TÉCNICO LISBOA

INSTITUTO SUPERIOR TÉCNICO

Measurement-Device-Independent Quantum Key Distribution

RESUMO ALARGADO

Author:
Jorge MARQUES

Supervisors:
Prof. João Carvalho de Sá SEIXAS
Prof. Yasser Rashid Revez OMAR

Research work performed for the Master in Engineering Physics

at

Tittel Lab
QuTech, Delft University of Technology and
Departamento de Física, Instituto Superior Técnico

September 2019

Abstract

In this thesis, we propose integrating the classical telecommunication infrastructure with measurement-device-independent quantum key distribution, a novel protocol that grants immunity to detector side-channel attacks by relying on a Bell state measurement to post-select entangled states. To accomplish this, we built a measurement-device-independent quantum key distribution system based on time-bin qubit encoding that is suited for coexistence with a classical telecommunications channel. Since a Bell state measurement relies on the indistinguishability between incoming states, we then characterize the indistinguishability of the system in a Hong-Ou-Mandel interference experiment with reported visibilities of $> 43\%$ for a single temporal mode and $> 41\%$ for two temporal modes. These values approach the fundamental limit of 50% characteristic of coherent states, and are therefore good indicators of the performance of the system.

1 Introduction

The ability to exchange information privately is a fundamental necessity in modern society. In order to fulfill this necessity, cryptography was invented. Currently, we face a dilemma in the field of information security. On the one hand, we have asymmetric-key cryptography which relies on assumptions about the computational abilities of an eavesdropper that might no longer be valid in the future due to the threat of quantum computing [1]. On the other hand, the secure one-time-pad encryption protocol, a symmetric-key protocol, is not practical to use in telecommunications as it requires the constant generation of secret key between the two parties. First proposed in 1984 [2], Quantum Key Distribution (QKD) was invented to fill in the gap between the one-time-pad encryption and the key exchange problem. Quantum key distribution provides a theoretically provable-secure way of exchanging a random symmetric secret key between two parties in the presence of an eavesdropper, ensured by the laws of quantum mechanics. However, initial real-world implementations of QKD protocols did not follow some of the idealistic assumptions made in the initial proposals. Some unmodeled behavior of equipment have a significant impact on the security of the system. These open loopholes that can be exploited by an eavesdropper to break the security of protocols in what we call a side-channel attack. It turns out that single-photon detectors in particular are very vulnerable to attacks, with several exploits having been proposed and carried out on existing QKD systems [3, 4, 5, 6, 7, 8, 9]. First proposed in 2012 [10], measurement-device-independent quantum key distribution (MDI QKD) grants immunity to all conceivable detector vulnerabilities. It achieves this by moving all the measurement equipment to the (untrusted) quantum channel, such that the security of the protocol no longer relies on the measurement equipment.

1.1 Quantum key distribution

In general, a QKD protocol is divided into two distinct parts: quantum communication; and classical post-processing. During quantum communication, the two parties (usually referred to as Alice and Bob) exchange random information encoded into non-orthogonal quantum states of light which are transmitted via a quantum channel controlled by an eavesdropper (Eve). The eavesdropper is assumed to have no technological limitations and is only restricted by the laws of nature. Due to the no-cloning theorem [11, 12], Eve cannot access the information encoded in the quantum states without disturbing them and hence, any attempt of gaining information, will result in a detectable error on Alice and Bob's side. At the end of quantum communication, Alice, Bob and Eve will each share a random correlated string α, β and γ (also known as sifted-key). The procedure to carry out this task varies significantly according to which protocol one uses, and different protocols have different advantages or disadvantages both in terms of practical implementation and secret-key rates.

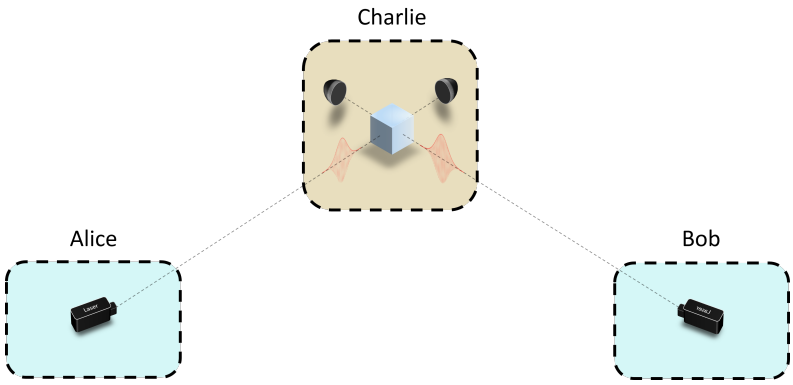

FIGURE 1: Communication scheme for measurement-device-independent quantum key distribution.

In the classical post-processing phase, Alice and Bob will extract a private key out of the previously obtained correlated strings and reduce Eve's information about the key to a negligible amount. To do this, Alice and Bob use a chunk of their partially correlated strings to estimate the number of errors between them, allowing them to characterize the transmissivity and noise of the quantum channel. The purpose of this is to estimate the maximum amount of information leaked to the eavesdropper. We call this step parameter estimation. Based on this information, they first detect and eliminate errors using error correction techniques, followed by a stage of privacy amplification that removes Eve's leaked information from the key. This is typically achieved by running the key through 2-universal hashing functions that compress the key, reducing the information obtained by an eavesdropper to almost zero. The outcome of classical post-processing is the secret key.

1.2 Measurement-device-independent quantum key distribution protocol

In MDI QKD, the quantum communication stage has both Alice and Bob preparing qubits and sending them (via two quantum channels) to a central measurement station (which we conveniently name Charlie). Here, Charlie -who can be an eavesdropper- performs a Bell state measurement with the incoming qubits, and announces the result to Alice and Bob. Here, Charlie's measurement result is used to post-select correlations between Alice and Bob's key. That is, based on the result of the BSM, Alice and Bob can do the process of key sifting similarly, as discussed in BB84. The detailed protocol follows four stages, which we will now describe.

State preparation and Bell state measurement

Alice and Bob start by preparing a random sequence of qubit states using the four states (Tab. 1) $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and send them to Charlie. For each pair of incoming qubits, Charlie performs a Bell state measurement and announces the result to Alice and Bob. The parties only keep track of qubits that yield a successful BSM at Charlie.

Bit value	Qubit basis	
	$\mathbb{Z}$	$\mathbb{X}$
0	$\|0\rangle$	$\|+\rangle$
1	$\|1\rangle$	$\|-\rangle$

TABLE 1: Qubit encoding scheme.

Key sifting

For each BSM reported by Charlie, Alice and Bob will make use of an authenticated classical channel to announce the basis used to encode the qubits. They discard all qubits for which their choice of basis did not match. After Alice and Bob have enough successful BSM's, they associate each qubit to a classical bit value (according to table 1). Following this step, one of the parties (say Bob) flips part of his bits according to table 2 in order to match Alice's bits. In the end, they will each obtain two bit strings, corresponding to bits sifted in the $\mathbb{Z}$ and $\mathbb{X}$ basis.

Basis	Bell state			
	Ψ^-	Ψ^+	Φ^-	Φ^+
$\mathbb{Z}$	Bit flip	Bit flip	-	-
$\mathbb{X}$	Bit flip	-	Bit flip	-

TABLE 2: Post-processing of data in the key sifting stage.

Parameter estimation

The parties assess the maximum amount of information leaked to a potential eavesdropper (which has to be removed from the key) using the secret-key rate formula. Since the error rate in the $\mathbb{X}$ basis is usually higher than in the $\mathbb{Z}$ basis, it is common to use the $\mathbb{X}$ to estimate the error rate and using the sifted key in the $\mathbb{Z}$ basis to distill the secret key. The secret-key rate is thus given in the asymptotic regime by:

$$R \geq Q^Z\Big(1 - H_2(E^X)\Big) - Q^Z f H_2(E^Z) \tag{1}$$

where Q^Z is the gain (probability of successful BSM event) in the $\mathbb{Z}$ basis, E_X the QBER (qubit error rate) in the $\mathbb{X}$ basis, f accounts for the efficiency of the error correction procedure ($f \geq 1$) and H_2 is the binary entropy.

Error correction and privacy amplification

Finally, Alice and Bob will distill a secret-key from the sifted key obtained in the $\mathbb{Z}$ basis. For this, they use error correction to detect and correct for errors in the sifted key and then remove the information leaked from the sifted key by using privacy amplification on the corrected key based on the secret-key rate calculated in the parameter estimation stage. In the end, Alice and Bob will share a symmetric, random, and -most importantly- private key.

1.3 Coexisting quantum key distribution

The cost of deploying dedicated fiber networks for quantum key distribution applications is a limitation for most applications. Therefore, having widespread adoption of quantum key distribution could be expedited by integrating QKD systems in the current network infrastructure. With this interest in mind, one could think of the possibility of quantum communication and classical telecommunication coexisting on the same fiber. That is, having classical data transmission coexisting with single-photon level signals at different wavelengths on the same fiber. However, this solution does not come without technical challenges. The most prominent of these is Raman scattering in the classical channels. Raman scattered light leaks out to other neighboring wavelengths in the spectrum potentially destroying the signal to noise ratio on the quantum channel. An obvious solution to this problem would be lowering the power on the classical data transmission channels, but since the goal here is to integrate QKD in the current infrastructure this is not an option. Then the only other solutions to minimize the impact of Raman noise by having the quantum channel far from the classical channels in the spectrum

and by minimizing the bandwidth of the quantum channel by using spectral filtering techniques. The coexistence of QKD and classical data transmission has been demonstrated from as far back as 1997 [13, 14, 15, 16, 17, 18]. In a recent study performed by our group [19], the coexistence of MDI QKD and five 10 Gbps classical channels in the telecom C-band was demonstrated. In this same study, the classical communication rate is projected to increase to 10 Tbps by moving the quantum channel to telecom O-band at the cost of having higher transmission loss.

2 Implementation

As one would expect for measurement-device-independent quantum key distribution, our system consists of two transmitters that make up the nodes of the QKD network (we call these Alice set-ups) and one central measurement station (which we refer to as Charlie set-up). Each set-up is built in a 19-inch rack cart for ease of transportation and implementation outside the lab. In the next subsections, we will discuss each of these set-ups individually in detail.

2.1 Alice set-up

The Alice system has two main functions, the generation of time-bin qubits and the tracking and storage of the sifted-key. It consists of three separate rack-mountable modules: pulse generation box, amplifier box, and optical box. Besides this, there is also auxiliary measurement and control equipment as well as dedicated power supplies. In the next subsections, we will go through each of these subsystems in detail as well as present some of the key technical challenges related to MDI QKD implementations. The optical box contains all the optical components and passive control electronics related to laser driving and frequency stabilization, and DC voltage biasing for the intensity modulators. It can be seen as the lowest level layer of the QKD system design stack. The optical set-up for qubit generation is displayed in Fig. 2. In our implementation, the quantum channel is powered by distributed

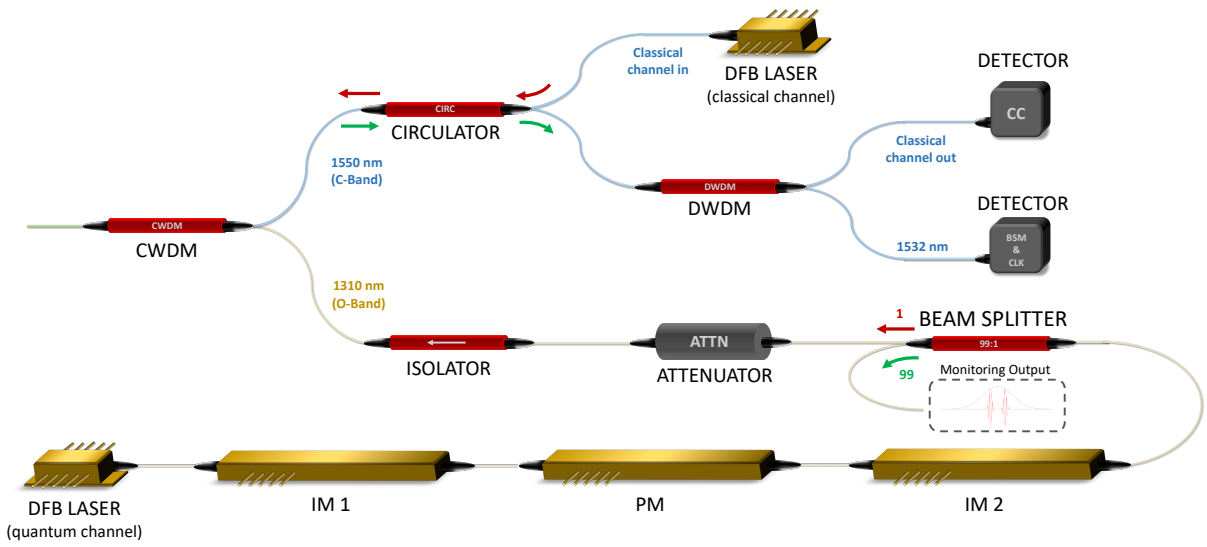

FIGURE 2: Alice optical set-up.

feedback (DFB) laser diode (at 1310 nm) that is mounted on a custom made laser-driver board that

pulses the laser below its threshold voltage in order to eliminate phase coherence between successive qubits. This is necessary to avoid a phase remapping attack [20]. The pulse is a square waveform with 200 MHz frequency and 80% duty cycle. This signal then goes through a sequence of an intensity and phase modulator (labeled as IM1 and PM respectively in Fig. 2) that carve and set the phase between early and late time-bins. The time-bins have a gaussian waveform with around 290 ps of FWHM and are separated by 800 ps from peak to peak. These are followed by a second intensity modulator (IM2) that adjusts the intensity of the signal for the implementation of the decoy-state method [21]. After this, we split the signal using a 99:1 ratio beam splitter and use the 99-arm for monitoring purposes. The remaining signal goes through a variable optical attenuator that brings the signal down to the single-photon level. Finally, there is an isolator that prevents the eavesdropper from back injecting light into the system and exploiting trojan-horse like attacks [3]. The quantum channel is combined with the classical channel using a coarse wavelength division multiplexer (CWDM) that combines the telecom O-band (1260-1360 nm) and C-band (1530-1565 nm). All classical communication takes place in the telecom C-band. A dense wavelength division multiplexer channel (DWDM ch36) is reserved for QKD related classical communication, namely the clock reference and BSM signal from Charlie. All other coexisting classical communication can make use of the remaining DWDM channels in the C-band. In the classical channel set-up, we first use a circulator to separate incoming signals from outgoing signals to Charlie. Incoming light from Charlie is split using a DWDM into the coexisting classical communication and the clock and BSM signal. The latter is encoded using a Manchester encoding technique which combines data and clock in the same signal allowing us to use a single channel for two different signals.

2.1.1 Alice system control

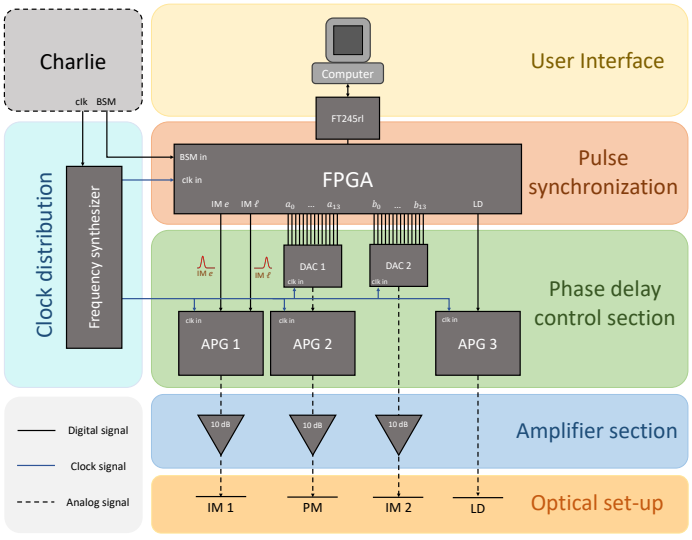

FIGURE 3: Alice system control stack. Field programmable gate array (FPGA); Digital-to-analog converter (DAC); Alice pulse generator board (APG).

The complete Alice system is designed as multi-layered control stack that starts at the lower level with the optical set-up and ends at the higher level user interface as seen in Fig. 3. Each of these layers provides control over a different aspect of the qubit generation procedure. In the user interface section, the user specifies the string of states they want to send to Charlie. This information is sent through a communication chip (FT245rl) to the FPGA. The logic programmed into the FPGA breaks down the qubit states into digital signals. The first two signals, IM e and IM ℓ are logic high if the respective time

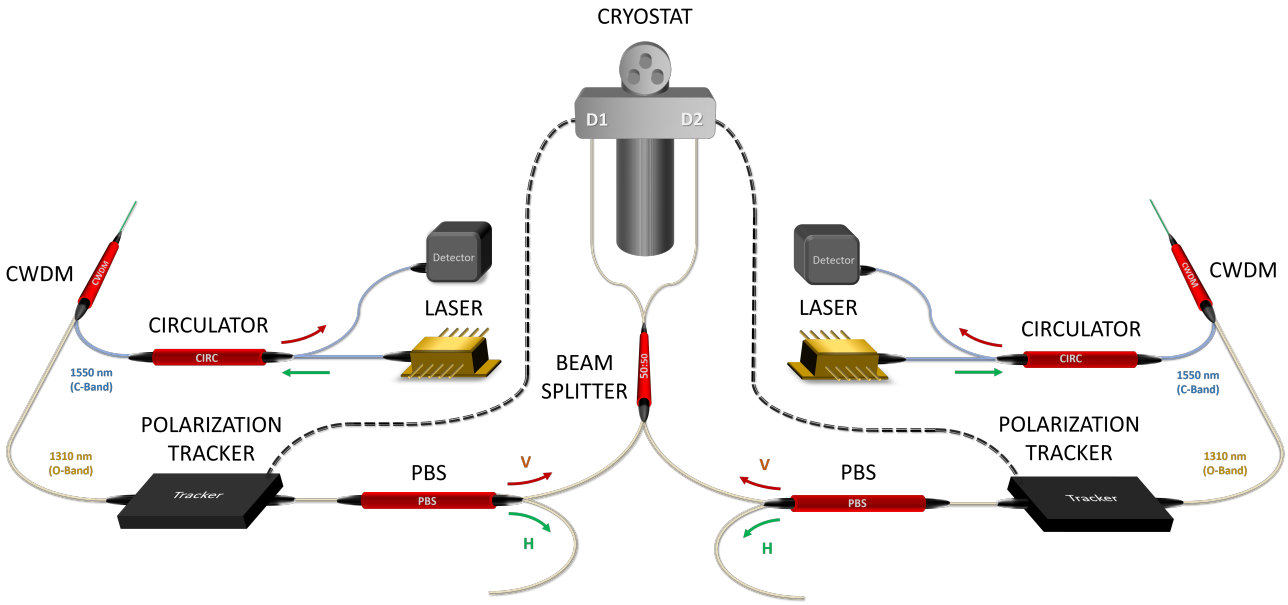

FIGURE 4: Charlie detection set-up. Polarization beam splitter (PBS); Coarse wavelength division multiplexer (CWDM).

bin is present in the qubit. Signals $\{b_0, ..., b_{13}\}$ are to be converted into analog voltage by a digital-to-analog converter (DAC 2, with 2^{14} voltage steps resolution) that will later drive the second intensity modulator (IM2). This allows for fine tuning of the mean number of photons per pulse necessary for realizing the decoy state method. Similarly, $\{a_0, ..., a_{13}\}$ will be used to drive the phase modulator. It may seem unnecessary to use an analog voltage to drive the phase modulator, since, in principle, the phase modulator only has to apply a π phase shift. However, experimentally, it is useful to have have some tunability over this voltage in order to make sure that were hitting the correct V_π voltage on the phase modulator. Finally, the LD signal provides a 200 MHz signal that will be fed to the laser driver. All these signals are synchronized by the FPGA every clock cycle. After this, we want to be able to control the phase of each signal within a clock cycle in order to carve the time bins accurately in the laser pulse. In order to accomplish this, we have designed the *Alice pulse generator board* (APG). This board takes one or more signal inputs and produces a new signal where one can set the phase of the rising and lowering edges within the 5 ns (200 MHz) clock cycle. The minimum rise and fall time achieved by the boards is 100-150 ps. Finally, the signals going to the optical modulators are amplified using high-bandwidth amplifiers. These are placed in their own box for cooling purposes. The system is synchronized using a frequency synthesizer board, that takes the signal incoming from Charlie and distributes across all other necessary components. The BSM signal from Charlie is stored in the FPGA and dumped into the computer so that it can be post-processed later.

2.2 Detection set-up

The Charlie optical set-up consists of a BSM for time-bin qubits plus a polarization control system, as demonstrated in Fig. 4. The input from Alice first goes through coarse wavelength division multiplexer (CWDM) that separates the quantum channel from the classical one. The classical communication subsystem consists of a circulator to route incoming and outgoing signals, a laser and a detector that send and receive classical signals from Alice respectively. In the quantum channel, we first find a polarization control feedback system. Light with vertical polarization generates a detection signal that is fed into the polarization tracker. The polarization tracker acts on the input light polarization in such a way that it maximizes that signal thus compensating for polarization drifts in the quantum channel. This is necessary in order to have polarization matching in the BSM. In the center, we

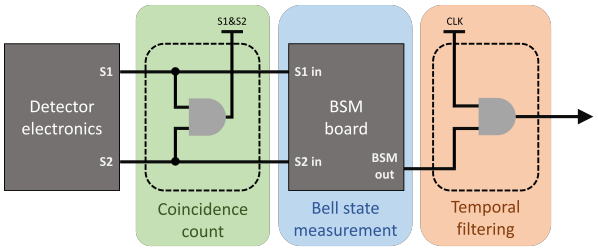

FIGURE 5: Detector signal processing at Charlie.

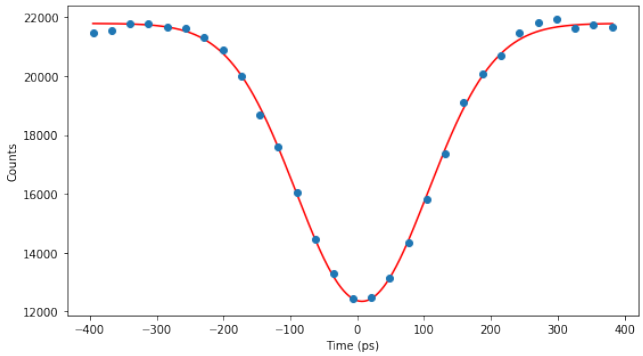

FIGURE 6: Hong-Ou-Mandel dip for a single temporal mode.

find the BSM set-up for time-bin qubits, which can be implemented with a 50:50 beam splitter and two single-photon detectors. The type of detectors used in this experiment were superconducting nanowire single-photon detectors (SNSPDs). These have to be cooled to cryogenic temperatures. For this purpose we used a commercial ID281 cryostat from *ID Quantique* that can go down to 800 mK. The SNSPDs were acquired from *Single quantum* and optimized for 1310 nm wavelength with 70% efficiency and a dark count rate of >10 Hz. In order to accurately trace a HOM dip and perform BSM, we need to turn the detection signals from the SNSPDs into coincidence and BSM counts. This is performed in three major steps, as depicted in Fig. 5. In the first step, we measure coincidences in the detectors by splitting the signal from each detector and perform a logic AND gate. This allows us to measure photon anti-bunching at Charlie in order to assess the indistinguishability of qubits incoming from Alice and Bob. In the next step, we feed the signal from the detectors to the BSM board, which contains the logic necessary for projecting the qubit states onto the $|\Psi^-\rangle$ state. This board outputs a BSM signal every time that logic is satisfied. Finally, we AND the output of the BSM board with the internal Charlie clock. This temporal filtering technique decreases the probability of erroneous BSM counts and thus decreases the overall qubit error rate (QBER).

3 Results

The main goal of this thesis was to build an MDI QKD system, and as such, the results obtained were intended as a means to assess the indistinguishability which will ultimately dictate the performance of the system. Photons are characterized by four principal degrees of freedom: polarization, frequency (spectrum), spatial mode, and temporal mode. In our system, we use standard single-mode telecom fiber (SMF-28) which ensures indistinguishability in the spatial mode degree of freedom. Polarization indistinguishability is ensured by using two polarization beam splitters at Charlie (with 20 dB extinction ratio) along with polarization maintaining (PM) fiber. The polarization beam splitter selects signals with the desired polarization, and the PM fiber keeps the polarization aligned along the

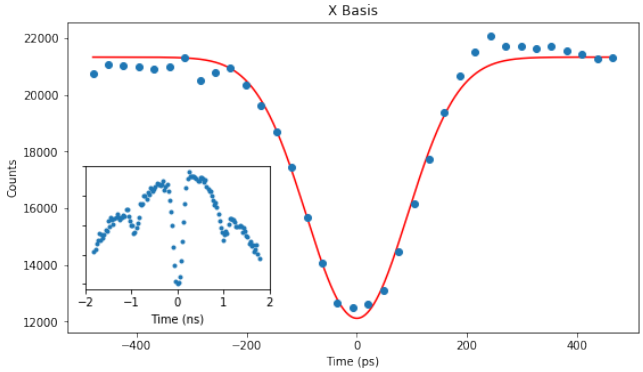

FIGURE 7: Hong-Ou-Mandel dip for the qubit state $|+\rangle$ (superposition of two temporal modes). The insected plot shows the same measurement data over a broader range of delay time.

desired fiber axis. In order to ensure indistinguishability in the frequency domain, the quantum channel laser of each Alice system has to be locked to the same frequency. This was achieved by using a temperature controller running on a PID control loop which resulted in 21 MHz frequency stability. Finally, the temporal modes were generated using a custom made pulse generation board which achieved pulse fidelities (between similar boards) of 99% and 94% for a single and two time-bins respectively. In order to assess the indistinguishability between the two Alice systems (crucial for MDI QKD), we performed Hong-Ou-Mandel interference with two different qubit states at Charlie. We do this by having each Alice system repeatedly sending the same qubit state to Charlie. Since the clock signal emitted from Charlie synchronizes each Alice system, one can trace a Hong-Ou-Mandel dip by varying the phase between the clock signals sent to "Alice 1" and "Alice 2" systems while measuring detector coincidences at Charlie. The first measurement was performed for both Alice systems sending a single temporal mode. The result is plotted in Fig. 6. We fitted the data with a Gaussian curve and then calculate the visibility where we take $Counts_{max}$ from the Gaussian fit and $Counts_{min}$ as the minimum measured value in the data. The measured visibility is 43%. This estimate was calculated without taking into account the detector noise level counts. We predict this value will get closer to the 50% limit once the detector noise level is subtracted from the data. In the second measurement, we did the same procedure now for the qubit state $|+\rangle$. The results are plotted in Fig. 7 a). The measured visibility for this state is 41.3%. This value is lower than the previous because, as we saw in the previous section, the signal fidelity for two temporal modes is lower than for a single temporal mode. It is interesting to look at the coincidence counts over a broader range of time delays for qubit state $|+\rangle$. Since this state is described by a superposition of two temporal modes, we now see three different dips in the coincidence counts. One main dip in the center and two other shallower side-dips. To understand this, consider the convolution of the two states arriving at Charlie. The overlap of an "early" temporal from one Alice system with a "late" temporal mode from the other Alice system results in photon-bunching, which gives rise to the side-dips. One can verify this by noticing that the side-dips are distanced from the main dip by around 1 ns which is the same as the temporal mode separation. Also, since only half of the qubit state is overlapping in these scenarios, the photon-bunching probability is half of that for total overlap. Because of this, the dept of the side-dips should be half of the main dip, which is what we see in Fig. 7.

References

[1] P. W. Shor. “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”. In: *SIAM J. Comput.* 26.5 (1997), pp. 1484–1509.

[2] C. Bennett and G. Brassard. "Quantum cryptography: Public key distribution and coin tossing". In: vol. 560. Jan. 1984, pp. 175–179.

[3] L. Lydersen et al. "Hacking commercial quantum cryptography systems by tailored bright illumination". In: *Nature Photonics* 4 (Oct. 2010), pp. 686–689.

[4] V. Makarov, A. Anisimov, and J. Skaar. "Effects of detector efficiency mismatch on security of quantum cryptosystems". In: *Phys. Rev. A* 74 (2 Aug. 2006), p. 022313.

[5] M. G. Tanner, V. Makarov, and R. H. Hadfield. "Optimised quantum hacking of superconducting nanowire single-photon detectors". In: *Opt. Express* 22.6 (Mar. 2014), pp. 6734–6748.

[6] Yi Zhao et al. "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems". In: *Phys. Rev. A* 78 (4 Oct. 2008), p. 042333.

[7] N. Jain et al. "Device Calibration Impacts Security of Quantum Key Distribution". In: *Phys. Rev. Lett.* 107 (11 Sept. 2011), p. 110501.

[8] H. Weier et al. "Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors". In: *New J. Phys.* 13 (July 2011).

[9] A. N. Bugge et al. "Laser Damage Helps the Eavesdropper in Quantum Cryptography". In: *Phys. Rev. Lett.* 112 (7 Feb. 2014), p. 070503.

[10] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. "Measurement-Device-Independent Quantum Key Distribution". In: *Phys. Rev. Lett.* 108 (13 Mar. 2012), p. 130503. DOI: 10.1103/PhysRevLett.108.130503.

[11] James L. Park. "The concept of transition in quantum mechanics". In: *Foundations of Physics* 1.1 (Mar. 1970), pp. 23–33.

[12] W K. Wootters and W H. Zurek. "A Single Quantum Cannot be Cloned". In: *Nature* 299 (Oct. 1982), p. 802.

[13] Paul D Townsend. "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing". In: *Electronics Letters* 33.3 (1997), pp. 188–190.

[14] Patrick Eraerds et al. "Quantum key distribution and 1 Gbps data encryption over a single fibre". In: *New Journal of Physics* 12.6 (2010), p. 063027.

[15] KA Patel et al. "Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks". In: *Applied Physics Letters* 104.5 (2014), p. 051123.

[16] Bernd Fröhlich et al. "Quantum secured gigabit optical access networks". In: *Scientific reports* 5 (2015), p. 18121.

[17] Liu-Jun Wang et al. "Long-distance copropagation of quantum key distribution and terabit classical optical data channels". In: *Physical Review A* 95.1 (2017), p. 012301.

[18] Tobias A Eriksson et al. "Coexistence of continuous variable quantum key distribution and 7× 12.5 Gbit/s classical channels". In: *2018 IEEE Photonics Society Summer Topical Meeting Series (SUM)*. IEEE. 2018, pp. 71–72.

[19] Raju Valivarthi et al. "Measurement-device-independent quantum key distribution coexisting with classical communication". In: *Quantum Science and Technology* 4.4 (2019), p. 045002.

[20] Chi-Hang Fred Fung et al. "Phase-remapping attack in practical quantum-key-distribution systems". In: *Phys. Rev. A* 75 (3 Mar. 2007), p. 032314.

[21] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. "Decoy State Quantum Key Distribution". In: *Phys. Rev. Lett.* 94 (23 June 2005), p. 230504.