiang, Dong Hun Kim, Gerald F Dionne, Lionel C Kimerling, and CA Ross. On-chip optical isolation in monolithically integrated non-reciprocal optical resonators. *Nature Photonics*, 5(12):758, 2011.

[121] Zongfu Yu and Shanhui Fan. Complete optical isolation created by indirect interband photonic transitions. *Nature photonics*, 3(2):91, 2009.

[122] Antia Lamas-Linares and James Troupe. Secure quantum clock synchronization. In *Advances in Photonics of Quantum Computing, Memory, and Communication XI*, volume 10547, page 105470L. International Society for Optics and Photonics, 2018.

[123] Jeeva Anandan. The geometric phase. *Nature*, 360(6402):307, 1992.

[124] J Zak. Geometric phase in magneto-optic faraday rotation. *Physics Letters A*, 154(9):471–474, 1991.