12-2019

Implementation of Quantum Key Distribution Protocols

Eleftherios Moschandreou
University of Tennessee, emoschan@vols.utk.edu

To the Graduate Council:

I am submitting herewith a dissertation written by Eleftherios Moschandreou entitled "Implementation of Quantum Key Distribution Protocols." I have examined the final electronic copy of this dissertation for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy, with a major in Physics.

George Siopsis, Major Professor

We have read this dissertation and recommend its acceptance:

Stefan Spanier, Thomas Papenbrock

Accepted for the Council:

Dixie L. Thompson

Vice Provost and Dean of the Graduate School

(Original signatures are on file with official student records.)

Quantum key distribution over turbulent atmospheric channels

A Dissertation Presented for the

Doctor of Philosophy

Degree

The University of Tennessee, Knoxville

Eleftherios Moschandreou

December 2019

Abstract

As a wide spectrum of the human activity rapidly transitions to a digital environment, the need for secure and efficient communication intensifies. The currently used public key distribution cryptosystems, such as the Rivest-Shamir-Adleman (RSA) protocol, source their security from the computational difficulty of certain mathematical problems. While widely successful, the security these cryptosystems offer remains heuristic and the development of Quantum computers may render them obsolete. The security that Quantum Key Distribution (QKD) guarantees, stems not from the mathematical complexity of the encryption algorithms but from the laws of Quantum Physics. Implementations of QKD protocols, however, rely on imperfect instruments and devices for information encoding, transmission and detection. Device imperfections limit the rate of information exchange and introduce vulnerabilities which can be exploited by a potential eavesdropper. This work explores practical aspects of QKD as it matures beyond proof-of-principle experiments, focusing on the Measurement Device Independent - QKD, a novel Quantum Communication protocol that offers an exceptional balance between security and efficiency. At the heart of the MDI-QKD lies the Hong-Ou-Mandel (HOM) interference which characterizes the indistinguishability of the photon states that the communicating parties independently send. This study examines the HOM interference in a realistic lab environment and concludes that exceptional interference visibility can be achieved using typical commercially available optical devices and detectors, further demonstrating the applicability of the MDI-QKD protocol.

An important limiting factor for every Quantum Communication protocol is the transmission medium. Fiber - based optical networks suffer significant losses that prohibit Quantum Communication beyond metropolitan scales. While Free Space communication is an attractive alternative for long distance communication, is susceptible to losses due to the atmospheric Turbulence of the channel. As a means to improve the key generation efficiency, this work examines and experimentally demonstrates the Prefixed-Threshold Real Time Selection (P-RTS) scheme, which improves the free-space communication efficiency by rejecting detections that occur while the channel transmittance drops below a predetermined threshold.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Historical overview of Cryptography

Cryptography presents a rich, more than two millenia history [1] describing the methods of secret communication. A neck-and-neck race between codemakers and codebrakers, between cryptographs and cryptanalysts, gradually evolved Cryptography form art to science. The encryption method requires an algorithm, which is called the Cipher, to reversibly convert the communicated message, which is called the Plaintext, to a text that seems devoid of any meaning called Ciphertext. The encryption is performed following a set of instructions or keyword, simply called the Key and the legitimate receiver, who must also have knowledge of the key, can use it to decrypt, i.e. reverse the encryption and read the intended message. The goal of Cryptography is the ciphertext to be completely meaningless to someone intercepting it, without having knowledge of the encryption key.

Caesar's substitution cipher, was the first well known encryption method, where the alphabet is shifted down a fixed number of steps creating a substitution rule. For example if the the alphabet is shifted by three steps the rule becomes `a`→`D`, `b`→`E`, `c`→`F` etc. Caesar's cipher is very simple to break since at most 26 trials (for the English alphabet) can reveal the number of steps the alphabet was shifted, but is part of a greater category of substitution encryption algorithms called mono-alphabetic ciphers. For such a cipher, typically a key word or phrase is chosen where spaces and repeating letters are removed. For example for the key word `"THE ART OF CRYPTOGRAPHY"` the cipher alphabet begins as `"THEAROFCYPG"` and then followed by the remaining letters in the right order, as shown in the example of Table 1.1.

Mono-alphabetic ciphers, being simple and efficient, dominated the art of secret writing for the first millennium A.D. Their breaking is attributed to the ninth-century polymath Al-Kindi, by employing a statistical analysis on the characters of the ciphertext. The

Table 1.1: Example of a mono-alphabetic cipher for the key word `"THE ART OF CRYPTOGRAPHY"`.

Plain Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Cipher Alphabet	T	H	E	A	R	O	F	C	Y	P	G	I	J	K	L	M	N	Q	S	U	V	W	X	Y	Z	B

cryptanalysis relies on specific linguistic traits of each language. For example in English the letters `e,t,a` appear in exceptionally high frequencies, while the letters `j,q,z` in exceptionally low.

By the 16th century mono-alphabetic ciphers had proven unreliable and the need for secure communication led to the development of polyalphabetic encryption methods, called Vigenère ciphers. The construction of a Vigenère encryption table begins with a repeating keyword. Each letter of the keyword dictates which cipher-alphabet would be used for the encryption of a plain-text letter. Although the Vigenère cipher remained unbreakable for more than four centuries, it contained a vulnerability: the repetition of the keyword introduced repeating patterns in the ciphertext. Charles Babbage and Friedrich Kasiski, in the 19th century were the first to recognize these patterns and cryptanalyze (Kasiski's test) the Vigenère cipher.

At the turn of the 20st century, the development of the radio telegram by Guglielmo Marconi and the outbreak of WWI intensified the search for more secure ciphers, for example the Playfair and the ADFGVX, but each time slight repetitions and patterns would give the nooks and crannies the cryptanalysts needed to latch on. Towards WWII encryption employed complex electro-mechanical devices. In response cryptanalysts build complex machines like the "Bomba" by Marian Rejewski, the "Bombe" project led by Alan Turing and Gordon Welchman and the "Colossus" project led by Tommy Flowers, which had tremendous impact in the outcome of the war and became the blueprint for the development of the modern computers. In the years post the war, computers became cheaper and more powerful and were employed in the development of more complex encryption block ciphers such as the DES (Data Encryption Standard), the GOST and since 2000, the AES (Advanced Encryption Standard)[2].

Table 1.2: Example of the Vigènere cipher. The plaintext `"the unbreakable cipher"` is encrypted with the key word `"vigenere"`. The keyword letters and their corresponding cipher-alphabets are highlighted in the Vigère table below.

Key	v	i	g	e	n	e	r	e	v	i	g	e	n	e	r	e	v	i	g	e
Plaintext	t	h	e	u	n	b	r	e	a	k	a	b	l	e	c	i	p	h	e	r
Ciphertext	O	P	K	Y	A	F	I	I	V	S	G	F	Y	I	T	M	K	P	K	V

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

1.2 Modern block ciphers

The core algorithm of a block cipher, first divides the plaintext data into fixed size blocks, (128bits per block for the AES). Each block undergoes multiple rounds of a sequence of "scrambling"operations, called Substitution-Permuation Networks (SPN). In particular for the AES, which currently is the most commonly used standard, each 128 bit block is organized in a 4×4 byte array. Then multiple rounds of the following SPN are applied, as described in Figure 1.1. The SPN is summarized as follows.

1. The internal state is XORed with a round key, different for each round.
2. (Substitution part): Each byte $\{s_0, \ldots, s_{15}\}$ is substituted with an other byte according to a preconstructed lookup table. To ensure strong encryption this lookup table should be highly non-linear and without any statistical bias.
3. (Permutation part). Row shifting: The ith row is shifted i positions, $i \in \{0, \ldots, 3\}$.
4. (Permutation part). Column Mixing: A linear transformation is applied to all the elements of each column.

Although the core algorithm of a block cipher provides very strong encryption, an improper mode of operation may compromise the communication security. A safe mode of operation is the Cipher Block Chaining, where the encryption of each block depends on the ciphertext of its previous block.

By the 1970s, encryption ciphers had become strong enough to provide secure communication, but the key distribution still relied on primitive methods such as trusted couriers. At that point, the attention shifted towards novel reliable key distribution methods.

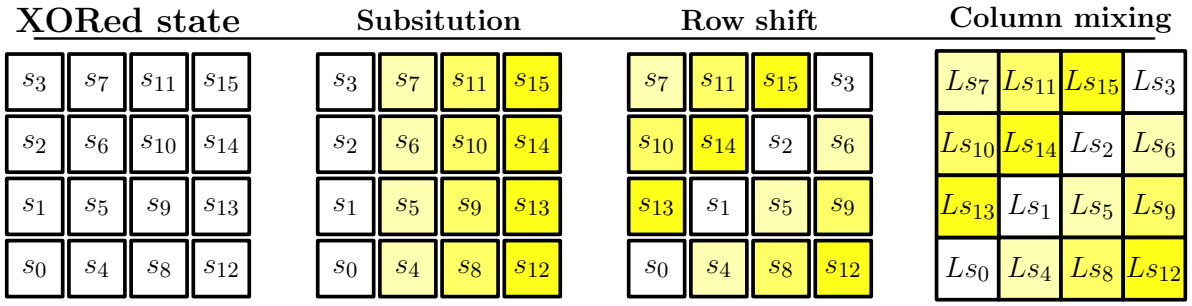

Figure 1.1: AES, principle of operation. (a) The initial 4×4 byte state is XORed with the round key. (b) Each byte is substituted according to the cipher's lookup table (c) Each row of the block is shifted (d) a linear transformation is applied to the members of each column (shown with the same shade)

1.3 Public key distribution

1.3.1 Diffie-Hellman-Merkle symmetric public key distribution

Based on the ideas of Ralph Merkle [3], Whitfield Diffie and Martin Hellman proposed a protocol where the communicating parties named Alice and Bob from now on, establish securely a shared key via a public channel [4]. The Diffie-Hellman-Merkle protocol is outlined as follows:

1. Alice and Bob choose publicly a suitable prime number p and an integer g where g is a primitive root modulo p.

2. Alice chooses an integer a and Bob chooses an integer b. Numbers a and b belong in the multiplicative group of integers modulo p, Z_p^*. Both keep their numbers secret.

3. Alice sends publicly the number $A = g^a \mathrm{mod} p$. Likewise, Bob sends publicly the number $B = g^a \mathrm{mod} p$. Noting that numbers A and B are simple to calculate no matter the size of the prime number p.

4. Having received B, Alice can calculate $K_a = B^a \mathrm{mod} p = \left(g^b \bmod p\right)^a \mathrm{mod} p$. Similarly Bob calculates $K_b = A^b \bmod p = \left(g^a \bmod p\right)^b \bmod p$.

5. It is $K = K_a = K_b$ since $\left(g^b \bmod p\right)^a \mathrm{mod} p = \left(g^a \bmod p\right)^b \bmod p$, therefore Alice and Bob share now a common secret number K.

6. An eavesdropper to calculate K , needs either a or b, but to find them needs to solve $A = g^a \mathrm{mod} p$ or $B = g^a \mathrm{mod} p$ given A, B, g, p. This is the discrete logarithm problem which is computationally difficult to solve. To increase the randomness of their common secret and thus the communication security the two parties use the hash of the number K they share.

The DHM protocol needs separate authentication of the legitimate participants, otherwise it is vulnerable to man-the-middle attacks. The DHM presents also some practical inefficiencies. To eliminate the possibility of smaller subgroups within Z_p^* [5] the prime number p should be chosen such as $\frac{p-1}{2}$ is also prime and so the generation of suitable public numbers does not scale efficiently, especially in cases were an entity needs to communicate securely with multiple parties. In [4] is also introduced the idea of asymmetric key distribution where the encryption key is different from the key used in decryption.

1.3.2 RSA asymmetric public key distribution

The first implementation of asymmetric key distribution was developed by Ron Rivest, Adi Shamir, and Leonard Adleman (RSA)[6]. The method utilizies numbers from the group Z_n^* of all numbers co-prime with n and with $\varphi(n)$ is the Euler's totient function, giving the order of the group i.e. the number of elements in Z_n^* as

$$\varphi(n) = (p_1 - 1) \times (p_2 - 1) \times \ldots \times (p_m - 1)$$

The protocol employs a mathematical object called trapdoor permutation where encrypting the plain number P to the cipher number C is easy using the public key, but extremely difficult to calculate P from C without knowledge of the private key (trapdoor). The method begins from the observation that for every integer number k, which is the message, we can find efficiently three large numbers (n, e, d) that satisfy

$$k = (k^e \bmod n)^d \bmod n \tag{1.1}$$

The numbers (e, n) consist the public key. The trapdoor number d is chosen as to satisfy $ed = 1 \mod \varphi(n)$, therefore the exponent e must be less than $\varphi(n)$. This trapdoor must be kept secret, in possession of Alice and can be calculated only if the factorization of $n = p \times q$ or equivalently the function $\varphi(n)$ is known. They key exchange proceeds as follows.

1. Bob encrypts his message k to a ciphertext c as $c = k^e \bmod n$.
2. Alice receives the message and deciphers it as $k = c^d \bmod n$

The security of the RSA stems from the difficulty of both the Discrete Logarithm Problem (DLP) and the integer factorization problem, since an eavesdropper in order to intercept the message k needs to either solve $c = k^e \mod n$ (DLP) or calculate the factorization $n = p \times q$ which is directly related to the secret exponent d. For sufficiently large numbers n , at least 2048 *bits* for modern encryption schemes, it is practically impossible to determine the factorization $n = p \times q$. The security of the RSA is heuristic in the sense that it has not been possible yet to solve the factorization problem or the discrete logarithm problem. A plethora of attacks on RSA exist that exploit either side channel timing attacks or faults in the implementation [7, 8, 9].

1.3.3 Elliptic curve Cryptography.

Introduced in 1985 Elliptic Curve Cryptography [10, 11] offered a more powerful and efficient public key distribution protocol. ECC utilizes pairs of natural numbers from the field Z_p

where p is a prime number that satisfy the Elliptic Curve equation.

$$y^2 = x^3 + a \cdot x + b \tag{1.2}$$

The security of the ECC protocol stems from the difficulty of the Elliptic Curve Discrete Logarithm problem: find the number k given a base point Q and a public point P where $P = kQ$. The Key agreement is similar to the Diffie-Hellmann method:

1. For a public point Q, Alice selects a random secret number and computes $P_A = d_A Q$. She sends P_A to Bob.

2. Bob selects a random secret number and computes $P_B = d_B Q$. He sends P_B to Bob.

3. Both share the secret $d_A P_B = d_B P_A = d_A d_B Q$

The security of ECC strongly depends on the choice of the coefficients a and b.

1.4 The one time pad

There is one cipher that is provably secure, immune to any brute force attacks, the One-Time-Pad (OTP) [12]. The security of the OTP is perfect in the sense that an adversary in possession of the ciphertext C cannot gain any information about the plaintext P i.e. $H(P) = H(P|C)$. If the plaintext , ciphertext and key are represented in binary than the OTP encryption is implemented as a bitwise XOR operation, $C = P \oplus K$ and decryption $C \oplus K = P \oplus K \oplus K = P$. To achieve perfect secrecy the OTP Key has to meet certain requirements. (i) The key has to be at least the same size as the message. If the message has length m and the key is shorter with length k where $k < m$, then part of it has to be reused and an attacker can rule out all 2^{m-k} plain-texts. (ii) The key has to be truly random and (iii) it has to be used only once. If the same a key is reused an adversary in possession of the cipher-texts can gain partial information. For example if the key K is used for both plain-texts P_1 and P_2 to encrypt $C_1 = P_1 \oplus K$ and $C_2 = P_2 \oplus K$, an eavesdropper can know $C_1 \oplus C_2 = P_1 \oplus K \oplus P_2 \oplus K = P_1 \oplus P_2$. The OTP is also known as the Vernar cipher.

1.5 Quantum key distribution.

The security of the RSA and DHM protocols relies on the mathematical difficulty of the integer factorization and discrete logarithms problems. Shor's quantum algorithm [13] can solve these problems, thus the development of quantum computers may render

classical Cryptography protocols obsolete. Within the framework of Quantum physics it is impossible for an Eavesdropper to distinguish non-orthogonal quantum states by any means of measurement due to the uncertainty principle. Equally impossible is any attempt to perform any kind of local measurement on an entangled state shared by the legitimate communicating parties, without disturbing their non-local correlations. These properties are uniquely quantum with no classical analogue can provide in principle provable unconditional communication security, unlike the heuristic security provided by the classical key distribution protocols.

1.5.1 The BB84 protocol

The first protocol utilizing the properties of quantum physics for secure communication was proposed by Charles Bennett and Gilles Brassard in 1984 (BB84)[14]. A common implementation requires the information to be encoded on the polarization states of light pulses. We can assume for example that the bit 0 is encoded as $|\rightarrow\rangle$ in the $+$ basis and $|\nearrow\rangle$ in the $\times$ basis and likewise the bit 1 is encoded as $|\uparrow\rangle$ in the $+$ basis and $|\nwarrow\rangle$ in the $\times$ basis, the protocol would proceed as follows.

1. Alice randomly selects the bits to prepare. If they intend to create a key of length n, then at least $(4+\delta)\,n$ bit should be prepared.

2. Alice randomly selects the basis on which she encodes her bits and sends the appropriate state one by one, over an authenticated public channel. Table 1.3.

3. Bob receives the pulses that have traveled through the quantum channel and randomly chooses the basis to perform his measurement.

4. Alice and Bob communicate over an authenticated public channel and compare the basis choice for each bit. They keep only the events where they used the same base, which are $2n$ with high probability.

5. They publicly reveal and compare n bits to determine the Quantum Bit Error Rate their strings exhibit and if it is above an acceptable threshold they abort the protocol. Otherwise they proceed to correct any errors between their shared keys by applying a classical error reconciliation scheme [15].

6. At this point Alice and Bob share with high probability identical key strings, but Eve may have some partial information on them either because she was eavesdropping or because of the information publicized during the reconciliation process. Alice and

Table 1.3: Principle of the BB84 protocol.

12 random bits sent by Alice

	1	2	3	4	5	6	7	8	9	10	11	12
Random Bit	0	1	1	0	1	1	1	0	1	0	1	0
Random basis	+	+	×	+	+	+	×	+	×	+	×	+
Alice sends	→	↑	↖	→	↑	↑	↖	→	↖	→	↖	→

Bob receives the qubits

	1	2	3	4	5	6	7	8	9	10	11	12
Random basis	×	+	×	×	+	×	+	+	×	×	×	+
Bob observes	↗	↑	↖	↖	↑	↗	↑	→	↖	↗	↖	→
public discussion		↑	↖		↑			→	↖		↖	→
raw key		1	1		1			0	1		1	0

Bob can perform privacy amplification [16] to bound any possible information an Eavesdropper may have on their shared key.

1.5.2 Entanglement as a source of information

Entanglement describes the joint state of two or more qubits which is not separable. This means the joint state of qubits A and B is entangled if and only if

$$|\psi\rangle \neq |\psi_A\rangle \otimes |\psi_B\rangle \tag{1.3}$$

Entangled states allow non-local correlations [17] which are purely a quantum property and cannot be classically replicated offering a fundamental new way for two parties to share information. For example if Alice and Bob share a Bell state of eq.(1.4) and eq.(1.5) with each possessing a qubit, then if Alice performs a measurement on her qubit, she instantly gains knowledge on Bob's bit value.

$$\left|\Psi^+\right\rangle = \frac{1}{\sqrt{2}}\left(|0_A 1_B\rangle + |1_A 0_B\rangle\right) \qquad \left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}}\left(|0_A 1_B\rangle - |1_A 0_B\rangle\right) \tag{1.4}$$

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}\left(|0_A 0_B\rangle + |1_A 1_B\rangle\right) \qquad \left|\Phi^-\right\rangle = \frac{1}{\sqrt{2}}\left(|0_A 0_B\rangle - |1_A 1_B\rangle\right) \tag{1.5}$$

The unique quantum nature of the correlations offered by entangled states are manifested through the violation of Bell inequalities [18] and their modern way to present them the

Clauser, Horne, Shimony, Holt (CHSH) games [19], Figure 1.2. First, looking the two particle distribution from a classical point of view, assume that a middleman delivers Alice and Bob each a classical particle. Alice chooses randomly to measure either the quantity Q or R with outcomes ± 1 (reflecting on the eigenvalues of $\hat{Z}$ on the $\{|0\rangle, |1\rangle\}$ basis and of $\hat{X}$ on the $\{|+\rangle, |-\rangle\}$ basis). Similarly Bob chooses randomly to measure either the quantity S or T with outcomes ± 1. Alice and Bob examine the correlator $QR + RS + RT - QT$. In the classical point of view the operators Q, R, S, T merely reveal the already existing state values q, r, s, t. Then the average value is

$$\begin{aligned} E(QS) + E(RS) + E(RT) - E(QT) &= E(QS + RS + RT - QT) \\ &= \sum_{q,r,s,t} p(q,r,s,t) \cdot (qr + rs + rt - qt) \end{aligned} \tag{1.6}$$

which leads to the Bell inequalities

$$-2 \leq E(QS) + E(RS) + E(RT) - E(QT) \leq 2 \tag{1.7}$$

If we re-examine now the same problem from the Quantum point of view, the source in the middle now provides Bell state qubits Alice and Bob. Alice randomly measures the observable $\hat{Q} = \hat{Z}_a$,i.e. the $\{0°, 90°\}$ basis, or the observable $\hat{R} = \hat{X}_a$,i.e. the $\{45°, 135°\}$ basis. Similarly Bob randomly measures the observable $\hat{S} = \frac{-1}{\sqrt{2}}\left(\hat{Z}_b + \hat{X}_b\right)$,i.e. the $\{67.5°, 157.5°\}$ basis, or the observable $\hat{T} = \frac{1}{\sqrt{2}}\left(\hat{Z}_b - \hat{X}_b\right)$,i.e. the $\{22.5°, 112.5°\}$ basis as shown in Figure 1.2.

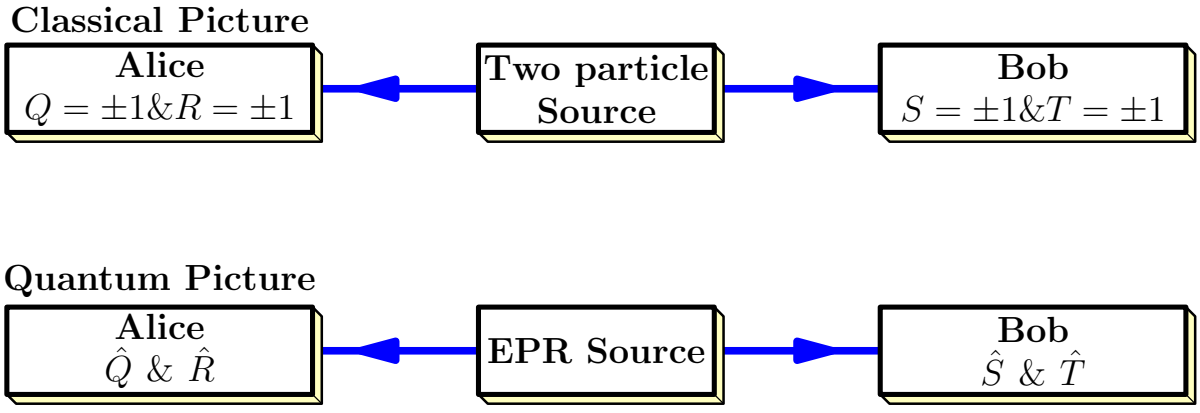

Figure 1.2: CHSH inequalities from the Classical and Quantum point of view.

Given the Bell state $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, the form of the operators $\hat{Q}, \hat{R}, \hat{S}, \hat{T}$, with $\langle\cdot\rangle = \langle\psi| \cdot |\psi\rangle$, and the action of the Pauli operators,

$$\begin{aligned} \hat{X}|0\rangle &= |1\rangle \qquad \hat{X}|1\rangle = |0\rangle \\ \hat{Z}|0\rangle &= |0\rangle \qquad \hat{X}|1\rangle = -|1\rangle \end{aligned} \tag{1.8}$$

it is easy to check that

$$\left\langle \hat{Q}\hat{S} \right\rangle + \left\langle \hat{R}\hat{S} \right\rangle + \left\langle \hat{R}\hat{T} \right\rangle - \left\langle \hat{Q}\hat{T} \right\rangle = 2\sqrt{2} \tag{1.9}$$

The correlator of eq.(1.9) clearly violates the classical inequality of eq.(1.7). In fact as the Tsirelson's inequality shows, the violation of eq.(1.9) is the maximum possible. By performing the CHSH test, i.e. by measuring the correlator of eq.(1.9), two communicating parties can determine whether they share qubits of an entangled state. What allows entangled states to be used as source for secure information is the property of entanglement monogamy [20, 17], if the two parties establish that they share a maximally entangled state $|\psi\rangle_{AB}$, then the state $|\psi\rangle_E$ an eavesdropper holds would be completely uncorrelated,

$$|\psi\rangle_{ABE} = |\psi\rangle_{AB} \otimes |\psi\rangle_E \tag{1.10}$$

Moreover the entanglement monogamy can be quantified. If the two parties discover they share a partially entangle state , they can bound the degree of correlation an eavesdropper may have, through means of the Coffman, Kundu, Wootters inequality [21, 22].

1.5.3 EPR - Ekert91 protocol

In the BB84 protocol, the key bits originate from states prepared by Alice. By using maximally entangled states Alice and Bob can generate a shared, secure key in the scheme known as Ekert91 [23, 24]. Assume that a Charlie prepares the maximally entangled two qubit state

$$\left|\Psi^+\right\rangle_{AB} = \frac{1}{\sqrt{2}}(|HV\rangle_{AB} + |VH\rangle_{AB}) \tag{1.11}$$

Alice measures the polarization with the basis being randomly chosen between the $\{0°, 90°\}$ or the $\{45°, 135°\}$ basis. Likewise, Bob measures the polarization in the $\{0°, 90°\}$, $\{22.5°, 112.5°\}$ or the $\{67.5°, 157.5°\}$ basis. In post-processing they publicly discuss their basis choice. When the both use the rectilinear $\{0°, 90°\}$ basis they use the bits to construct the shared key. When they both record an event, but used different basis, they perform the CHSH game, to check whether the Bell inequality is violated. The monogamous nature of

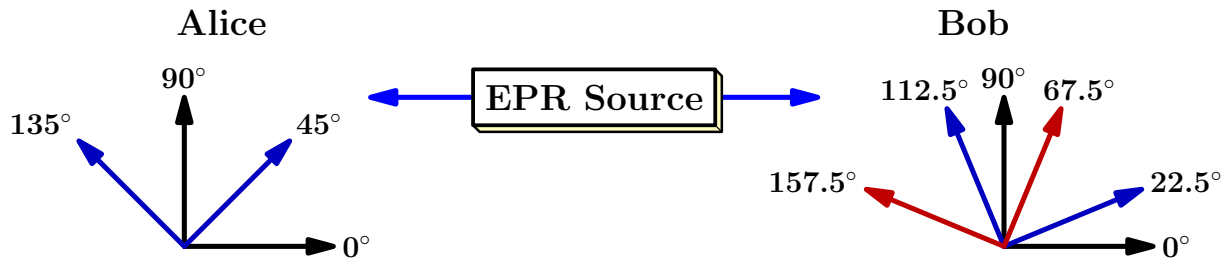

Figure 1.3: Ekert91 protocol. When Alice and Bob, both use the rectilinear basis they convert their measurements to the secret key.

entanglement guarantees that an eavesdropper, even if is the one that creates the EPR pair, can not gain any information without being detected.

1.5.4 BBM92 protocol

In a simplified version if Ekert's protocol, Bennett, Brassard and Mermin [25] consider the source to still produce EPR pairs but the need to perform a Bell inequality test is removed. Alice and Bob receive their qubits and each measure in either the rectilinear or diagonal basis, randomly chosen. In post-processing they publicly compare their basis choice and keep events when only both successfully detected using the same basis. The security is guaranteed because even if the Eavesdropper controls the production and distribution of the EPR pairs, she cannot create a state that is correlated to the state Alice and Bob receive, without disturbing the statistics that Alice and Bob expect, as discussed in 1.5.6. The protocol implicitly assumes that Alice's and Bob's detection systems can perform measurements flawlessly.

1.5.5 Time-reversed EPR protocol

In Ekert91 and BBM protocols, someone in the middle, who may even be untrusted, prepares maximally entangled EPR states and sends Alice and Bob each, one qubit. Performing the reverse procedure still enables two parties to generate a secure key as described in the time-reversed EPR protocol [26]. Alice and Bob each prepare independently a random BB84 state: Horizontal, Vertical, Diagonal, Anti-diagonal ($|H\rangle, |V\rangle, |D\rangle, |A\rangle$). Each sends his/her state to a middleman Charlie who perform a Bell state discrimination measurement, Figure 1.4. When Charlie announces a successful Bell state projection, Alice and Bob publicly compare the basis they used, and if it is the same, they know how their bits are correlated while Charlie cannot know the exact bit value. If the middleman is being dishonest, announcing

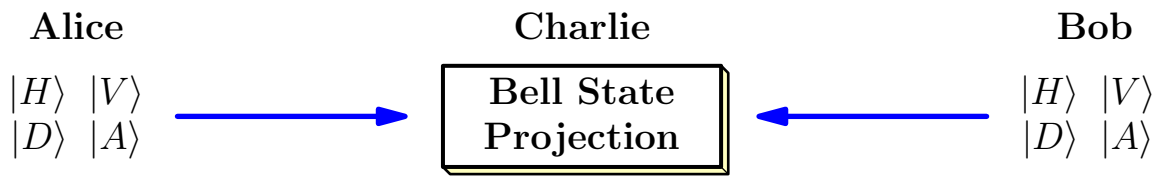

Figure 1.4: Time-Reversed EPR protocol.

false Bell state projections, Alice and Bob can identify this during their public discussion. The security of the time-reversed protocol is proven in [27].

1.5.6 BB84 , EPR and time-reversed EPR are equivalent

The three protocols, BB84, EPR and time-reversed EPR are in fact equivalent, the security of one scheme implies the security of the others. For example we can assume that Alice and Charlie are given the EPR pair $|\Psi\rangle_{AC_1} = \frac{1}{\sqrt{2}}(|HV\rangle + |VH\rangle)$ and Bob and Charlie are given the pair $|\Psi\rangle_{BC_2} = \frac{1}{\sqrt{2}}(|HV\rangle + |VH\rangle)$. If Charlie is trying to intercept the communication between Alice and Bob he will first attach an ancilla state A_{init}, and the combined state can be written,

$$|\Psi\rangle_{ABC} = \frac{1}{\sqrt{2}}(|HV\rangle_{AC} + |VH\rangle_{AC}) \otimes \frac{1}{\sqrt{2}}(|HV\rangle_{BC} + |VH\rangle_{BC}) \otimes A_{init} \tag{1.12}$$

$$= \frac{1}{2}\big(|HH\rangle_{AB} \otimes |VV\rangle_C + |HV\rangle_{AB} \otimes |VH\rangle_C + |VH\rangle_{AB} \otimes |HV\rangle_C + |VV\rangle_{AB} \otimes |HH\rangle_C\big) \otimes A_{init} \tag{1.13}$$

His most general attack would be to apply a Unitary transformation U to entangle his particles with his ancilla:

$$U|\Psi\rangle_{ABC} = \frac{1}{2}\big(|HH\rangle_{AB} \otimes |VV\rangle_C \otimes A_1 + |HV\rangle_{AB} \otimes |VH\rangle_C \otimes A_2 + |VH\rangle_{AB} \otimes |HV\rangle_C \otimes A_3 + |VV\rangle_{AB} \otimes |HH\rangle_C \otimes A_4\big) \tag{1.14}$$

The measurement performed by the center corresponds to a projection onto the state $|\psi_M\rangle = \alpha|VV\rangle_C + \beta|VH\rangle_C + \gamma|HV\rangle_C + \delta|HH\rangle_C$ and the resulting state is written:

$$|\Phi\rangle_{ABC} = \frac{1}{2}\big(\alpha^*|HH\rangle_{AB} \otimes A_1 + \beta^*|HV\rangle_{AB} \otimes A_2 + \gamma^*|VH\rangle_{AB} \otimes A_3 + \delta^*|VV\rangle_{AB} \otimes A_4\big) \tag{1.15}$$

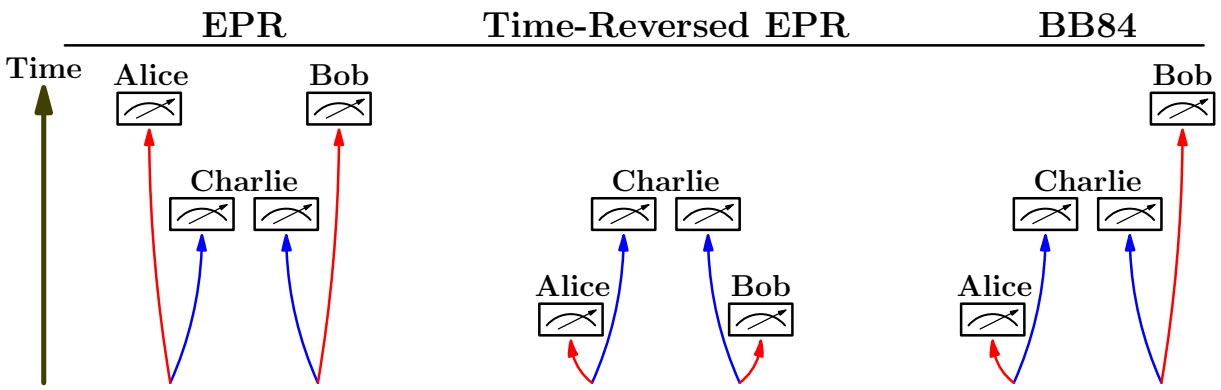

Figure 1.5: Equivalence between EPR , Time-Reversed EPR and BB84 protocols. Two EPR pairs are being distributed to Alice Bob and Charlie. The order in which the projective measurements are performed, determines which protocol is implemented.

In order for the eavesdropper to escape detection, the general state must be an eigenstate of $\sigma_Z^A \sigma_Z^B$ with eigenvalue -1 and eigenstate of $\sigma_X^A \sigma_X^B$ with eigenvalue $+1$. As eigenstate of $\sigma_Z^A \sigma_Z^B$ the state is restricted to have the form,

$$|\Phi\rangle_{ABC} = \frac{1}{2}\left(\beta^* |HV\rangle_{AB} \otimes A_2 + \gamma^* |VH\rangle_{AB} \otimes A_3\right) \tag{1.16}$$

As an eigenstate of $\sigma_X^A \sigma_X^B$ the state is finally restricted to have the form,

$$|\Phi\rangle_{ABC} = \frac{1}{2} c^* \left(|HV\rangle_{AB} + |VH\rangle_{AB}\right) \otimes A_C \tag{1.17}$$

So even in the most general attack, the untrusted center cannot inconspicuously correlate his state to Alice's and Bob's shared state. Noting that in the above the order in which each party perform their measurement does not matter justifying the equivalence of the three protocols, displayed in Figure 1.5.

1.6 Thesis outline

The content of this work is organized as follows.

- Chapter 2 discusses loopholes and exploits that realistic device imperfections may introduce into Quantum Communication schemes. The Measurement-Device-Independent QKD protocol is introduced as a means of defending against any possible Quantum Hacking attacks that target vulnerabilities on the detection instruments.

- Chapter 3 presents our study on the applicability of selection methods in free-space Quantum communication protocols. We simulate the transmittance profile of a

turbulent channel and apply the Prefixed -Threshold selection method on the decoy-state BB84 as an intermediate step towards future implementations for the MDI-QKD protocol. We demonstrate significant improvement on the generated key rate while the implementation does not require any significant technological upgrades.

- Chapter 4 presents an extensive study on realistic implementations of the Hong-Ou-Mandel (HOM) interference. We demonstrate that exceptional HOM interference visibility can be achieved using of the shelf optical components. Since HOM interference is at the heart of the MDI-QKD protocol, this study demonstrates the feasibility of MDI-QKD in realistic applications.

- Chapter 5 discusses three possible future extensions of this work: MDI-QKD over turbulent channels, Quantum Position Verification and Reconfigurable QKD. The successful implementation of the P-RTS selection methods and the study on the H.O.M. interference immediately extend to the experimental demonstration of the MDI-QKD protocol over turbulent channels. Quantum Position Verification offers a quantum solution to the authentication problem. Reconfigurable QKD is an adaptive protocol that switches between the more efficient BB84 or the more secure MDI-QKD depending on the confidence the communicating parties have on the security of their channel.

Chapter 2

Quantum hacking and counter-measures

Quantum Key Distribution provides in principle unconditionally secure communication between two legitimate parties. The security is proved based on the laws of quantum physics. However, any security proof requires certain assumptions which in practice cannot always be fulfilled. Imperfections on the implementation of the protocol may insert loopholes that compromise the communication security. Such imperfections, when recognized, can be included in the security proof such as the G.L.L.P. proof [28]. The pessimistic assumptions though in the GLLP proof reduce the key generation efficiency significantly. Alternatively, the protocol can be modified to pro-actively counter certain attacks as is done with Phase randomization and the decoy state method 2.2. Finally the system can be patched against specific attacks but these patches in turn could open potential unrecognised loopholes. The constant threat that implementation imperfections pose, drove the development of QKD protocols that remove the dependence on the devices that realize thm, such as the Device Independent QKD, section 2.4 and the Measurement Device Independent QKD, section 2.5.

2.1 Attacks on source imperfections; phase randomization and the photon number splitting attack

Quantum communication protocols encode information on modes of the electromagnetic field, with most commonly used the Polarization of single photons or their phase difference from a reference pulse. Single photons sources can exist using spontaneous parametric down conversion but using weak coherent states realized as attenuated laser pulses is far more

convenient. A coherent state for a certain electro-magnetic field mode is expressed as

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \tag{2.1}$$

where $\alpha = |\alpha| e^{\imath\theta}$ and $|\alpha|^2 = \mu$ the average photon number and θ its phase. To remove the phase dependence, which may be exploited by an eavesdropper [29], we phase randomize,

$$\rho = \int_0^{2\pi} \frac{\mathrm{d}\theta}{2\pi} |\alpha\rangle \langle\alpha| \tag{2.2}$$

$$= e^{-|\alpha|^2} \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} \frac{|\alpha|^2}{\sqrt{n!}\sqrt{m!}} |n\rangle \langle m| \int_0^{2\pi} \frac{\mathrm{d}\theta}{2\pi} e^{\imath(n-m)\theta} \tag{2.3}$$

$$= \sum_{n=0}^{\infty} \frac{\mu}{n!} e^{-\mu} |n\rangle \langle n| \tag{2.4}$$

which is interpreted as a classical mixture of number states $|n\rangle$ following a Poissonian distribution. In practice, phase randomization is implemented with a Phase Modulator driven at $\sim kHZ$ frequencies at random amplitudes.

As the photon number follows a Poissonian distribution, there is a probability $p_m(\mu) = 1 - e^{-\mu} - \mu e^{-\mu}$ of pulses with multiple photons. For example for a typical average photon number $\mu = 0.3$, about 3.7% of the pulses contain $n \geq 2$ photons. This can be exploited in the powerful Photon Number Splitting attack [30, 31, 32] where the communication occurs in a lossy channel. An eavesdropper in principle can replace the lossy channel with a lossless one, block part or all of the single photon pulses, since she can not intercept any information from them, split the multi-photon pulses keeping a fraction of photons and wait the public basis discussion to perform her measurement in the correct basis. The strength of the attack is that Eve can completely reproduce Poissonian statistics and depending on the channel loss and the pulse average photon number, she can even intercept the complete key without introducing detectable disturbances [32] . This can be shown as Bob expects to detect with Poisson probability distribution,

$$P_{loss}[n] = \frac{(\eta\mu)^n}{n!} e^{-\eta\mu} \tag{2.5}$$

Eve's strategy first is to block a fraction b of the single photon pulses, creating a distribution

$$P_{PNS}[n] = \begin{cases} (1+b\mu)\, e^{-\mu} & n=0 \\ ((1-b)\,\mu + \mu^2/2)\, e^{-\mu} & n=1 \\ \frac{\mu^{n+1}}{(n+1)!} e^{-\mu} & n>1 \end{cases} \tag{2.6}$$

The value of b is fixed by the condition that the two distributions must give the same vacuum signal probability $P_{loss}[n] = P_{PNS}[0]$ at $b_{match} = \frac{1}{\mu} e^{\mu[(1-\eta)-1]}$. The resulting distribution is not yet Poissonian, but Eve can still replicate Poissonian statistics by removing additional photons from higher multiphoton pulses. The necessary and sufficient condition for Eve to perform the photon redistribution is that $\sum_{i=0}^{n} P_{PNS}[n] \leq \sum_{i=0}^{n} P_{loss}[n]$, which allows photon transfer from higher to lower photon numbers. This condition can easily be fulfilled for a wide range of realistic transmittance η and mean photon μ parameters.

Such attack can be realized with linear optics [33] or by performing a quantum non-demolition measurement to determine the photon number in the pulse. The attacker does not gain information about the polarization , but the polarization mode is preserved. Eve waits until the public discussion to perform the measurement in the correct basis on her preserved photons. To split one photon, Eve can employ the unitary $\hat{U}_{PNS}^{(n)}$ to transfer one photon to modes that she retains.

$$\hat{U}_{PNS}^{(n)} |n,0,0,0\rangle = |n-1,0,1,0\rangle \tag{2.7}$$

$$\hat{U}_{PNS}^{(n)} |0,n,0,0\rangle = |0,n-1,0,1\rangle \tag{2.8}$$

Such a transformation can be realized in terms of the Jaynes-Cummings Hamiltonian, $H_{JC}^{(1)} = \lambda\left(a_1^\dagger \sigma_1 + a_1 \sigma_1^\dagger + a_2^\dagger \sigma_2 + a_2 \sigma_2^\dagger\right)$. She uses a three level atomic system, with ground state $|g\rangle$ and excited states $|e_1\rangle, |e_2\rangle$ and atomic excitation operators $\sigma_1^\dagger, \sigma_2^\dagger$.

$$a_1 \sigma_1^\dagger |n,0,0,0\rangle |g\rangle = |n-1,0,0,0\rangle |e_1\rangle \tag{2.9}$$

$$b_1^\dagger \sigma_1 |n-1,0,0,0\rangle |e_1\rangle = |n-1,0,1,0\rangle |g\rangle \tag{2.10}$$

Source imperfections were included in the theoretical proof GLLP [28], where pessimistically it was assumed that all multi-photon pulses emitted by Alice, are received by Bob $Y_n = 1$, for $n \geq 2$. In the previous the Yield Y_n is the probability that a pulse containing n

photons will eventually give a detection event. The extracted secure key rate R_{GLLP} is

$$R_{GLLP} \geq Q_\mu \cdot \Omega \left[1 - H_2\left(\frac{E_\mu}{\Omega}\right)\right] - Q_\mu \cdot H_2\left(E_\mu\right) \tag{2.11}$$

Where Q_μ is the gain ,i.e. the detection rate, of the signal, E_μ is the error rate for the signal , $\Omega = 1 - \frac{p_{multi}}{Q_\mu}$ is the fraction of detection events originating from single photon pulses and $H_2\left(\cdot\right)$ is the binary entropy fraction

$$H_2(p) = -p\log_2 p - (1-p)\log_2(1-p) \tag{2.12}$$

2.2 The decoy state QKD

To defend against the PNS attack, Hwang introduced [34] the innovative idea that Alice shuffles within her signal pulses, decoy pulses of different intensities. The decoy state method [35, 36, 37] effectively counters the PNS attack, while providing a practical method to tightly bound the estimation on the gain of single photon pulses Q_1 and the error rate e_1 for single photon pulses. Since Eve's measurement can only reveal the number of photons in the pulse but she cannot know whether the pulse is a signal or a decoy, any attack that changes the channel's expected statistics, will be detected. For a state of photon number μ, we can expand the gain Q_μ and QBER $Q_\mu E_\mu$ in terms of the yields of each number state Y_n and the error for each number state $Y_n e_n$,

$$Q_\mu = Y_0 e^{-\mu} + Y_1 \mu e^{-\mu} + Y_2\left(\frac{\mu^2}{2}\right)e^{-\mu} + \ldots + Y_n\left(\frac{\mu^n}{n!}\right)e^{-\mu} \tag{2.13}$$

$$Q_\mu E_\mu = Y_0 e_0 e^{-\mu} + Y_1 e_1 \mu e^{-\mu} + Y_2 e_2\left(\frac{\mu^2}{2}\right)e^{-\mu} + \ldots + Y_n e_n\left(\frac{\mu^n}{n!}\right)e^{-\mu} \tag{2.14}$$

By introducing infinite number of decoys, we get an equation for each decoy $Q_{\nu_1}, Q_{\nu_2}, \ldots, Q_{\nu_n}$, which all share the same Y_n since the yield depends on the channel transmittance and the detection efficiency.

$$
\begin{aligned}
Q_\mu &= Y_0 e^{-\mu} + Y_1 \mu e^{-\mu} + Y_2 \left(\frac{\mu^2}{2}\right) e^{-\mu} + \ldots + Y_n \left(\frac{\mu^n}{n!}\right) e^{-\mu} \\
Q_{\nu_1} &= Y_0 e^{-\nu_1} + Y_1 \nu_1 e^{-\nu_1} + Y_2 \left(\frac{\nu_1^2}{2}\right) e^{-\nu_1} + \ldots + Y_n \left(\frac{\nu_1^n}{n!}\right) e^{-\nu_1} \\
&\vdots \\
Q_{\nu_n} &= Y_0 e^{-\nu_n} + Y_1 \nu_n e^{-\nu_n} + Y_2 \left(\frac{\nu_n^2}{2}\right) e^{-\nu_n} + \ldots + Y_n \left(\frac{\nu_n^n}{n!}\right) e^{-\nu_n}
\end{aligned} \tag{2.15}
$$

Similar for the bit errors, $Q_\mu E_\mu, E_{\nu_1} Q_{\nu_1}, E_{\nu_2} Q_{\nu_2}, \ldots, E_{\nu_n} Q_{\nu_n}$. In principle the set of infinite equations (2.15) can give the exact values of Y_n and $e_n Y_n$ for every n since the $\{Q_\mu, Q_{\nu_1}, \ldots, Q_{\nu_n}\}$ and $\{E_\mu Q_\mu, E_{\nu_1} Q_{\nu_1}, \ldots, E_{\nu_n} Q_{\nu_n}\}$ can be directly measured in the experiment. The secure key rate for a decoy-state QKD protocol is now [35]

$$
R_{decoy-GLLP} \geq Q_1 \left[1 - H_2\left(e_1\right)\right] - Q_\mu \cdot f\left(E_\mu\right) \cdot H_2\left(E_\mu\right) \tag{2.16}
$$

with $Q_1 = Y_1 \mu e^{-\mu}$. Compared to the R_{GLLP} rate of (2.11), the decoy state rate (2.16) offers more than two order of magnitude improvement[35] for typical experimental parameters. In practice since we use decoys with photon number $\nu \ll 1$, the higher order terms of eq.(2.15) quickly become insignificant and just two decoy states [37] are enough to give tight bounds on Q_1 and e_1. Indeed for a signal state of photon number μ and two decoy states of photon numbers ν_1, ν_2 where $0 \leq \nu_1 \leq \nu_2$ and $\nu_1 + \nu_2 < \mu$ we have

$$
Q_\mu = Y_0 e^{-\mu} + Y_1 \mu e^{-\mu} + Y_2 \left(\frac{\mu^2}{2}\right) e^{-\mu} + \ldots + Y_n \left(\frac{\mu^n}{n!}\right) e^{-\mu} \tag{2.17}
$$

$$
Q_{\nu_1} = Y_0 e^{-\nu_1} + Y_1 \nu_1 e^{-\nu_1} + Y_2 \left(\frac{\nu_1^2}{2}\right) e^{-\nu_1} + \ldots + Y_n \left(\frac{\nu_1^n}{n!}\right) e^{-\nu_1} \tag{2.18}
$$

$$
Q_{\nu_2} = Y_0 e^{-\nu_2} + Y_1 \nu_2 e^{-\nu_2} + Y_2 \left(\frac{\nu_2^2}{2}\right) e^{-\nu_1} + \ldots + Y_n \left(\frac{\nu_2^n}{n!}\right) e^{-\nu_1} \tag{2.19}
$$

The goal is to find tight bounds on the yields Y_0 and Y_1. Combining eq.(2.18) and eq.(2.19) to eliminate the Y_1 term we have

$$
\nu_1 Q_{\nu_2} e^{\nu_2} - \nu_2 Q_{\nu_1} e^{\nu_1} = \left(\nu_1 - \nu_2\right) Y_0 - \nu_1 \nu_2 \left(Y_2 \frac{\nu_1 - \nu_2}{2!} + Y_3 \frac{\nu_1^2 - \nu_2^2}{3!} + \ldots\right) \tag{2.20}
$$

the second term is quite less significant especially as $\nu_2 \to 0$ so Y_0 can be bounded as

$$
Y_0 \geq \max\left[\frac{\nu_1 Q_{\nu_2} e^{\nu_2} - \nu_2 Q_{\nu_1} e^{\nu_1}}{\nu_1 - \nu_2}, 0\right] \tag{2.21}
$$

Similarly, combining again eq.(2.18) and eq.(2.19) to eliminate the Y_0 term we have

$$Q_{\nu_1}e^{\nu_1} - Q_{\nu_2}e^{\nu_2} = (\nu_1 - \nu_2)\, Y_1 + \sum_{i=2}^{\infty} \frac{Y_i}{i!} \left(\nu_1^i - \nu_2^i\right) \tag{2.22}$$

the summation series in eq.(2.22) are comparable with the Y_1 term and cannot be discarded, but can be bounded since for $i \geq 2$ and $1 > \nu_1 + \nu_2 > 0$ it is $\nu_1^2 - \nu_2^2 \geq \nu_1^i - \nu_2^i$ we have

$$\sum_{i=2}^{\infty} \frac{Y_i}{i!} \left(\nu_1^i - \nu_2^i\right) \leq \frac{\nu_1^2 - \nu_2^2}{\mu^2} \sum_{i=2}^{\infty} Y_i \frac{\mu^i}{i!} \tag{2.23}$$

The quantity $\sum_{i=2}^{\infty} Y_i \frac{\mu^i}{i!}$ describes the multi-photon contributions and can expressed as the total detections minus the vacuum and single photon contributions,

$$\sum_{i=2}^{\infty} Y_i \frac{\mu^i}{i!} = Q_\mu e^\mu - Y_0 - Y_1 \mu \tag{2.24}$$

Putting eq.(2.22), eq.(2.23), eq.(2.24) together, the single photon yield is lower bounded as

$$Y_1 \geq \frac{\mu}{\mu\nu_1 - \mu\nu_2 - \nu_1^2 + \nu_2^2} \left(Q_{\nu_1}e^{\nu_1} - Q_{\nu_2}e^{\nu_2} - \frac{\nu_1^2 - \nu_2^2}{\mu^2} \left(Q_\mu e^\mu - Y_0\right) \right) \tag{2.25}$$

In a similar fashion expanding the QBER associated with the decoys ν_1 and ν_2

$$E_{\nu_1} Q_{\nu_1} e^{\nu_1} = e_0 Y_0 + e_1 Y_1 \nu_1 + \sum_{i=2}^{\infty} e_i Y_i \frac{\nu_1^i}{i!} \tag{2.26}$$

$$E_{\nu_2} Q_{\nu_2} e^{\nu_2} = e_0 Y_0 + e_1 Y_1 \nu_2 + \sum_{i=2}^{\infty} e_i Y_i \frac{\nu_2^i}{i!} \tag{2.27}$$

Subtracting eq.(2.26,2.27), eq.(2.27) simply yields

$$e_1 \leq \frac{E_{\nu_1} Q_{\nu_1} e^{\nu_1} - E_{\nu_2} Q_{\nu_2} e^{\nu_2}}{(\nu_1 - \nu_2)\, Y_1^L} \tag{2.28}$$

Active phase randomization and the decoy-state method have been a standard in modern QKD applications and are implemented on our study of the BB84 protocol in a turbulent channel in Chapter 3.

2.3 Attacks on detector side imperfections

A QKD protocol requires a detection setup, typically realized with a set of Single Photon Avalanche Detectors. These devices employ a $p-n$ junction diode, reversed biased well above it's breakdown voltage. At this point the arrival of even a single photon, at the appropriate wavelength, can trigger a self sustaining avalanche of photoelectrons which is registered as an electronic pulse. After a successful detection event, the detector blanks its active detection region for a time interval called the dead-time, typically a few μs, to allow any active carriers to discharge and so minimine unwanted false events called afterpulses. The intricate operation of such detectors allow side channel attacks and multiple research groups have demonstrated the feasibility of such attacks on existing QKD systems even with existing technology.

The Time shift attack [38, 39] targets systems that employ gated single photon detectors. The efficiency of these detectors is time dependent, exhibiting a finite response time and steady detection plateau. Alice and Bob calibrate their systems so the signals arrive at the center of the detection plateau for each detector but the efficiency profiles may not completely overlap in time, Figure 2.1. Eve ,who can in principle control the channel, can exploit this mismatch by introducing delays that shift the pulse randomly between positions t_0 and t_1 causing an asymmetry in the detection efficiency between the two detectors. The attack allows Eve to know the recorded bit with probability depending on the efficiency mismatch and since it does not require interception of Alice's state, no errors are introduced making it harder for Alice and Bob to detect the eavesdropping. Eve also can hide the efficiency decrease caused by her attack, since she can control in principle the channel loss either in the calibration phase or in the actual communication phase. The attack was launched successfully on the commercially available QKD system, ID-500 from ID Quantique [39].

The Phase remapping attack [40, 41] targets QKD systems where the bit is encoded as the relative phase between consecutive pulses by exploiting imperfections on the phase modulator used for the encoding. Eve intercepts Bob's reference pulse and sends to Alice signal pulses, carefully delayed so it arrives on the rising or falling edge of the modulating signal Figure 2.1 used by Alice to apply the phase difference. Even if the rising edge is comparable with the pulse width, Eve can still manipulate the polarization of the pulse and exploit the asymmetry of the modulation depth for orthogonal polarizations. The feasibility of the attack was demonstrated against a commercial QKD system, ID-500 from ID Quantique [41]. The attack can be extended by exploiting potential mismatches in the detector efficiencies [42].

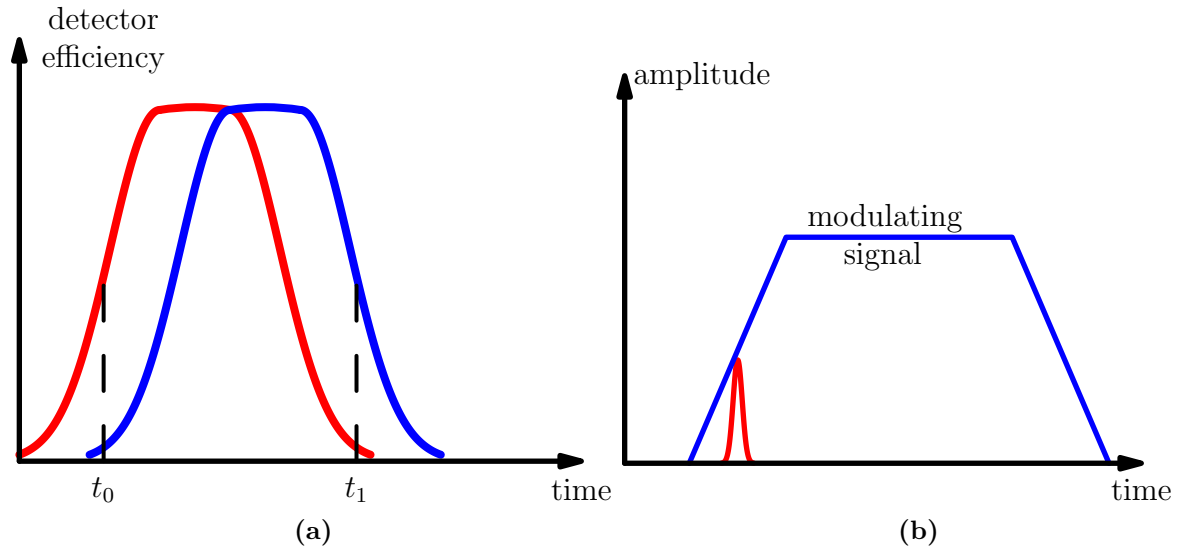

Figure 2.1: (a) Time shift attack. (b) Phase remapping attack.

Lyderesen *et al.* [43] used strong pulses to blind [44] Bob's single photon avalanche detectors at will. A blinded detector no longer behaves as a single photon detector but rather as a classical photo-diode, where the generated photo-current is linearly proportional to the input light power. If Eve sends bright pulses above a certain power threshold she can force a detection event that mimics the detections of legitimate single photons, completely manipulating the key generation. To execute the attack, Eve intercepts Alice's pulses and measures them, as Bob would. Then she sends strong pulses to Bob according to her measurement result targeting the linear mode of Bob's detectors. Eve calibrates the pulse power in way that Bob's detector clicks only when Eve and Bob use the same basis and finally listens to the public discussion and performs the same error correction and privacy amplification as Alice and Bob. The group demonstrated the feasibility of the attack on the commercial QKD systems Clavis2 from ID Quantique and QPN 5505 from MagiQ. Gerhart *et al.* [45] launched the intercept and resend tailored light attack on a fully functional experimental QKD setup and completely intercepted the shared key. Wiechers *et al.* [46] launched a similar intercept and resend attack on the Clavis2 commercial QKD system from ID Quantique. The system has a loophole where it accepts strong pulses sent few ns before or after the gate as legitimate signals, while the detector is in linear mode. This attack increases the QBER due to increased afterpulses, but Eve can exploit an additional loophole in the system since it registers the strong pulses even during the dead-time phase, allowing her to extend the dead-time phase at will and so register fake signals without increasing the QBER due to afterpulses. Possible countermeasures could involve a careful time resolving to check whether the detection occurred in or outside the gate, a watchdog detector to check

the intensity of the incoming pulses, or by randomly removing gates and check if detections are still registered.

Ref.[47] demonstrates a simple but effective attack that exploits the dead-time setting on Single Photon Avalance detectors working in Free Running mode. For her attack, Eve sends a blinding pulse with effective photon number $\eta\mu \sim 10$ photons at one of the four BB84 states $\{H, V, D, A\}$. Eve's pulse arrives a little before Alice's pulse, and blinds three detectors with high probability. For example if Eve sends an H blinding pulse, the H, D and A detectors are blinded, each with certain probability. Thus she gains knowledge on Bob's detection bit since probably it was acquired by the detector orthogonal to her state. A simple countermeasure would be to accept events only when all detectors are active.

2.4 Device Independent QKD

In the Device-Independent QKD [48, 49, 50, 51, 52, 53], an EPR source in the middle creates pairs of entangled qubits. Alice and Bob, each receive a qubit and perform a measurement just as the original Ekert91-EPR protocol. This time we assume that all the devices, Alice and Bob use to implement the protocol, including measurement and source preparation, can be in Eve's control. In fact the apparatuses can be seen as collective black boxes that accept some classical inputs and return classical outputs, while the source they are being distributed may belong to a Hilbert space that is a subset of the Hilbert space that Eve controls. Alice and Bob though can still use the classical outputs and calculate the CHSH polynomial, and because of the monogamous nature of the entanglement, as soon as they establish that the Bell inequalities are violated, they can bound Eve's information. In a particular implementation, Alice performs the measurements A_0, A_1, A_2 with outcomes $\{a_0, a_1, a_2\}$ and Bob B_1, B_2 with outcomes $\{b_1, b_2\}$, just as in Ekert91 [23]. The raw key is extracted from the measurements of A_0 and B_1 while the QBER is $Q = Prob\,(a_0 \neq b_1 \mid 01)$. For example it could be $A_0 = B_1 = \sigma_z$, $A_1 = \dfrac{\sigma_Z + \sigma_X}{2}$, $A_2 = \dfrac{\sigma_Z - \sigma_X}{2}$.

Alice and bob use a subset of their data to compute the CHSH polynomial [19]

$$\mathcal{S} = \langle a_1 b_1 \rangle + \langle a_1 b_2 \rangle + \langle a_2 b_1 \rangle - \langle a_2 b_2 \rangle \tag{2.29}$$

where the correlator $\langle a_i b_j \rangle = Prob\,(a = b \mid ij) - Prob\,(a \neq b \mid ij)$. Then they can upper bound the information Eve has on their shared key as

$$\chi\,(B_1 : E) \leq h\left[\frac{1}{2}\left(1 + \sqrt{(\mathcal{S}/2)^2 - 1}\right)\right] \tag{2.30}$$

which is independent of Q, with $h(\cdot)$ the binary entropy function. They can extract a secure key at rate

$$R \geq 1 - h\left(Q\right) - \chi\left(B_1 : E\right) \tag{2.31}$$

As the violation of the Bell inequalities is the cornerstone of the DI-QKD, failure to produce genuine violation could compromise the protocol's security. Two important loopholes in Bell experiments can impact DIQKD protocos. First the locality loophole which requires the communicating parties to be space-like separated as otherwise a classical protocol can reproduce any observed correlations. The second and more difficult to mitigate, is the detection loophole [54], where if the detection efficiency is below a certain value, a local model can exploit not-detected events and reproduce non-local correlations. The detection loophole severely restricts the efficiency of the DIQKD as it requires very high detection setups with efficiencies $\eta > 82.8\%$ for testing the CHSH inequality [49].

2.5 Measurement-Device-Independent QKD

Realistic implementations of QKD protocols introduce back-doors that can be exploited by an eavesdropper. One solution could be to fully characterize the flaws of the devices. But this is highly impractical and can prove dangerous since unexpected attacks are the most threatening. The Device-Independent QKD protocol discussed in section 2.4, based on the entanglement monogamy, removes in principle all possible device loopholes, but in practice it is difficult to realize since it requires near perfect efficiency detectors. The time reversed EPR protocol [26] discussed in subsection 1.5.5 assumes a completely untrusted detection center. The authors revolve the discussion around the spin singlet state since it can be discriminated but also mention that the protocol could be implemented with a general Bell state discriminator. Furthermore, Inamori in his security proof [27] mentions the use of polarized photon states for this purpose. Few years later Bell state discrimination was proposed using linear optics [55, 56]. While linear optics utilize weak coherent pulses which can introduce vulnerabilities and exploits as discussed in subsection 2.2, active phase randomization and the decoy state method can protect against possible source attacks without compromising the protocol's efficiency. Putting everything together, Lo , Curty and Qi proposed the protocol Measurement-Device-Independent (MDI) QKD [57] that removes all possible loopholes that flaws in the detection setup may introduce, under the assumption that Alice and Bob can perfectly prepare their states.

The principle of the protocol is presented in the schematic of Figure 2.2. Alice and Bob prepare independently in their labs, phase randomized weak coherent states realized

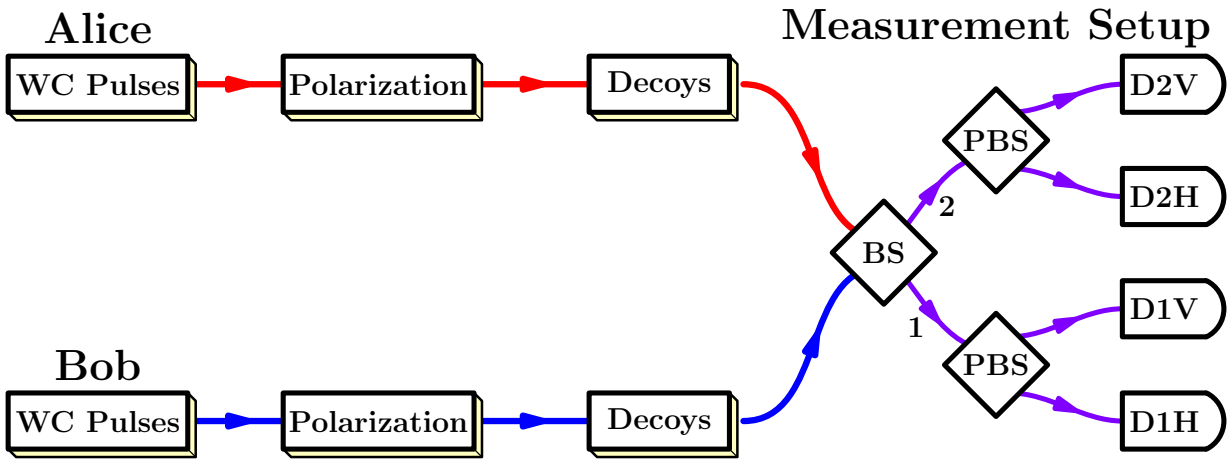

Figure 2.2: MDI-QKD schematic. Alice and Bob prepare independently phase randomized weak coherent (WC) pulses. In their respective lab they encode their bits as polarization states and modulate the pulse intensities to implement the decoy state method. Then they send their states to a middleman , Charlie who performs a Bell state projection measurement and announces the results.

as attenuated laser pulses. They encode their bits as polarization in the four BB84 states : Horizontal, Vertical, Diagonal, Anti-diagonal ($|H\rangle, |V\rangle, |D\rangle, |A\rangle$). They implement the decoy state method by modulating the pulse intensities. Then they send their states to a middleman Charlie ,who may even be untrusted, to perform a Bell state projection and announce the results. Charlie's setup consists of a 50 : 50 Beam Splitter where the incoming states undergo Hong-Ou-Mandel (H.O.M.) interference [58]. Each output of the Beam Splitter is directed to a Polarization Beam Splitter (PBS) and a pair of Single Photon Avalance Detectors (SPAD) to measure the Polarization state (Horizontal or Vertical).

Depending on the result announced, Alice and Bob can correlate the bits they have in their possession. Specifically, with the indices 1&2 in Figure 2.2 denoting the output ports of the beam splitter, the Bell state projection is understood as follows ,

- Coinciding detections on opposite beam splitter (BS) ports:
  (D1V and D2H) or (D2V and D1H) correspond to a projection on the $|\Psi^-\rangle = \frac{1}{\sqrt{2}}[|HV\rangle - |VH\rangle]$ state.
- Coinciding detections from the same beam splitter (BS) port :
  (D1V and D1H) or (D2V and D2H) correspond to the $|\Psi^+\rangle = \frac{1}{\sqrt{2}}[|HV\rangle + |VH\rangle]$ state.

The above projection can be understood as a two photon state is a symmetric state since photons are bosons, particles with integer spin, and can be written as the product of their

spatial and polarization sate,

$$|\psi\rangle = |\psi\rangle_{spatial} \otimes |\psi\rangle_{poalrization} \tag{2.32}$$

When the photons exit on opposite ports, the spatial state is necessarily anti-symmetric, so their polarization state has to be anti-symmetric as well, with the state $|\Psi^-\rangle$ being the only possibility. Similarly, exit at the same port corresponds to a symmetric spatial state and therefore a symmetric $|\Psi^+\rangle$ polarization state. Noting that the Bell states $|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}[|HH\rangle \pm |VV\rangle]$ cannot be utilized since they require the photons to land on the same detector, but typical single photon detectors cannot resolve multiple incoming photons. Depending on the announcement made by Charlie , Alice and Bob can determine how their bits are correlated during the public basis comparison. If they both used the rectilinear basis and Charlie announces either $|\Psi^+\rangle$ or $|\Psi^-\rangle$, one has to perform a bit flip during post-processing. If they both used the diagonal then if the relay projects on to the $|\Psi^-\rangle$ again one has to perform flip but if the relay outputs $|\Psi^+\rangle$ no bit flip is required, as summarized in Table 2.1.

The correlations presented in Table 2.1 can easily be shown. For example if we assume that both Alice and Bob use the diagonal basis and the choose the same bit $\nearrow$ then if the Bell state projection is successful, it can only be the $|\Psi^+\rangle$. For the schematic of Fig.(2.2) assume that Alice and Bob send single photons $a^\dagger_{\nearrow} b^\dagger_{\nearrow} |0\rangle$ as input to the beam splitter and the beam splitter is represented by the unitary matrix,

$$\hat{U_{BS}} = \frac{1}{\sqrt{2}} \begin{pmatrix} \imath & 1 \\ 1 & \imath \end{pmatrix} \tag{2.33}$$

with $c^\dagger_k |0\rangle$ and $d^\dagger_k |0\rangle$ being the creation operators for the polarization k on the c and d output ports respectively, the beam splitter output state can be written as,

$$|\psi_{out}\rangle = \frac{\imath}{4}\left[\left(c^\dagger_H c^\dagger_H + 2c^\dagger_H c^\dagger_V + c^\dagger_V c^\dagger_V\right) + \left(d^\dagger_H d^\dagger_H + 2d^\dagger_H d^\dagger_V + d^\dagger_V d^\dagger_V\right)\right]|0\rangle \tag{2.34}$$

Table 2.1: Bits sent by Alice , encoded as polarization states on randomly selected bases.

Basis used by both Alice and Bob	Charlie announces $\|\Psi^-\rangle$	Charlie announces $\|\Psi^+\rangle$
Rectilinear	Bit flip is required	Bit flip is required
Diagonal	Bit flip is required	No bit flip required

The valid events $c_H^\dagger c_V^\dagger |0\rangle$ and $d_H^\dagger d_V^\dagger |0\rangle$ are equivalent to a $|\Psi^+\rangle$ projection. Alice and Bob have the same bit $|\nearrow\rangle$ in possession and no bit flip is required, in accordance with Table 2.1.

For a realistic implementation, including detection errors the protocol produces a key generation rate,

$$R = Q_{rect}^{1,1}\left[1 - H\left(e_{diag}^{1,1}\right)\right] - Q_{rect} f\left(E_{rect}\right) H\left(E_{rect}\right) \tag{2.35}$$

with $Q_{rect}^{1,1}$ the single photon gain, i.e. the gain when Alice and Bob both sent single photon pulses in the rectilinear basis and $e_{diag}^{1,1}$ the error associated with single photon pulses in the diagonal basis. These two parameters are estimated with the decoy state method. Also Q_{rect} and E_{rect} are the gain and Quantum Bit Error rate for the rectilinear basis and are directly determined experimentally.

MDI-QKD is ideal for applications involving remote and mobile communicating parties that cannot utilize fiber networks, such as ships and planes. The measurement center could be a satellite or a foreign agency who may not be trusted. In this scenario, as the communication takes place over free space channel, atmospheric turbulence has a significant impact in the degradation of the secure key generation rate as is responsible for the loss of transmitted photons. The implementation of selection methods that reject or discard recorded bits, depending on the transmittance they experience, significantly improves the signal-to-noise ratio and pairing with the MDI-QKD offer a secure and efficient communication scheme over free-space turbulent channels. The following chapters examine the main components of this scheme: the application of the selections methods over turbulent channel for the simpler BB84 protocol and the Hong-Ou-Mandel interference which is at the heart of MDI-QKD and characterizes its efficiency.

Chapter 3

Experimental decoy state BB84 quantum key distribution using the prefixed-threshold real-time selection method

3.1 Motivation

As Quantum communication grows beyond proof-of-principle in lab experiments towards large scale commercial deployment in the near future a lot of attention is on the optical medium such networks will be realized on. Fiber optical networks are possible at metropolitan scales [59, 60] but are limited in distance due to transmission losses, typically 0.18 $^{dB}/_{km}$ at a 1550nm wavelength [61]. While classical optical signals travelling in fiber, can be enhanced by intermediate amplifiers and reach far larger distances, such techniques cannot be employed for Quantum Communication schemes due to the no-cloning theorem [62]. Quantum Repeaters [63] appear as a possible solution but still a lot of progress needs to be made before they become available for practical Quantum Communication. Free-space channels offer an attractive alternative for intermediate distances for mobile or remote communicating parties or as part of a ground-to-satellite network. So far experimental demonstrations in free-space include ground to plane [64], to hot air balloon [65] and to drones [66]. Signals travelling in free-space experience losses due to the divergence of the beam diameter, absorption and scattering, and the atmospheric turbulence. The beam divergence can be accommodated by increasing the size of the receiving lenses and absorption and scattering cause a consistent degradation of the signal intensity. On the other hand

turbulence is associated with fluctuations in the temperature , pressure and humidity of the air which result in random variations in the atmospheric refractive index [67]. The description of light propagation in a turbulent medium is a very difficult problem but the channel can be described statistically and is accepted that the transmission coefficient can be approached by a log-normal probability distribution [68, 69, 70]. Free-space implementations so far treat the effect of the turbulence as an average loss and do not consider the particular distribution of the transmittance coefficient.

Taking the channel statistics into account, various selection methods have been recently proposed that reject or discard recorded bits if they experience low channel transmittance, aiming to improve the signal-to-noise ratio (SNR). Evren *et al.* [71] developed a signal-to-noise ratio filter (SNRF) where the quantum data are grouped into bins during post-processing. Any bins containing a detection rate below a certain threshold are discarded. The algorithm searches for the optimal bin-size and optimal detection rate per bin threshold that maximizes the extracted secret key rate. Vallone *et al.* [72] employed a secondary classical laser beam to probe the channel statistics. They observed a good correlation between the classical and quantum detection data and developed the Adaptive Real-Time Selection method (ARTS) to adaptively select high transmittance bits and therefore decrease in post-processing the Quantum Bit Error rate (QBER), improving the extracted secure key rate. Wang *et al.* [73] proposed the Prefixed-Real Time Selection (P-RTS) method and show that the optimal selection threshold is independent of the channel statistics and depends mainly on the receiver's detection setup characteristics i.e. the detection efficiency and background noise and secondarily to the intensity of the quantum signals. Thus the selection cutoff can be predetermined and the rejection can be accomplished in real time without the need to store unnecessary bits or perform extra post-processing. While the authors of [73] demonstrated the P-RTS method in single photon and decoy-state BB84 QKD, including finite-size effects, the method is general and can be applied in other Quantum Communication protocols. Indeed a recent study [74] applies the selection method to the Measurement-Device-Independent QKD (MDI-QKD) protocol [57].

In this study the selection method is employed experimentally on the finite-size decoy state BB84 [14] QKD protocol. The random transmittance fluctuations caused by the atmospheric turbulence are simulated using an Intensity Modulator. Performing the experiments in a laboratory environment allows the study of different atmospheric conditions in a controllable and predictable manner. Noting also a recent study where the effects of turbulence on the optical wave-front are also simulated. [75].

3.2 Key generation in a turbulent channel

By keeping all the experimental parameters fixed, i.e. Bob's detection parameters: his detector's efficiencies, background noise and optical misalignment as well as Alice's quantum state parameters, we can write the key rate as a single function of the transmittance $R(\eta)$. The maximum information we can extract by the channel's statistics is by convoluting the Probability Density of the Transmission Coefficient (PDTC) $p(\eta)$ with the rate $R(\eta)$.

$$R^{max} = \int_0^1 R(\eta)\, p(\eta)\, \mathrm{d}\eta \tag{3.1}$$

On the other hand such an integration is not possible in practical applications. What we can do is set a threshold η_{TH} below which recorded bits are discarded, thus keeping only a fraction $\int_{\eta_{TH}}^1 p(\eta)\, \mathrm{d}\eta$ of the sent signals and then treat the remaining recordings as they have passed through a static channel of average transmittance $\langle\eta\rangle$ which is computed only from the transmittances above the threshold:

$$\langle\eta\rangle = \frac{\int_{\eta_T}^1 \eta p(\eta)\, \mathrm{d}\eta}{\int_{\eta_T}^1 p(\eta)\, \mathrm{d}\eta} \tag{3.2}$$

Thus the rate we can calculate is:

$$R(\eta_T) = R(\langle\eta\rangle) \times \int_{\eta_T}^1 p(\eta)\, \mathrm{d}\eta \tag{3.3}$$

The authors of [73] show that the rate (3.3) we can calculate can approach very well the ideal rate of eq.(3.1) by making two key observations. First there exists a critical η_{CR} that $R(\eta) = 0$ for $\eta < \eta_{CR}$. Thus we have

$$R^{max} = \int_0^1 R(\eta)\, p(\eta)\, \mathrm{d}\eta = \int_{\eta_{CR}}^1 R(\eta)\, p(\eta)\, \mathrm{d}\eta \tag{3.4}$$

Secondly the rate $R(\eta)$ although convex in general, approaches linearity very well as shown in Figure 3.1 for the asymptotic Gottesman-Lo-Lütkenhaus-Preskill Rate (GLLP) [28].

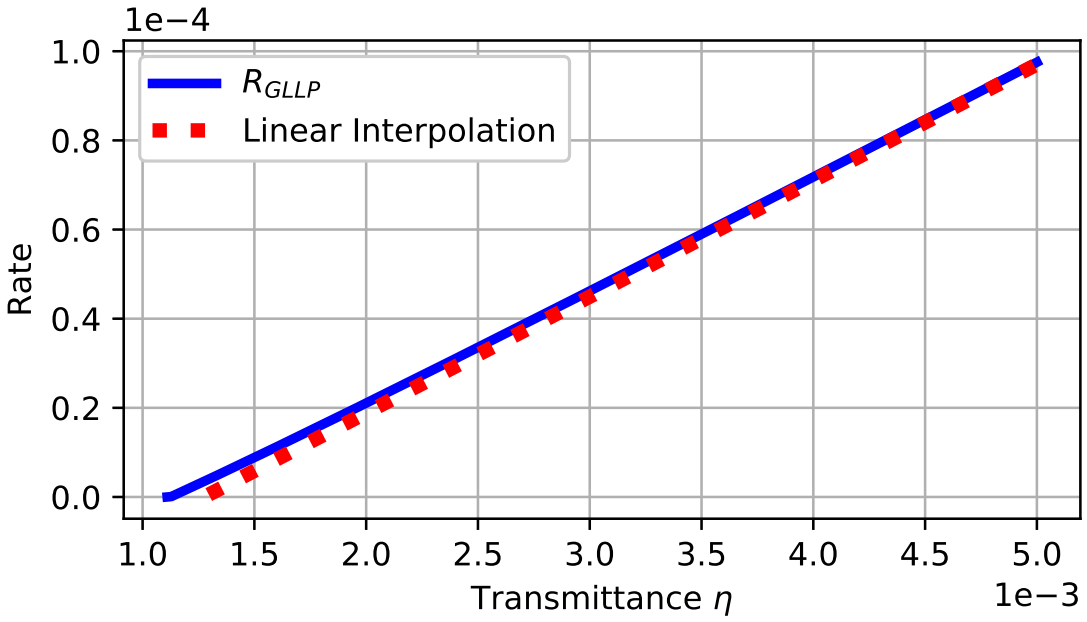

Figure 3.1: Reproduction from [73]. The R_{GLLP} rate approaches linearity very well.

Approaching the rate $R(\eta)$ as linear $R(\eta) \approx \alpha \cdot \eta + \beta$ we have,

$$\int_{\eta_{CR}}^{1} R(\eta)\, p_{\eta_0,\sigma}(\eta)\, \mathrm{d}\eta \approx \int_{\eta_{CR}}^{1} (\alpha \cdot \eta + \beta)\, p_{\eta_0,\sigma}(\eta)\, \mathrm{d}\eta \tag{3.5}$$

$$= \int_{\eta_{CR}}^{1} \alpha \cdot \eta p_{\eta_0,\sigma}(\eta)\, \mathrm{d}\eta + \int_{\eta_{CR}}^{1} \beta p_{\eta_0,\sigma}(\eta)\, \mathrm{d}\eta \tag{3.6}$$

$$= R(\langle\eta\rangle) \times \int_{\eta_{CR}}^{1} p_{\eta_0,\sigma}(\eta)\, \mathrm{d}\eta \tag{3.7}$$

In eq.(3.6) the average $\langle\eta\rangle$ is calculated in the $[\eta_{CR}, 1]$ region using the truncated distribution according to eq.(3.2). Finally we note that η_{CR} is the optimal choice for the threshold since both factors of eq.(3.7) decrease monotonically for $\eta > \eta_{CR}$. In conclusion, the simple rate of eq.(3.3) is a very good approximation of the maximum rate eq.(3.1) if we choose the threshold to be equal with the the critical transmission η_{CR}.

If we take into account the divergence of linearity, the optimum threshold does not coincide with η_{CR} any more. As a result the approximation of eq.(3.7) is slightly below the maximum rate form eq.(3.4) .

When we consider the finite-size effects the parameters needed for the secure key rate calculation depend on the number of pulses N sent by Alice. Discarding low transmittance

events affects the available pulses, so we need to modify $N \rightarrow N \times \int_{\eta_T}^{1} p(\eta)\,\mathrm{d}\eta$ and the distilled secure key rate is modified as:

$$R = R_{Finite-size}\left(\langle\eta\rangle, N \times \int_{\eta_T}^{1} p(\eta)\,\mathrm{d}\eta\right) \times \int_{\eta_T}^{1} p(\eta)\,\mathrm{d}\eta \tag{3.8}$$

The estimation of the secure key rate utilizes the decoy-state QKD with finite size effects model from Lim *et al.* [76].

3.3 Experimental setup

In Figure 3.2 the experimental setup is presented. A continuous-wave (CW) laser source (Wavelength References) at $1550.5nm$, in-between the ITU channels 33 and 34, is used to encode our quantum states on. The light is directed to a Phase Modulator (EOSPACE) that performs phase randomization and subsequently to a $LiNbO_3$ (EOSPACE) Intensity Modulator to carve out pulses of FWHM $\sim 1.5ns$ at $25MHz$ repetition rate. The DC bias Voltage of the Intensity modulator is automatically adjusted by a Null Point Controller (PlugTech) to achieve optimal extinction ratio (typically $\sim 1 \cdot 10^{-3}$). This modulator also implements the decoy-state method as it is driven by an Arbitrary Waveform generator where the amplitudes of the pulses are created according to the desired decoy intensities and frequencies. The polarization state is encoded by a homemade high-speed polarization modulation setup which shown in the schematic of Figure 3.3. This set-up is described in reference [77] and was proposed in [78].

The pulses are attenuated by a combination of digital and analog variable attenuators down to single photon levels. The quantum states are multiplexed with classical laser pulses that are used to probe the channel's transmittance statistics and both are directed to an Acousto-Optic Modulator (Brimrose) that is simulating the turbulent channel. Bob's selection setup consists of a De-multiplexer (Lightel) that separates the classical laser probing the intensity fluctuations and the quantum laser in which Alice's state is encoded. The classical laser is collected by a high gain detector (Thorlabs) and an oscilloscope (Tektronix) stores the data for the fluctuations. The quantum signal is directed to an additional De-multiplexer to enhance the isolation between classical & quantum signal. In overall combining time multiplexing with isolation $\sim 10^{-3}$ and frequency multiplexing with isolation $\sim 10^{-4} \times 10^{-4}$ we achieve a crosstalk between classical and quantum lasers $\sim 10^{-11}$. A $50:50$ Beam Splitter passively selects Bob's detection basis, rectilinear or diagonal. Each basis is realized by a Polarization Beam Splitter and a pair of InGaAs Single Photon Avalance Detectors (IDQ210) gated at $25MHz$ with $\sim 5ns$ gate width.

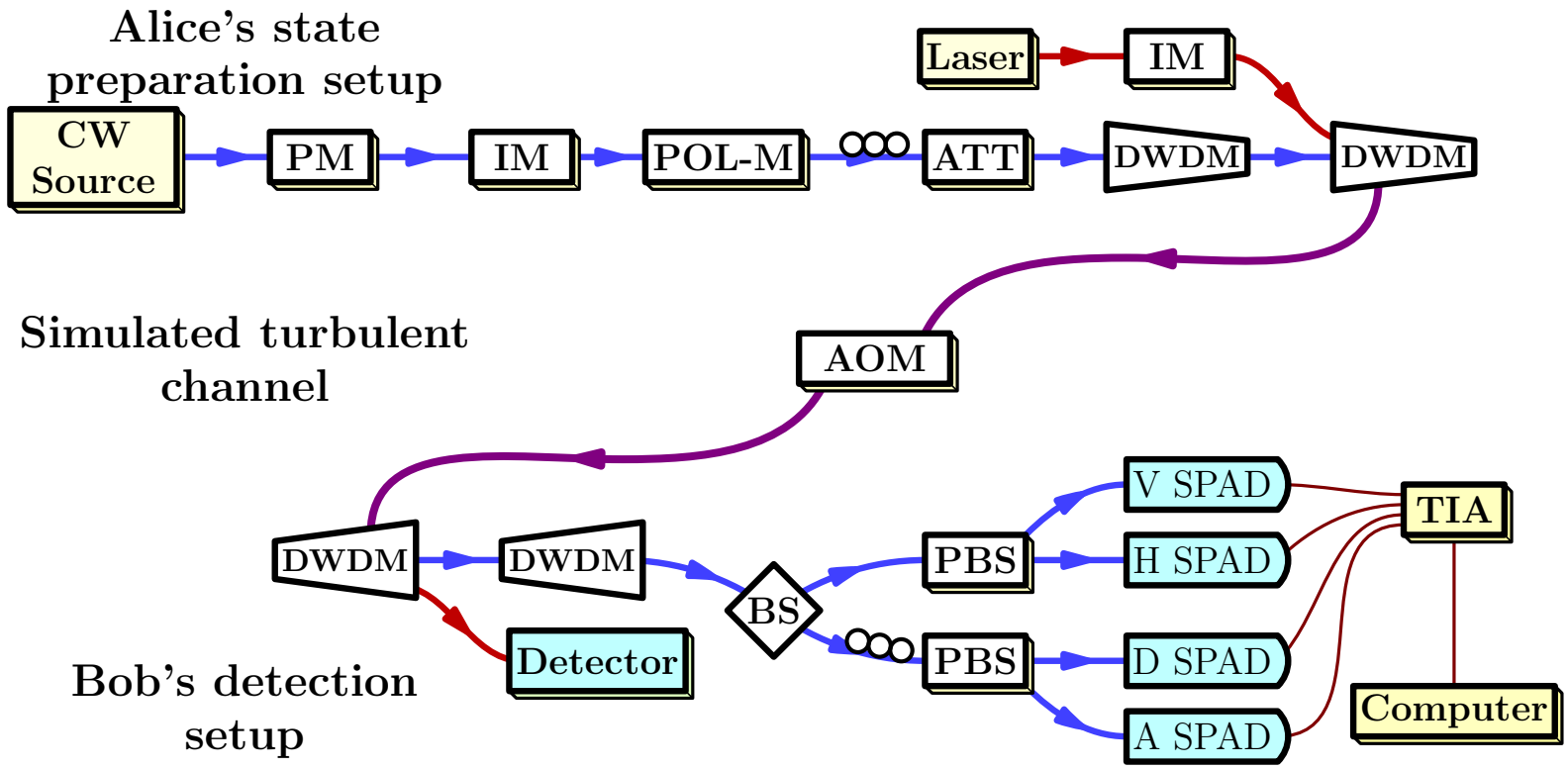

Figure 3.2: Schematic of the experimental setup. DWDM: Dense Wavelength Division Multiplexer, IM: Intensity Modulator, Pol-M: Polarization Modulator setup depicted in Figure(3.3), ATT: Variable Attenuator, AOM: Acousto-Optic Modulator, BS: 50:50 Beam Splitter, PBS: Polarization Beam Splitter, {H,V,D,A} SPAD: Single Photon Avalanche Detectors, TIA: Time Interval Analyzer. Blue connecting lines represent fibers that transmit the quantum signals , Red fibers that transmit the classical probing laser and Purple fibers where the two lasers coexist.

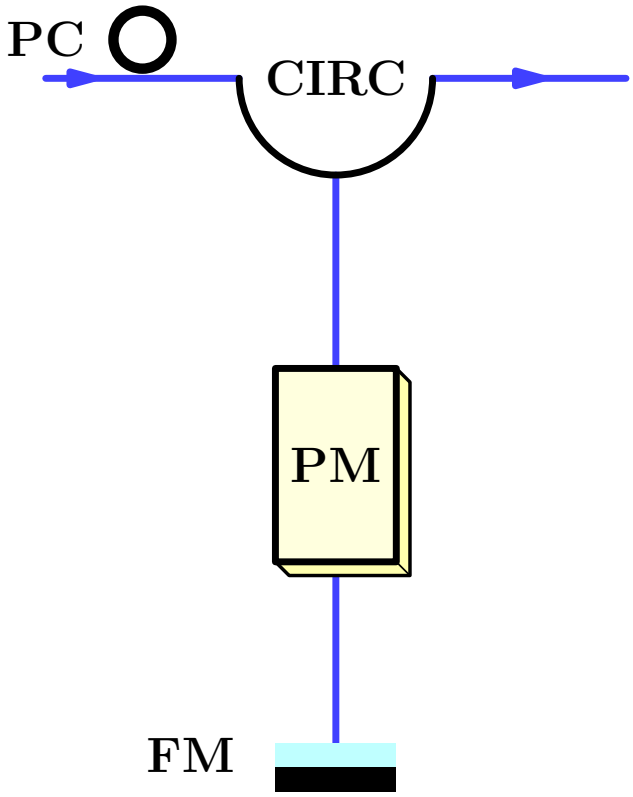

Figure 3.3: Schematic of the Polarization Modulation setup. PC: single paddle Polarization Controller, CIRC: Circulator, PM: Phase Modulator, FM: Faraday Mirror.

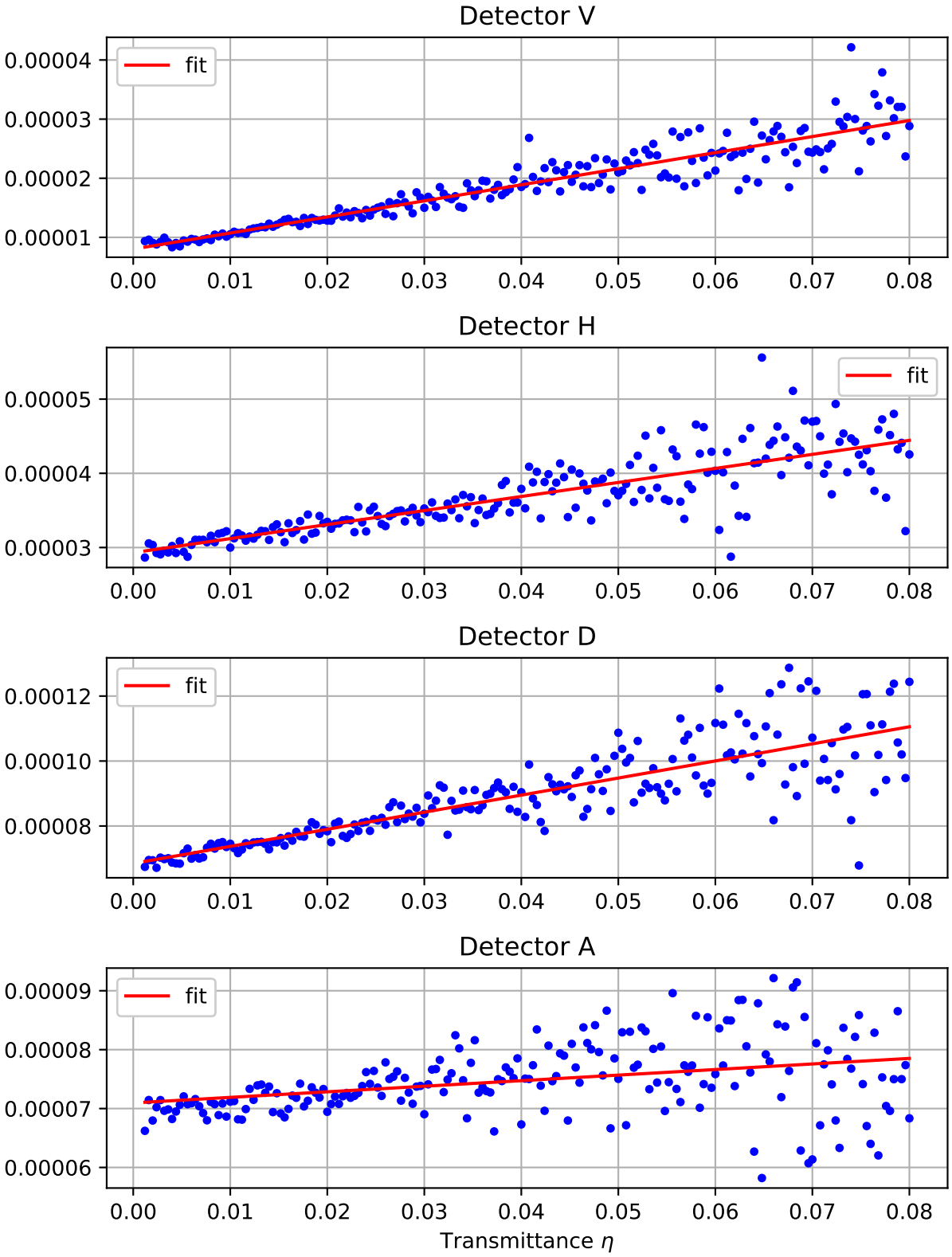

Figure 3.4: Fits to extract the background noise parameters for each detector. On the vertical axis the detection probaility.

Table 3.1: Dark Count probability per gate of each Single Photon Avalance Detector of Figure 3.2

	H	V	D	A
P_{dc}	$8 \cdot 10^{-6}$	$2.9 \cdot 10^{-5}$	$6.8 \cdot 10^{-5}$	$7.0 \cdot 10^{-5}$
b	$2.8 \cdot 10^{-4}$	$1.9 \cdot 10^{-4}$	$5.0 \cdot 10^{-4}$	$9 \cdot 10^{-5}$

Table 3.2: Detection Setup parameters

Bob's optical transmittance	Bob's detector efficiency	optical misalignment
0.42	10%	$3 \cdot 10^{-3}$
Dead-time	Gating Frequency	Gate Width
$9\mu s$	$25MHz$	$5ns$

The dead-time was set to $9\mu s$ to reduce the afterpulse probability. Since the afterpulse probability depends on the light intensity received by the detectors, we observe a linear dependence of the background probability P_{bg} in terms of the transmittance η of the form $P_{bg}(\eta) = P_{dc} + b \cdot \eta$. The parameters P_{dc} and b are extracted experimentally with the linear fits shown in Figure 3.4 from test measurements and are displayed in Table 3.1. The optical misalignment is approximately $3 \cdot 10^{-3}$. The Single photon detectors were set to 10% quantum efficiency. Bob's detection system parameters are summarized in Table 3.2. Bob's optical transmittance refers to the instruments in Bob's setup i.e. the Beam Splitter, the Polarization Beam Splitters and any fiber links.

3.4 All-fiber turbulence simulator

Given the turbulence parameters (η_0, σ) we sample the set of transmittances from the probability density of the transmission coefficient (PDTC) :

$$p(\eta) = \frac{1}{\sqrt{2\pi}\sigma\eta} \text{Exp}\left[-\frac{\left(\ln(\eta/\eta_0) + \frac{\sigma^2}{2} \right)^2}{2\sigma^2} \right] \tag{3.9}$$

with η the channel transmittance and η_0 , σ the mean and variance of the distribution.

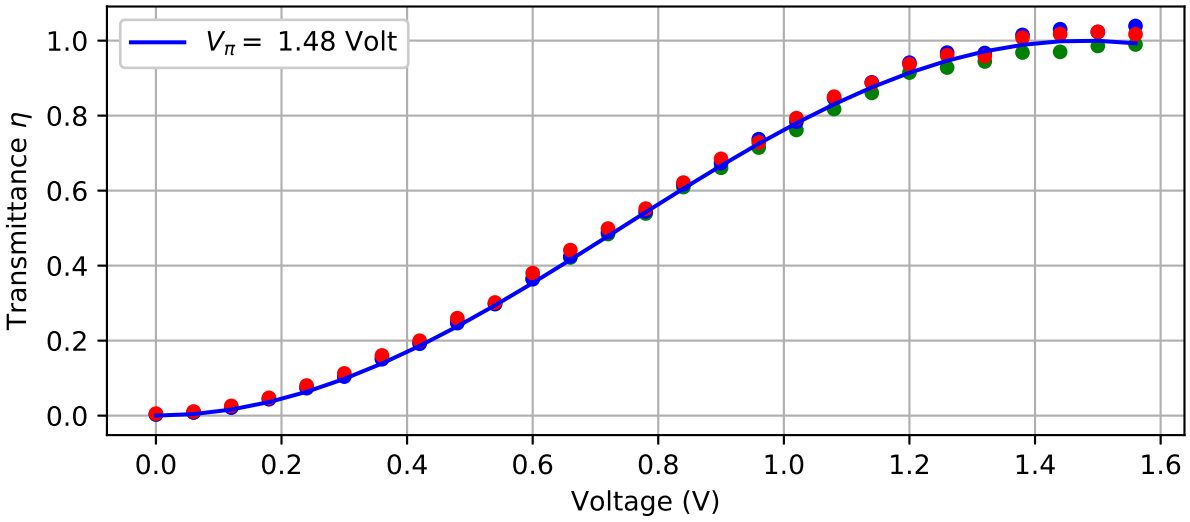

Figure 3.5: Fit to determine the modulator's V_π

With I_{in} the intensity input to the Acousto-Optical Modulator and I_{out} the output intensity, the transmittance $\eta = {}^{I_{out}}/_{I_{in}}$ produced by the Intensity Modulator is given by

$$\eta = \frac{1}{2}\left[1 + \cos\left(\frac{\pi V^{SQ}}{V\pi}\right)\right] \tag{3.10}$$

where V^{SQ} is the amplitude of the applied modulating square pulse, and V_π is a fixed parameter describing the Voltage required to introduce a π phase difference between the two arms of the modulator. The value of V_π is determined by scanning the transmittances for different amplitudes in Figure 3.5 and then fitting eq.(3.10) to the data. The fit returns $V_\pi = 1.48 Volt$.

Reversing eq.(3.10) we acquire V^{SQ} as a function of the transmittance $V^{SQ}(\eta)$ with which we map the desired transmittance values to the a modulating voltage sequence.

$$V^{SQ} = \frac{V\pi}{\pi}\cos^{-1}(2\eta - 1) \tag{3.11}$$

3.5 Experimental procedure

We calibrate the polarization basis using the alignment Polarization Controllers in Figure 3.2. We calibrate the decoy intensities using a classical detection setup to monitor the intensities and applying the appropriate attenuation. We fine-tune the optical efficiency by slightly adjusting the pulse position within the detector's gate. For each measurement we

send $N = 4 \cdot 10^{10}$ pulses which at frequency $25MHz$ require 26.7 minutes of runtime. The detection data are recorded by the Time Interval Analyser along with the SYNC signals of the decoy, polarization and turbulence sequences and a custom made program sifts them to collect the sets nX_k, mX_k, nZ_k, mZ_k for $k \in (\mu_s, \mu_w, \mu_v)$, that are needed for the secure key distillation parameters according to the model of [76]. In the previous nB_k is the set of detections where both Alice and Bob use the basis B and the decoy intensity k is used and mB_k the detections in error for the basis B and decoy k. In particular these sets produce the zero and single photon pulses contribution $s_{X,0}$ and $s_{X,1}$ the phase error ϕ_X and the total observed error in the rectilinear basis ${}^{m_X}/_{n_X}$ that are used to calculate the secure key of length ℓ,

$$\ell = \left\lfloor s_{X,0} + s_{X,1}\left(1 - h(\phi_X)\right) - n_X \cdot f_{EC} \cdot h({}^{m_X}/_{n_X}) - 6\log_2\frac{21}{\varepsilon_{sec}} - \log_2\frac{2}{\varepsilon_{cor}} \right\rfloor \tag{3.12}$$

with $f_{EC} = 1.16$ the efficiency of the classical error correction algorithm [15], $\varepsilon_{sec} = 10^{-10}$ the secrecy parameter and $\varepsilon_{cor} = 10^{-15}$ the correctness parameter. Using the previously presented experimental parameters we run an optimization algorithm to find the optimal parameters $\{q_X, P_{\mu_s}, P_{\mu_w}, \mu_s, \mu_w\}$ and program our polarization and decoy waveforms. In the previous q_X is the proportion of the rectilinear basis, P_{μ_s} and P_{μ_w} the proportions of the signal and weak decoy and μ_s, μ_w the signal and weak decoy intensities, for the desired Turbulence parameters $\{\eta_0, \sigma\}$. The details of the optimization routine are presented in Appendix B

In Figure 3.6 we present our measurement results of the error in the rectilinear basis by applying increasing transmittance thresholds, for moderate Turbulence parameters $\{\eta_0 = 10^{-1.7}, \sigma = 0.9\}$ and $\{q_X = 0.770, P_{\mu_s} = 0.548, P_{\mu_w} = 0.288, \mu_s = 0.527, \mu_w = 0.241\}$

In Figure 3.7 we present the secure key rate for different choices of transmittance cutoffs for $17db$ channel loss and $\sigma = 0.9$.

We must note that to calculate the secure key rate we need the exact number of photons per pulse for each decoy. We observed fluctuations $\lesssim 0.01$ for our signal and weak decoy states but these fluctuations are not taken into account in this study. Moreover there is an additional uncertainty in the weak decoy intensity at ~ 0.01 due to the uncertainty in the choice of the Voltage amplitude that drives the Intensity Modulator that carves the decoy pulses. Any future studies and implementations should include uncertainties and fluctuations of the intensities. A model for finite-size decoy-state QKD with fluctuating intensities can be found in Mizutani *et al.*[79].

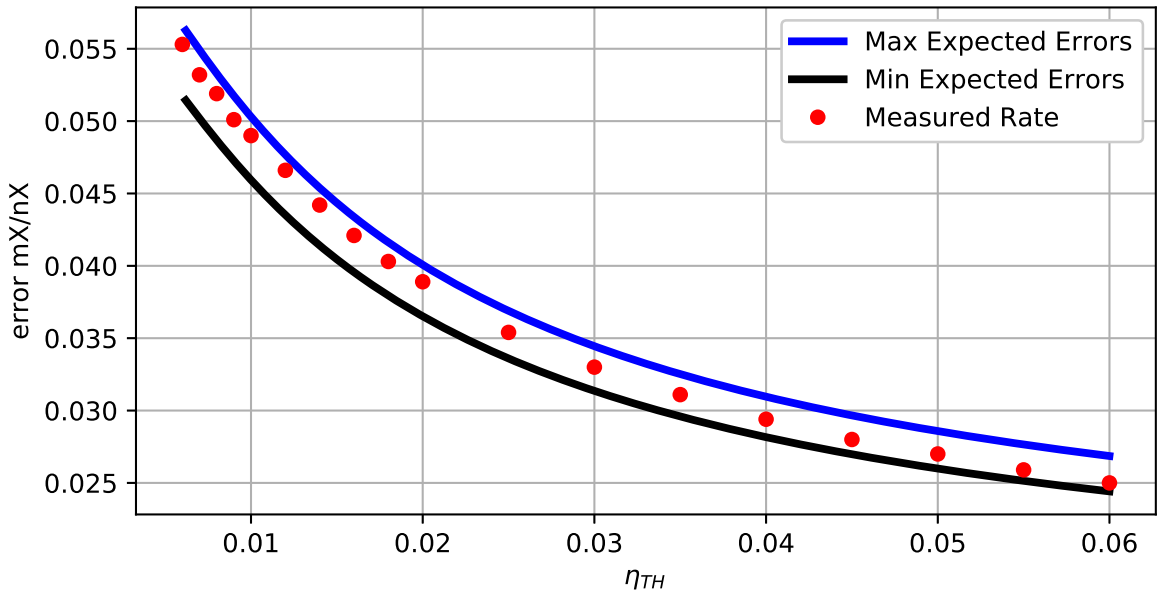

Figure 3.6: Error rate in the rectilinear basis while applying increasing transmittance cutoffs. The solid lines represent a ±5% uncertainty in Bob's detection efficiency and misalignment and background noise.

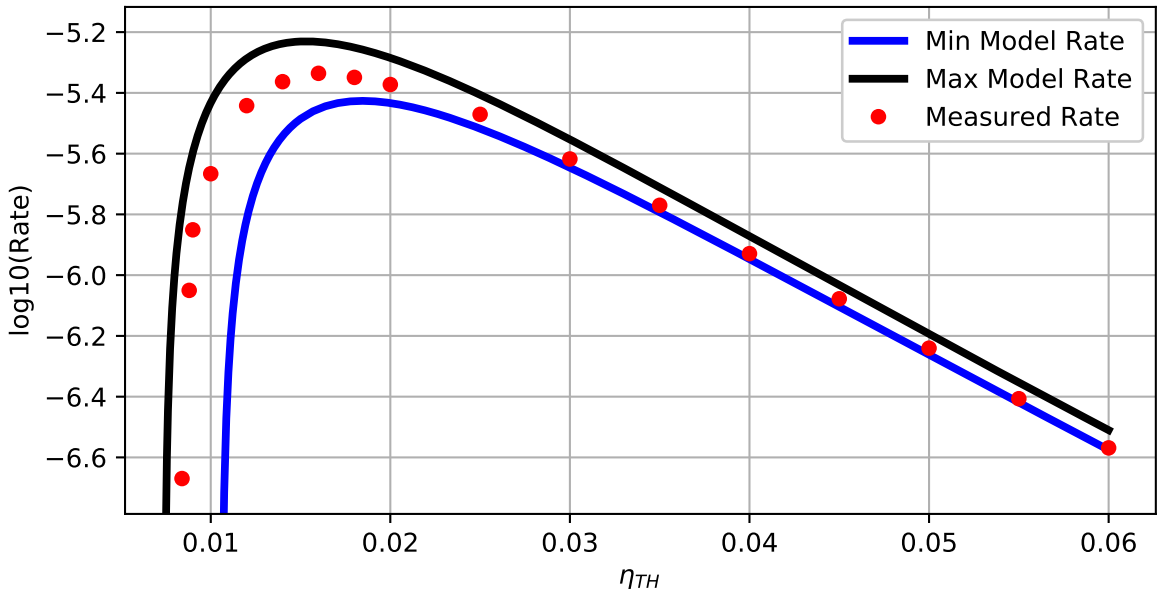

Figure 3.7: Secure Key rate at 17*db* loss, while applying increasing transmittance cutoffs. The solid lines represent a ±5% uncertainty in Bob's detection efficiency and misalignment and background noise.

3.6 Concluding remarks

In Figures 3.6 and 3.7 the benefit from applying the Selection method is clearly demonstrated. In Figure 3.6 we observe a significant reduction of the error rate among the post-selected recordings and most importantly, Figure 3.7 shows that the error decrease translates into a significant increase of the secure key generation. It is important to emphasize that without the Selection method, the key generation for the Turbulence conditions of Figure 3.7 is zero, thus creating "something out of nothing" as stated in [73]. At the optimal threshold, which according to the P-RTS method can be predetermined we generate $10^{-5.3}$ bits per pulse, so for this session a secure key of length $10^{-5.3} \times 4 \cdot 10^{10} = 200$kbits was extracted.

The Selection method can be easily implemented without any significant technological upgrades, on the contrary while saving computational resources. We observe that the Selection method is especially beneficial for lower quality detection setups i.e. lower detection efficiency and/or higher detection noise as the Turbulence impacts their Signal-to-Noise ratio more severely. We note also that the application presented in Figure 3.7 is not even the optimal. Typically Avalance detectors offer a variety of efficiency and dead-time settings. As each setting significantly impacts the background noise profile of Figure 3.4, the choice of the optimal settings becomes on its own an optimization problem. For example decreasing the dead-time, increases the gates that are available to accept an event but also increases the background noise due to afterpulses, so any benefit of decreasing the dead-time is quickly lost due to the decrease of the Signal-to-Noise ratio.

Chapter 4

Toward measurement-device independent quantum key distribution over turbulent channels; Hong-Ou-Mandel interference

This chapter presents the study on the Hong-Ou-Mandel interference in realistic implementations published in [80].

4.1 Motivation, importance of HOM interferometers

The interference of two photons in a beam splitter was first examined by Hong, Ou and Mandel [58]. As the input photons (Figure 4.1) become more and more indistinguishable in all degrees of freedom, the coincidence rate of the beam splitter output photons exhibits a characteristic dip, the depth of which depends on the degree of indistinguishability of the input photons [81]. Hong-Ou-Mandel interferometers are valuable tools in many Quantum Information and Quantum Optics applications that require photon indistinguishability. The theoretical limit for the Hong-Ou-Mandel visibility is 0.5 for indistinguishable weak coherent photon states, but several device imperfections may hinder the experimental implementation to reach this value. In this work we examine how the interference visibility is affected by (i) detector side imperfections due to after-pulses (ii) mismatches in the intensities and states of polarization of the input signals and (iii) the overall intensity of the input signals.

A convenient alternative to PDC heralded photons is using weak coherent states [82], implemented as attenuated laser light. Studies have been conducted to examine the HOM

visibility using coherent states, including the effect of the laser frequency chirp and time jitter [83, 84], the optical delay between the inputs and detection time differences [85] and the frequency mismatch [86].

Since the HOM interference can be used in experimental Bell state analysis [55, 56], it lies at the heart of Measurement Device Independent-QKD [57], discussed in section 2.5. The applicability of the protocol has been demonstrated in multiple experiments [87, 60, 88, 89]. In MDI-QKD the interference visibility significantly affects the final key generation rate [83, 89, 90]. Using coherent states instead of single photon states could open up a potential vulnerability due to the non-zero probability of multiple photon pulses but the implementation of the decoy state method [34, 29, 37] can overcome such a threat.

Wang, *et al* in [91] examine how realistic imperfections of the devices used in an HOM interference experiment affect the Visibility. In particular they consider possible imperfections on the beam splitter , mismatches in the input intensities and examine the effect of the Afterpulses when using single photon avalanche detectors. In this work we provide experimental measurements and extend the work to include possible mismatches in the state of polarization of the inputs and to examine how the overall intensity of the inputs affects the Visibility.

4.2 Parameterizing the Hong-Ou-Mandel interference visibility

The set-up for our Hong-Ou-Mandel interference measurements consists of two independent input laser pulses, interfering at a beam splitter (BS) and with each output directed to a single-photon avalanche detector (SPAD) (Figure 4.1).

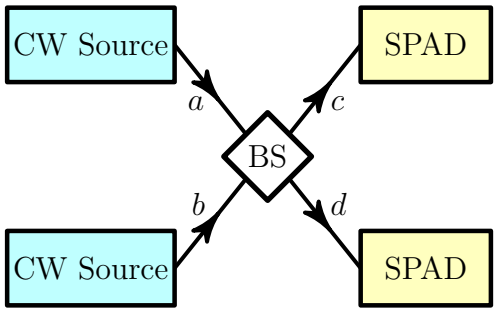

Figure 4.1: Schematic of the HOM set-up. Two weak coherent pulses enter the a and b ports of the beam splitter and interfere. Each output port (c & d) is directed to a single-photon avalanche InGaAs detector.

We model the input to the beam-splitter state as two weak coherent states:

$$|\Psi_{in}\rangle = |\alpha\rangle \otimes |\beta\rangle = e^{-\frac{\mu_a+\mu_b}{2}} e^{\alpha\hat{a}^\dagger + \beta\hat{b}^\dagger} |0\rangle \tag{4.1}$$

created by creation operators $\hat{a}^\dagger$ and $\hat{b}^\dagger$, and of parameters α and β, respectively. The coherent-state parameters are complex and include a phase, $\alpha = \sqrt{\mu_a} e^{i\theta_\alpha}$, $\beta = \sqrt{\mu_b} e^{i\theta_\beta}$, where $\mu_{a,b}$ are the corresponding average photon numbers of the two beams. In our experimental setup, the phases are randomized. Therefore, the initial state is

$$\begin{aligned} \rho_{in} &= \int_0^{2\pi} \frac{d\theta_\alpha}{2\pi} \int_0^{2\pi} \frac{d\theta_\beta}{2\pi} |\Psi_{in}\rangle\langle\Psi_{in}| \\ &= e^{-\mu_a-\mu_b} \sum_{m,n=0}^{\infty} \frac{\mu_a^m \mu_b^n}{(m!n!)^2} \left(a^\dagger\right)^m \left(b^\dagger\right)^n |0\rangle\langle 0| a^m b^n \end{aligned} \tag{4.2}$$

Nevertheless, we will continue to work with the state eq.((4.1)) and average over the phases at the end.

To account for the action of the beam splitter, we introduce a pair of orthogonal directions, named horizontal and vertical, respectively, and express the polarization vectors of the incoming beams $\hat{\varepsilon}_{a,b}$ in terms of unit vectors in the chosen directions, $\hat{\varepsilon}_{H,V}$. The creation operators are similarly expressed as linear combinations:

$$\begin{aligned} \hat{a}^\dagger &= \hat{\varepsilon}_a \cdot \hat{\varepsilon}_H \, a_H^\dagger + \hat{\varepsilon}_a \cdot \hat{\varepsilon}_V \, a_V^\dagger \\ \hat{b}^\dagger &= \hat{\varepsilon}_b \cdot \hat{\varepsilon}_H \, b_H^\dagger + \hat{\varepsilon}_b \cdot \hat{\varepsilon}_V \, b_V^\dagger \end{aligned} \tag{4.3}$$

The action of a beam splitter with reflectivity $R = r^2$ and transmissivity $T = t^2$, with $R + T = 1$, is described by the unitary transformation:

$$\begin{aligned} a_i^\dagger &\to t c_i^\dagger + r d_i^\dagger \\ b_i^\dagger &\to r c_i^\dagger - t d_i^\dagger \end{aligned} \tag{4.4}$$

where $c_i^\dagger$ and $d_i^\dagger$ are the creation operators of the respective output beams, with $i = H, V$. The input state eq.(4.1) transforms into the output state

$$\begin{aligned} |\Psi_{out}\rangle &= e^{-\frac{\mu_a+\mu_b}{2}} \\ &\quad \times \prod_{i=H,V} e^{\alpha\left(t c_i^\dagger + r d_i^\dagger\right)\hat{\varepsilon}_a \hat{\varepsilon}_i} e^{\beta\left(r c_i^\dagger - t d_i^\dagger\right)\hat{\varepsilon}_b \hat{\varepsilon}_i} |0\rangle \end{aligned} \tag{4.5}$$

Given this output state, the probability P_{mn} that m (n) photons emerge at output port c (d) is found to be (refer to Appendix A for details)

$$P_{mn}^{(out)} = e^{-\mu_c-\mu_d}\frac{\mu_c^m\mu_d^n}{m!n!} \tag{4.6}$$

where $\mu_{c,d}$ are the corresponding mean photon numbers at the two output ports of the beam splitter,

$$\begin{aligned}\mu_c &= \mu_a t^2 + \mu_b r^2 + 2tr\Re\left(\alpha\beta^*\hat{\varepsilon}_a\cdot\hat{\varepsilon}_b^*\right)\\ \mu_d &= \mu_a r^2 + \mu_b t^2 - 2tr\Re\left(\alpha\beta^*\hat{\varepsilon}_a\cdot\hat{\varepsilon}_b^*\right)\end{aligned} \tag{4.7}$$

Notice that the mean photon numbers of the beams obey the conservation law

$$\mu_a + \mu_b = \mu_c + \mu_d \tag{4.8}$$

which is a consequence of the unitarity of the beam-splitter transformation eq.(4.4), $R+T = r^2+t^2 = 1$.

Our real detectors at the two beam-splitter ports have efficiencies η_c and η_d, and dark-count probabilities d_c and d_d, respectively. Therefore the probability that the detectors click is given by

$$\begin{aligned}P_{mn} &= P_{mn}^{(out)}\\ &\quad\times(1-(1-\eta_C)^m(1-d_c))\\ &\quad\times(1-(1-\eta_D)^n(1-d_d))\end{aligned} \tag{4.9}$$

The total coincidence probability is given by

$$P^{(coin)} = \sum_{m,n=0}^{\infty} P_{mn} \tag{4.10}$$

After averaging over the phases, we obtain the total coincidence probability corresponding to the state of eq.(4.2) (details presented in Appendix A) in terms of Bessel functions:

$$\begin{aligned}P^{(coin)} &= 1 - \mathcal{C}I_0\left(2\eta_c\sqrt{\mu_a\mu_b}tr\cos\Phi\right)\\ &\quad - \mathcal{D}I_0(2\eta_d\sqrt{\mu_a\mu_b}tr\cos\Phi)\\ &\quad + \mathcal{C}\mathcal{D}I_0(2(\eta_c-\eta_d)\sqrt{\mu_a\mu_b}tr\cos\Phi)\end{aligned} \tag{4.11}$$

where

$$\mathcal{C} = e^{-\eta_c(\mu_a t^2 + \mu_b r^2)}(1 - d_c) \ ,$$
$$\mathcal{D} = e^{-\eta_d(\mu_a r^2 + \mu_b t^2)}(1 - d_d) \ , \tag{4.12}$$

and Φ is a measure of the polarization mismatch between the two incoming beams defined by

$$\cos\Phi = |\hat{\varepsilon}_a \cdot \hat{\varepsilon}_b^*| \tag{4.13}$$

The total probability that the detector at port c clicks, after averaging over phases, is also expressed similarly in terms of a Bessel function,

$$P^{(c)} = 1 - \mathcal{C} I_0(2\eta_c \sqrt{\mu_a \mu_b} tr \cos\Phi) \tag{4.14}$$

The total probability that the detector at port d clicks is found similarly:

$$P^{(d)} = 1 - \mathcal{D} I_0(2\eta_d \sqrt{\mu_a \mu_b} tr \cos\Phi) \tag{4.15}$$

The Hong-Ou-Mandel visibility is defined as

$$V_{HOM} = 1 - \frac{P^{(coin)}}{P^{(c)} P^{(d)}} \tag{4.16}$$

Using the explicit expressions (4.11), (4.14), and (4.15), we find that $V_{HOM} \in [0, 0.5]$. We aim at maximizing the value of V_{HOM}.

4.3 Experimental setup

Our experimental setup is shown on Figure 4.2. Two independent continuous wave (CW) lasers (Wavelength References) at 1550 nm were employed to prepare weak coherent states. The frequency difference between the two lasers stayed below 10 MHz without performing any feedback control. Note, in all experiments, the phase difference between the two lasers swept through a multi-2π range within the data acquisition time. This is equivalent to the phase averaging process assumed in the theoretical analysis. To generate laser pulses, two $LiNbO_3$ intensity modulators were used to modulate the outputs of the two lasers. The two intensity modulators were driven by the same digital delay generator (Stanford Research Systems) and their DC bias voltages were carefully adjusted to achieve high extinction ratios.

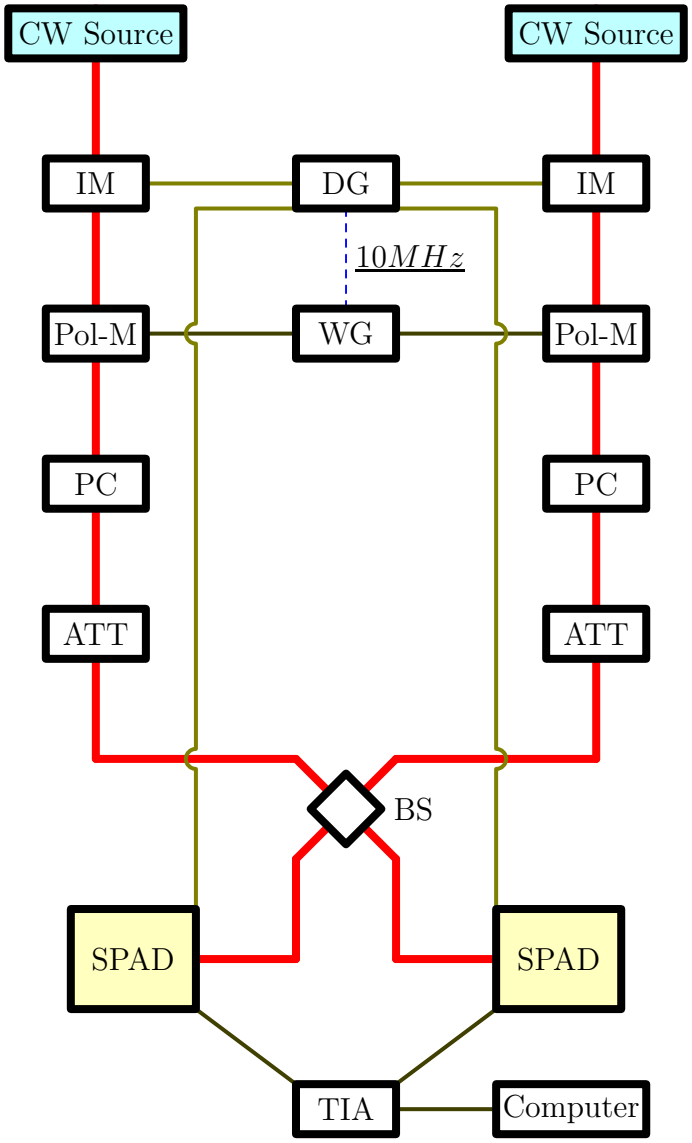

Figure 4.2: Schematic of the experimental setup.

The polarization state of each pulse can be randomly changed with a home-made high-speed polarization modulator, which is driven by a Keysight Waveform Generator (WG) . Details about the polarization modulator can be found in [77]. Once the polarization is applied to the pulse, it passes through a beam circulator and enters free space. Upon returning to fiber, the pulses enter an additional polarization controller where HOM visibility is fine-tuned prior to data collection. The pulse is then digitally attenuated in order to reach the single-photon level to interfere at the beam splitter and be read by single-photon avalanche detectors (SPAD). The detectors are both IdQuantique 210 with one being an ultra-low noise model run in gated mode. Timestamps of detection events are recorded on a time-interval analyzer (TIA) with a resolution of 80.9576 ps.

4.4 Results

Here we report on our experimental results. We examine how the HOM Visibility is affected by the after-pulse effect and by various imperfections in the source preparation.

HOM visibility and detector imperfections

We consider the effect on HOM visibility due to detector imperfections. Ref. [91] highlights the after-pulse effect as a significant source of error in an experimental implementation of the HOM interference. The authors of [91] employed a non-Markovian model and showed that the coincidence probability, after considering the after-pulse effect, can be written as:

$$P^{(coin;aft)} = P^{(coin)} + \left[P^{(c)} - P^{(coin)}\right] P^{(d)} P_d^{(total;aft)} + \left[P^{(d)} - P^{(coin)}\right] P^{(c)} P_c^{(total;aft)} \quad (4.17)$$

where $P^{(coin)}$ is the coincidence probability given by eq.(4.17), and $P^{(c)}$, $P^{(d)}$ are the detection probabilities for the detectors at ports c and d, respectively, given by eq.(4.14) and eq.(4.15). In eq.(4.17), $P_c^{(total;aft)}$ and $P_d^{(total;aft)}$, describe the total after-pulse probability for each detector. We assume that the after-pulse probability decays with time as a simple exponential $P(t) = P_0 \cdot e^{-t/\tau}$, with P_0 the initial after-pulse probability and τ the characteristic decay time. In gated mode the total after-pulse probability, receives contributions only when the gate is open:

$$\begin{aligned} P^{(total;aft)} &= P(T_{dt}) + P(T_{dt} + T_{gat}) + \dots \\ &= P_0 \frac{e^{-T_{dt}/\tau}}{1 - e^{-T_{gat}/\tau}} \end{aligned} \quad (4.18)$$

with T_{dt} the detector dead time and T_{gat} the gating period. Probabilities $P^{(c)}$ and $P^{(d)}$ of eq.(4.14) and eq.(4.15) are similarly modified as,

$$P^{(c,aft)} = P^{(c)}\left[1 + (1 - P^{(c)})P_c^{(total;aft)}\right] \tag{4.19}$$

$$P^{(d,aft)} = P^{(d)}\left[1 + (1 - P^{(d)})P_d^{(total;aft)}\right] \tag{4.20}$$

With eq.(4.18) we can relate the HOM visibility with the dead time settings on our detectors. First, we need to determine the parameters P_0 and experimentally. We follow the procedure described in [92] and collect histograms of detection events binned into time intervals between successive detection events. By fitting the logarithm of the frequencies with equation (6) in [92] we extract the parameters P_0 and τ experimentally. For our first run the gating and pulse frequency was set to $2MHz$. The detection histograms presented in Figure 4.3 gave the values $P_0^C = 0.018$ and $\tau_C = 0.85\mu s$ for detector C, and $P_0^D = 0.033$ and $\tau_D = 1.41\mu s$ for detector D.

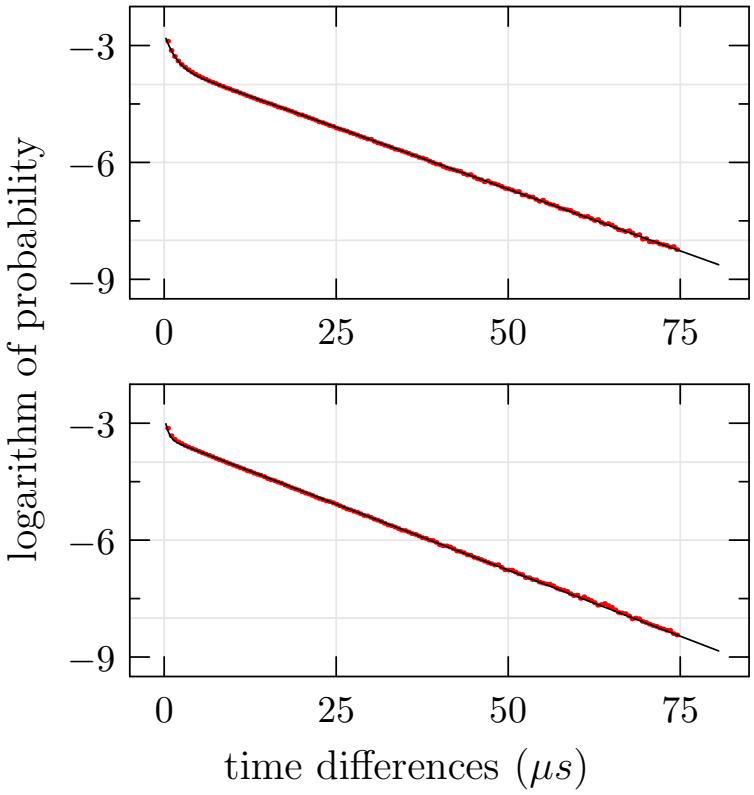

Figure 4.3: Histograms of the detection probability. The fits are used to extract the total afterpulse Probability for each detector.

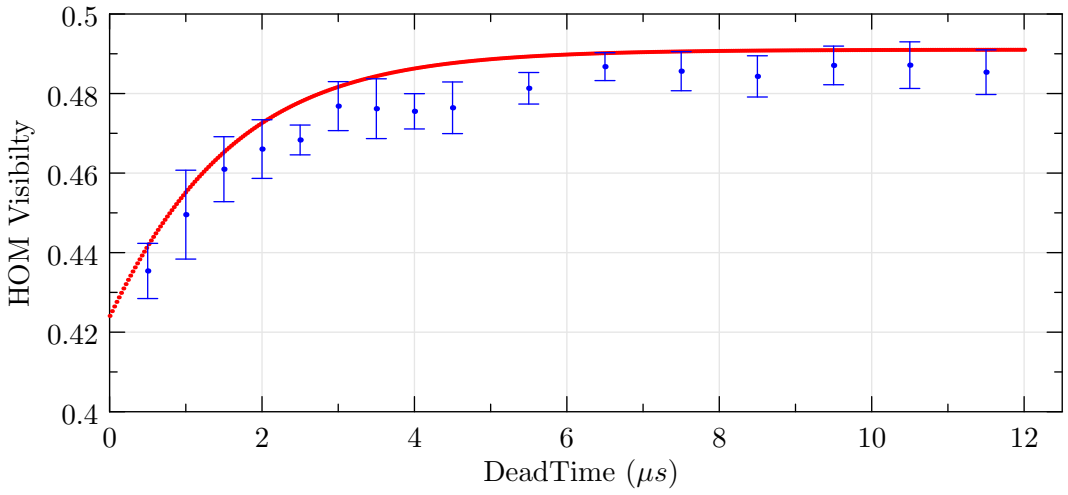

Figure 4.4: HOM Visibility vs the applied Dead-time

A measurement of the HOM Visibility was then performed. The pulse width was set to 2 ns and the gate width at nominal width of 7 ns. Each of these widths can be changed by about 10% without appreciable change in the reported results. The dark counts were recorded for the two detectors at 10^{-4} and 4×10^{-5} per gate, respectively while the dead time was set to $0.1\mu s$. Increasing the dead time further decreased the dark counts. In Fig. 4.4, the measurement results are presented in comparison to our model showing good agreement.

Source effects on HOM visibility

By lowering the total input intensity, the HOM visibility is improved. However, reaching very low intensities may render the experiment vulnerable to dark counts, and increases the required time to perform a measurement. This in turn renders the experiment vulnerable to various drifts (e.g., the drift in the state of polarization, or in the DC offset of the modulators). We examined the effect of the overall input intensity on the HOM visibility. Setting the intensities of the input beams equal, $\mu_a = \mu_b = \mu$ in eq.(4.10), eq.(4.14), and eq.(4.15), we studied the dependence of the HOM visibility on the average input photon number μ. Theoretically, the HOM visibility approaches the limit value 0 at large input intensities, whereas it approaches the maximum value 0.5 at weak intensities.

In our measurements, we used $2-ns$ width pulses. Our detectors were running in external gating mode at $1-MHz$ trigger frequency with an effective gate width of approximately $3ns$ (nominal gate width set to $7ns$) and 10% efficiency. The dark counts of the two detectors were recorded approximately as 2.5×10^{-5} and 1.5×10^{-5} per gate, respectively. The dead time

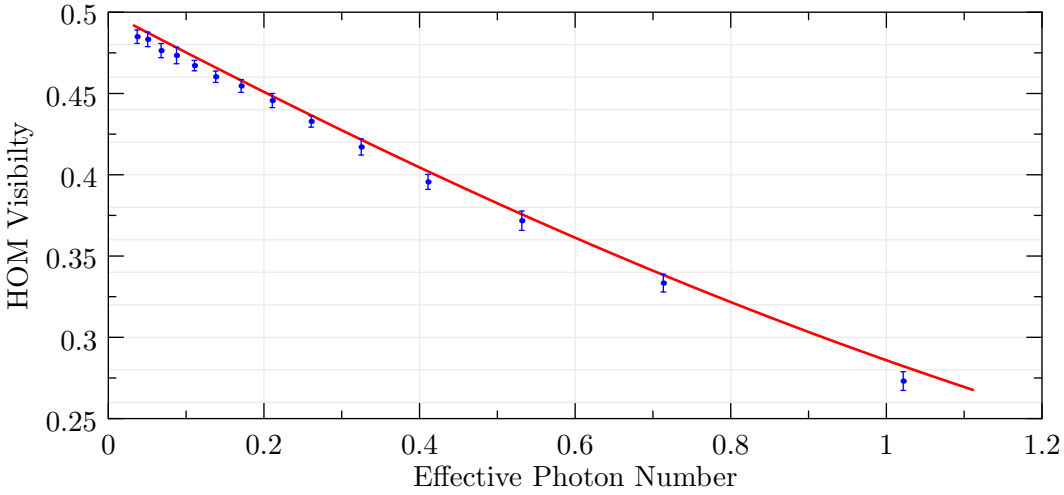

Figure 4.5: H.O.M. Visibility vs the effective photon number each pulse contains.

on the detectors was set to $7\mu s$ (a longer dead time does not change the results appreciably). To make sure that the beam-splitter inputs were equal, the free-space path of one arm was blocked, and the intensity of the unblocked armed was digitally attenuated until the detection rate reached the desired value. The average photon-number input to the beam splitter is related to the observed detection rate by

$$\mu = \frac{2}{\eta} \ln \left(\frac{1 - R_{det} T_{dt} + R_{det} T_{gat}}{1 - R_{det} T_{det}} \right) \tag{4.21}$$

where η is the detector efficiency, R_{det} is the detector rate of each unblocked input, T_{dt} is the dead time, and T_{gat} is the gating period. The factor of 2 in eq.(4.21) accommodates the intensity splitting at the 50 : 50 beam splitter. In Fig. 4.5, the measurement results of the HOM visibility as a function of the input photon number are presented and compared with the theoretical model (calculated using eq.(4.10), (4.14), and (4.15)), showing good agreement between theory and experiment.

Next, we consider the effect of imperfections in input state preparationon the HOM visibility.

In a realistic experimental setup, two independent laser beams are independently attenuated. In practice, perfect intensity balance may be not possible. Using eq.(4.10), (4.14), and (4.15), we can model the HOM visibility theoretically as a function of the ratio of the input photon numbers μ_a/μ_b.

For our measurements, the dead time for each detector was set to $7\mu s$ with efficiency 10%. Each free-space arm was blocked for either Alice/Bob between data points to record detector

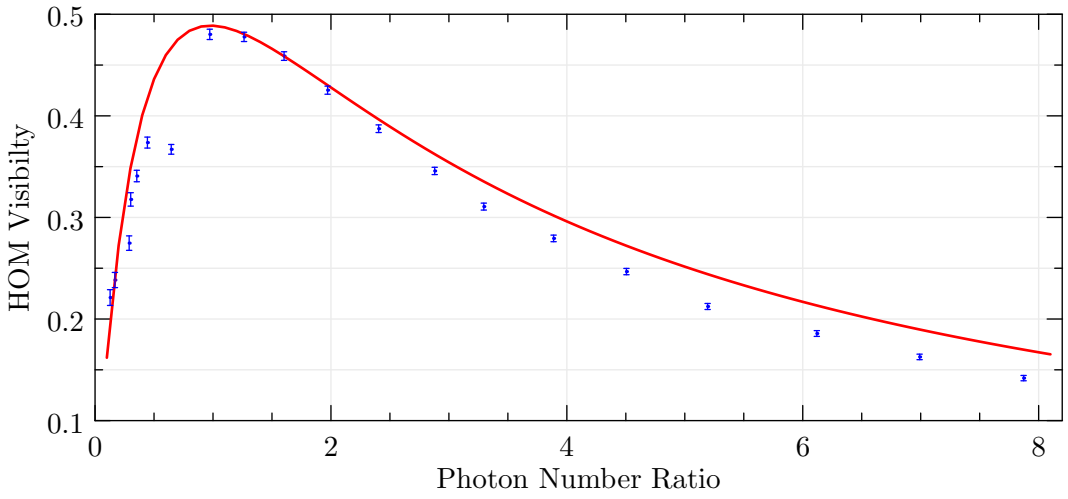

Figure 4.6: H.O.M. vs the Intensity Mismatch between the incoming pulses.

count-rates. The count rates were controlled via digital attenuation and set to desired values to within 2%. From the detector count-rates and using formula (4.21), the photon number can be extracted for each count-rate. In this measurement the photon number for the input arm at port α was fixed at $\mu_a = 0.47$, while varying the attenuation on the input at port digitally. We sent weak coherent pulses at 1 MHz with pulse widths of $2ns$ through the beam splitter and to our detectors. Each detector's gate width was approximately $7ns$ to mitigate the detection of background source photons outside the intended pulse width. In Fig. 4.6, the measurement results of the HOM visibility as a function of the ratio of input photon numbers are plotted with the theoretical model (eq.(4.10), (4.14), and (4.15)), showing good agreement.

Next, we consider the effect of the polarization misalignment of the incoming beams on the HOM visibility. Equations (4.10), (4.14), and (4.15) show the dependence of the HOM visibility on the polarization misalignment Φ in eq.(4.13). Assuming that the bases of the two inputs are perfectly aligned, we can write the polarization vectors $\hat{\varepsilon}_a$ and $\hat{\varepsilon}_b$ in terms of the transverse-electric (TE) and transverse-magnetic (TM) modes of the phase modulator's waveguide as:

$$\begin{aligned} \hat{\varepsilon}_a &= \cos\phi_a \left|TE\right\rangle + \sin\phi_a e^{\imath\phi_0} \left|TM\right\rangle \\ \hat{\varepsilon}_b &= \cos\phi_b \left|TE\right\rangle + \sin\phi_b e^{\imath\phi_0} e^{\imath\phi_M} \left|TM\right\rangle \end{aligned} \tag{4.22}$$

where $\phi_M = \frac{V_g}{V_\pi}\pi$ is the modulation phase caused by the driving generator, V_g is the voltage applied by the generator, and V_π is the constant voltage that causes a π phase shift. Using a

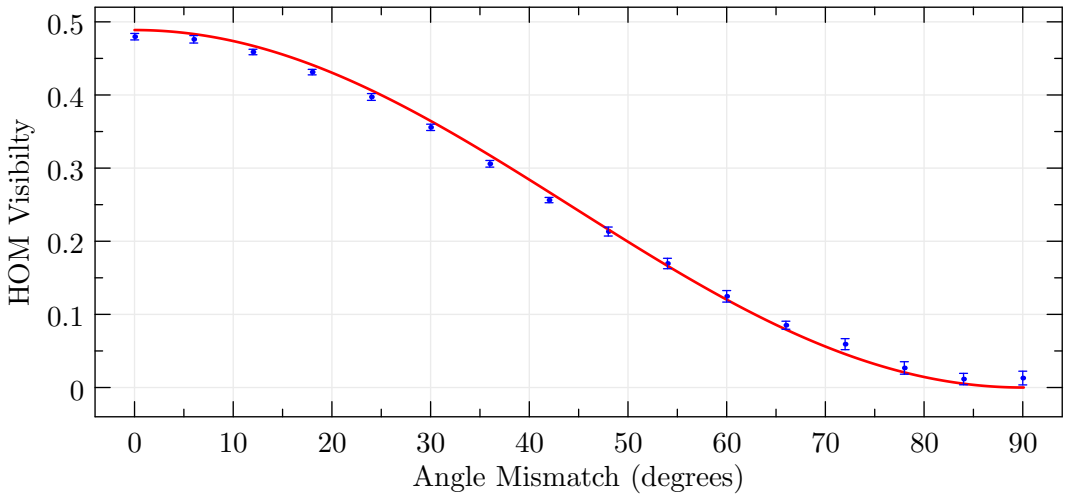

Figure 4.7: H.O.M. Visibility vs the mismatch in the Polarization of the icoming pulses.

manual polarization controller we carefully arrange the input to the waveguide to be at 45° with respect to the waveguide's axis, so $\cos\phi_a = \cos\phi_b = \frac{1}{\sqrt{2}}$. The polarization misalignment angle Φ eq. (4.13) can then be related to the applied voltage as:

$$\cos\Phi = |\hat{\varepsilon}_a \cdot \hat{\varepsilon}_b^*| = \cos\frac{\pi V_g}{2V_\pi} \tag{4.23}$$

For our measurements, we controlled the state of polarization using the Polarization Modulation set-up described in [78]. We used a Keysight waveform generator to drive an EOSpace Phase Modulator. The V_π voltage of the phase modulator was determined to be 5.25 V. Pulses of width $2.1ns$ and average photon number $\mu = 0.45 \pm 0.05$ interfered at a 50 : 50 beam splitter. The outputs were directed to two SPADs operated at free-gated mode at $\sim 10\%$ efficiency with gate period 1 μs, dead time set at 7.5 μs, and gate width of $6.5ns$. The dark counts were recorded approximately 5.5×10^{-5} and 2.0×10^{-5} per gate, respectively. The coincidence window was set at $5ns$. Plot in Fig. 4.7.

4.5 Discussion

In this work, we parametrized the Hong-Ou-Mandel interference visibility in terms of realistic imperfections that may appear in experimental implementations using weak coherent states. We examined the effect of mismatches in the state of polarization and intensities of the inputs. We also considered imperfections on the detector side resulting from the detector's after pulses as well as the effect of the overall intensity of otherwise perfect sources. We

conducted measurements that resulted in experimental data that agreed very well with our theoretical models. In conclusion, good Hong-Ou-Mandel interference visibility is attainable using standard commercially available optical components and single-photon detectors. We conclude that the after-pulse effect can be effectively mitigated by applying a dead time $6 - 8\mu s$, when the detectors are triggered at a few-MHz frequencies. Realistic intensity imbalances were less than 10% and they have minimal impact on the measured HOM visibility. For example, the HOM visibility is expected to be 0.489 for $\mu_a = \mu_b = 0.45$. A realistic imbalance $\mu_a = 0.45$ and $\mu_b = 0.50$ would decrease the visibility to just 0.487. Some extra care should be taken when adjusting the state of polarization for the two arms. Assuming $\mu_a = \mu_b = 0.45$, while a 0° misalignment gives a visibility of 0.489, a 6° misalignment gives a visibility of 0.483. Given that manual polarization controllers can achieve typical extinction ratios 20-30 dB [93], a misalignment of that order should be expected. We identify the state of polarization misalignment as the major source of error in the measurements we present in this work. We finally discussed how the HOM visibility is affected by the overall input intensity aiming to achieve efficient intensities for practical measurements while remaining in the quantum regime.

Chapter 5

Future extensions of this work

5.1 P-RTS method for the MDI-QKD protocol

In Chapter 3 we successfully demonstrate the P-RTS method for the BB84 protocol, while in Chapter 4 our extensive study on the H.O.M. interference reaffirms the applicability of the MDI-QKD protocol in realistic implementations. An immediate extension is the implementation of the selection method for the MDI-QKD protocol, which could be very beneficial for remote communicating parties that need to securely communicate utilizing untrusted relays such satellites. For realistic applications we need to assume finite resources for the communicating parties and consider finite-size effects to the secure key distillation [94]. Figure 5.1 depicts the schematic of a possible experimental demonstration.

5.2 Quantum position verification

The need to verify that an untrusted party (someone with no credentials), which can be a potential communicating partner or a measurement relay, is indeed at a particular geographical location can be included in general communication schemes. A successful position verification can be included as a prerequisite to other cryptographic tasks such as authentication and key distribution. A classical position verification scheme would require the prover, the party whose position needs to be verified, to interactively communicate with a set of a verifiers. As the verifiers can communicate privately among themselves the can compare their results and pinpoint the position of the prover. In the quantum version of the scheme [95], the verifiers send independently a quantum state and the classical information about the appropriate measurement basis. Two colluding eavesdroppers could try to pose as the legitimate prover, one intercepts the classical basis information and the other performs

the quantum measurement. The verifiers can defend by designing the scheme in a way that the eavesdropper intercepting the basis information cannot inform his partner in time to perform his measurement. This defence can be demonstrated experimentally with a setup similar to the our current BB84 experiment.

5.3 Reconfigurable QKD

Despite offering an exceptional balance between security and efficiency, MDI-QKD is surely less efficient the BB84 QKD protocol since it requires coinciding detection events which scale as the square of the detector's efficiency. Furthermore for free space applications, turbulence may hinder the synchronization of the arrival time of the independent pulses, further reducing the efficiency of MDIQKD. Reconfigurable QKD [96, 97] proposes an adaptive setup where the parties switch between the two protocols depending on the degree of confidence they have on their channel's security.

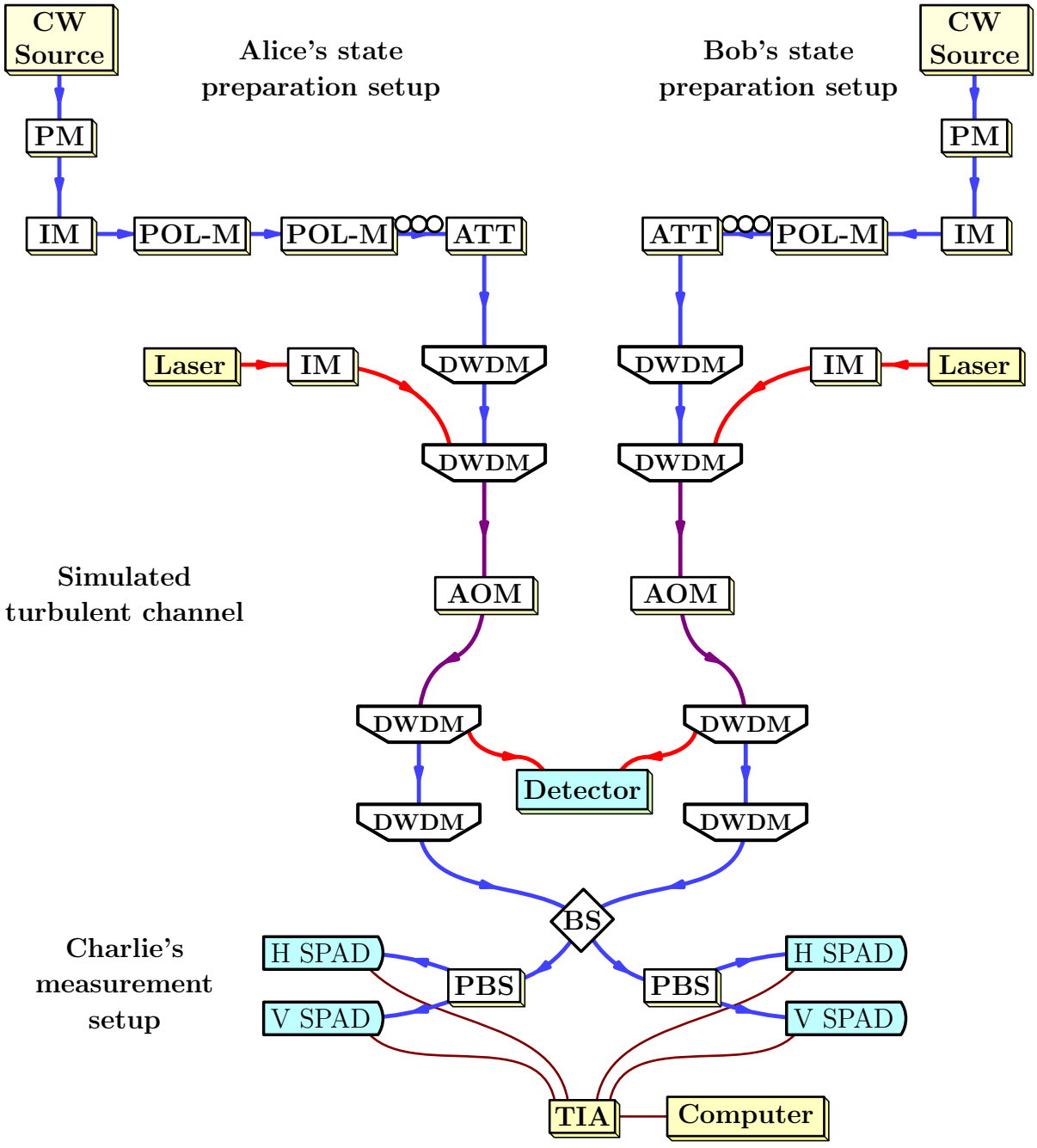

Figure 5.1: Schematic for implementing the demonstration of the P-RTS method for the MDI-QKD protocol using all fiber Turbulence simulators

Bibliography

[1] Simon Singh. *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography*. Doubleday, New York, NY, USA, 1st edition, 1999. 1

[2] Jean-Philippe Aumasson. *Serious Cryptography: A Practical Introduction to Modern Encryption*. No Starch Press, San Francisco, CA, USA, 2017. 2

[3] Ralph C. Merkle. Secure communications over insecure channels. *Commun. ACM*, 21(4):294–299, April 1978. 5

[4] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, November 1976. 5

[5] Chae Hoon Lim and Pil Joong Lee. A key recovery attack on discrete log-based schemes using a prime order subgroup. In Burton S. Kaliski, editor, *Advances in Cryptology — CRYPTO '97*, pages 249–263, Berlin, Heidelberg, 1997. Springer Berlin Heidelberg. 5

[6] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, February 1978. 6

[7] Dan Boneh et al. Twenty years of attacks on the rsa cryptosystem. *Notices of the AMS*, 46(2):203–213, 1999. 6

[8] Dan Boneh, Richard A. DeMillo, and Richard J. Lipton. On the importance of eliminating errors in cryptographic computations. *Journal of Cryptology*, 14(2):101–119, Mar 2001. 6

[9] David Brumley and Dan Boneh. Remote timing attacks are practical. In *Proceedings of the 12th Conference on USENIX Security Symposium - Volume 12*, SSYM'03, pages 1–1, Berkeley, CA, USA, 2003. USENIX Association. 6

[10] Victor S. Miller. Use of elliptic curves in cryptography. In Hugh C. Williams, editor, *Advances in Cryptology — CRYPTO '85 Proceedings*, pages 417–426, Berlin, Heidelberg, 1986. Springer Berlin Heidelberg. 6

[11] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177):203–203, January 1987. 6

[12] C. E. Shannon. Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656–715, Oct 1949. 7

[13] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, Nov 1994. 7

[14] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, 2014. 8, 30

[15] Gilles Brassard and Louis Salvail. Secret-key reconciliation by public discussion. In Tor Helleseth, editor, *Advances in Cryptology — EUROCRYPT '93*, pages 410–423, Berlin, Heidelberg, 1994. Springer Berlin Heidelberg. 8, 39

[16] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6):1915–1923, Nov 1995. 9

[17] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Rev. Mod. Phys.*, 86:419–478, Apr 2014. 9, 11

[18] J. S. Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1:195–200, Nov 1964. 9

[19] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, Oct 1969. 10, 24

[20] B. M. Terhal. Is entanglement monogamous? *IBM Journal of Research and Development*, 48(1):71–78, Jan 2004. 11

[21] Valerie Coffman, Joydip Kundu, and William K. Wootters. Distributed entanglement. *Phys. Rev. A*, 61:052306, Apr 2000. 11

[22] Tobias J. Osborne and Frank Verstraete. General monogamy inequality for bipartite qubit entanglement. *Phys. Rev. Lett.*, 96:220503, Jun 2006. 11

[23] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991. 11, 24

[24] Antonio Acín, Serge Massar, and Stefano Pironio. Efficient quantum key distribution secure against no-signalling eavesdroppers. *New Journal of Physics*, 8(8):126–126, aug 2006. 11

[25] Charles H. Bennett, Gilles Brassard, and N. David Mermin. Quantum cryptography without bell's theorem. *Phys. Rev. Lett.*, 68:557–559, Feb 1992. 12

[26] Eli Biham, Bruno Huttner, and Tal Mor. Quantum cryptographic network based on quantum memories. *Phys. Rev. A*, 54:2651–2658, Oct 1996. 12, 25

[27] Inamori. Security of practical time-reversed epr quantum key distribution. *Algorithmica*, 34(4):340–365, Nov 2002. 13, 25

[28] Daniel Gottesman, Hoi-Kwong Lo, Norbert Ltkenhaus, and John Preskill. Security of quantum key distribution with imperfect devices. 2002. 16, 18, 31

[29] Hoi-Kwong Lo and John Preskill. Phase randomization improves the security of quantum key distribution, 2005. 17, 43

[30] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C. Sanders. Limitations on practical quantum cryptography. *Phys. Rev. Lett.*, 85:1330–1333, Aug 2000. 17

[31] Norbert Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A*, 61:052304, Apr 2000. 17

[32] Norbert Ltkenhaus and Mika Jahma. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. *New Journal of Physics*, 4:44–44, jul 2002. 17

[33] John Calsamiglia, Stephen M. Barnett, and Norbert Lütkenhaus. Conditional beam-splitting attack on quantum key distribution. *Phys. Rev. A*, 65:012312, Dec 2001. 18

[34] Won-Young Hwang. Quantum Key Distribution with High Loss: Toward Global Secure Communication. *Phys. Rev. Lett.*, 91:057901, Aug 2003. 19, 43

[35] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy State Quantum Key Distribution. *Phys. Rev. Lett.*, 94:230504, Jun 2005. 19, 20

[36] Xiang-Bin Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.*, 94:230503, Jun 2005. 19

[37] Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo. Practical decoy state for quantum key distribution. *Phys. Rev. A*, 72:012326, Jul 2005. 19, 20, 43, 74

[38] Bing Qi, Chi-Hang Fred Fung, Hoi-Kwong Lo, and Xiongfeng Ma. Time-shift attack in practical quantum cryptosystems. *arXiv e-prints*, pages quant–ph/0512080, Dec 2005. 22

[39] Yi Zhao, Chi-Hang Fred Fung, Bing Qi, Christine Chen, and Hoi-Kwong Lo. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A*, 78:042333, Oct 2008. 22

[40] Chi-Hang Fred Fung, Bing Qi, Kiyoshi Tamaki, and Hoi-Kwong Lo. Phase-remapping attack in practical quantum-key-distribution systems. *Phys. Rev. A*, 75:032314, Mar 2007. 22

[41] Feihu Xu, Bing Qi, and Hoi-Kwong Lo. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New Journal of Physics*, 12(11):113026, nov 2010. 22

[42] Vadim Makarov, Andrey Anisimov, and Johannes Skaar. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A*, 74:022313, Aug 2006. 22

[43] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*, 4:686 EP –, Aug 2010. 23

[44] Sebastien Sauge, Lars Lydersen, Andrey Anisimov, Johannes Skaar, and Vadim Makarov. Controlling an actively-quenched single photon detector with bright light. *Opt. Express*, 19(23):23590–23600, Nov 2011. 23

[45] Ilja Gerhardt, Qin Liu, Antía Lamas-Linares, Johannes Skaar, Christian Kurtsiefer, and Vadim Makarov. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nature Communications*, 2:349 EP –, Jun 2011. Article. 23

[46] C Wiechers, L Lydersen, C Wittmann, D Elser, J Skaar, Ch Marquardt, V Makarov, and G Leuchs. After-gate attack on a quantum cryptosystem. *New Journal of Physics*, 13(1):013043, jan 2011. 23

[47] Henning Weier, Harald Krauss, Markus Rau, Martin Frst, Sebastian Nauerth, and Harald Weinfurter. Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors. *New Journal of Physics*, 13(7):073024, jul 2011. 24

[48] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, 98:230501, Jun 2007. 24

[49] Stefano Pironio, Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11(4):045021, apr 2009. 24, 25

[50] Nicolas Gisin, Stefano Pironio, and Nicolas Sangouard. Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier. *Phys. Rev. Lett.*, 105:070501, Aug 2010. 24

[51] Lluís Masanes, Stefano Pironio, and Antonio Acín. Secure device-independent quantum key distribution with causally independent measurement devices. *Nature Communications*, 2:238 EP –, Mar 2011. Article. 24

[52] Marcos Curty and Tobias Moroder. Heralded-qubit amplifiers for practical device-independent quantum key distribution. *Phys. Rev. A*, 84:010304, Jul 2011. 24

[53] Umesh Vazirani and Thomas Vidick. Fully device-independent quantum key distribution. *Phys. Rev. Lett.*, 113:140501, Sep 2014. 24

[54] Philip M. Pearle. Hidden-variable example based upon data rejection. *Phys. Rev. D*, 2:1418–1425, Oct 1970. 25

[55] H. Weinfurter. Experimental bell-state analysis. *EPL (Europhysics Letters)*, 25(8):559, 1994. 25, 43

[56] Markus Michler, Klaus Mattle, Harald Weinfurter, and Anton Zeilinger. Interferometric bell-state analysis. *Phys. Rev. A*, 53:R1209–R1212, Mar 1996. 25, 43

[57] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.*, 108(13):130503, mar 2012. 25, 30, 43

[58] C. K. Hong, Z. Y. Ou, and L. Mandel. Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.*, 59:2044–2046, Nov 1987. 26, 42

[59] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger. Field test of quantum key

distribution in the tokyo qkd network. *Opt. Express*, 19(11):10387–10409, May 2011. 29

[60] Yan-Lin Tang, Hua-Lei Yin, Qi Zhao, Hui Liu, Xiang-Xiang Sun, Ming-Qi Huang, Wei-Jun Zhang, Si-Jing Chen, Lu Zhang, Li-Xing You, Zhen Wang, Yang Liu, Chao-Yang Lu, Xiao Jiang, Xiongfeng Ma, Qiang Zhang, Teng-Yun Chen, and Jian-Wei Pan. Measurement-device-independent quantum key distribution over untrustful metropolitan network. *Phys. Rev. X*, 6:011024, Mar 2016. 29, 43

[61] Christoph Simon. Towards a global quantum network. *Nature Photonics*, 11(11):678–680, 2017. 29

[62] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982. 29

[63] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication. *Phys. Rev. Lett.*, 81:5932–5935, Dec 1998. 29

[64] Sebastian Nauerth, Florian Moll, Markus Rau, Christian Fuchs, Joachim Horwath, Stefan Frick, and Harald Weinfurter. Air-to-ground quantum communication. *Nature Photonics*, 7:382 EP –, Mar 2013. 29

[65] Jian-Yu Wang, Bin Yang, Sheng-Kai Liao, Liang Zhang, Qi Shen, Xiao-Fang Hu, Jin-Cai Wu, Shi-Ji Yang, Hao Jiang, Yan-Lin Tang, Bo Zhong, Hao Liang, Wei-Yue Liu, Yi-Hua Hu, Yong-Mei Huang, Bo Qi, Ji-Gang Ren, Ge-Sheng Pan, Juan Yin, Jian-Jun Jia, Yu-Ao Chen, Kai Chen, Cheng-Zhi Peng, and Jian-Wei Pan. Direct and full-scale experimental verifications towards ground-satellite quantum key distribution. *Nature Photonics*, 7:387 EP –, Apr 2013. Article. 29

[66] Hua-Ying Liu, Xiao-Hui Tian, Changsheng Gu, Pengfei Fan, Xin Ni, Ran Yang, Ji-Ning Zhang, Mingzhe Hu, Yang Niu, Xun Cao, Xiaopeng Hu, Gang Zhao, Yan-Qing Lu, Zhenda Xie, Yan-Xiao Gong, and Shi-Ning Zhu. Drone-based all-weather entanglement distribution, 2019. 29

[67] W. Vogel D. Vasylyev, A. A. Semenov. Characterization of free-space quantum channels, 2018. 30

[68] Peter W Milonni, John H Carter, Charles G Peterson, and Richard J Hughes. Effects of propagation through atmospheric turbulence on photon statistics. *Journal of Optics B: Quantum and Semiclassical Optics*, 6(8):S742—-S745, jul 2004. 30

[69] Ivan Capraro, Andrea Tomaello, Alberto Dall'Arche, Francesca Gerlin, Ruper Ursin, Giuseppe Vallone, and Paolo Villoresi. Impact of Turbulence in Long Range Quantum and Classical Communications. *Phys. Rev. Lett.*, 109:200502, Nov 2012. 30

[70] D. Vasylyev, A. A. Semenov, and W. Vogel. Atmospheric quantum channels with weak and strong turbulence. *Phys. Rev. Lett.*, 117:090501, Aug 2016. 30

[71] C Erven, B Heim, E Meyer-Scott, J P Bourgoin, R Laflamme, G Weihs, and T Jennewein. Studying free-space transmission statistics and improving free-space quantum key distribution in the turbulent atmosphere. *New Journal of Physics*, 14(12):123018, dec 2012. 30

[72] Giuseppe Vallone, Davide G. Marangon, Matteo Canale, Ilaria Savorgnan, Davide Bacco, Mauro Barbieri, Simon Calimani, Cesare Barbieri, Nicola Laurenti, and Paolo Villoresi. Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels. *Phys. Rev. A*, 91:042320, Apr 2015. 30

[73] Wenyuan Wang, Feihu Xu, and Hoi-Kwong Lo. Prefixed-threshold real-time selection method in free-space quantum key distribution. *Phys. Rev. A*, 97:032337, Mar 2018. 30, 31, 32, 41

[74] Zhuo-Dan Zhu, Dong Chen, Shang-Hong Zhao, Qin-Hui Zhang, and Jun-Hua Xi. Real-time selection for free-space measurement device independent quantum key distribution. *Quantum Information Processing*, 18(1):33, dec 2018. 30

[75] Poompong Chaiwongkhot, Katanya B. Kuntz, Yanbao Zhang, Anqi Huang, Jean-Philippe Bourgoin, Shihan Sajeed, Norbert Ltkenhaus, Thomas Jennewein, and Vadim Makarov. A hacker's guide to attacking a free-space quantum key distribution receiver in atmospheric turbulence, 2019. 30

[76] Charles Ci Wen Lim, Marcos Curty, Nino Walenta, Feihu Xu, and Hugo Zbinden. Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A*, 89:022307, Feb 2014. 33, 39, 73, 74

[77] Zhiyuan Tang, Zhongfa Liao, Feihu Xu, Bing Qi, Li Qian, and Hoi-Kwong Lo. Experimental Demonstration of Polarization Encoding Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.*, 112:190503, May 2014. 33, 48

[78] I Lucio-Martinez, P Chan, X Mo, S Hosier, and W Tittel. Proof-of-concept of real-world quantum key distribution with quantum frames. *New Journal of Physics*, 11(9):95001, 2009. 33, 53

[79] Akihiro Mizutani, Marcos Curty, Charles Ci Wen Lim, Nobuyuki Imoto, and Kiyoshi Tamaki. . *New Journal of Physics*, 17(9):093011, sep 2015. 39

[80] E. Moschandreou, J. I. Garcia, B. J. Rollick, B. Qi, R. Pooser, and G. Siopsis. Experimental study of hongoumandel interference using independent phase randomized weak coherent states. *Journal of Lightwave Technology*, 36(17):3752–3759, Sep. 2018. 42

[81] A. M. Brańczyk. Hong-Ou-Mandel Interference. *ArXiv e-prints*, Oct 2017. 42

[82] J G Rarity, P R Tapster, and R Loudon. Non-classical interference between independent sources. *Journal of Optics B: Quantum and Semiclassical Optics*, 7(7):S171, 2005. 42

[83] Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Fröhlich, M. B. Ward, and A. J. Shields. Interference of short optical pulses from independent gain-switched laser diodes for quantum secure communications. *Phys. Rev. Applied*, 2:064006, Dec 2014. 43

[84] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, Z. L. Yuan, and A. J. Shields. Near perfect mode overlap between independently seeded, gain-switched lasers. *Opt. Express*, 24(16):17849–17859, Aug 2016. 43

[85] Yong-Su Kim, Oliver Slattery, Paulina S. Kuo, and Xiao Tang. Two-photon interference with continuous-wave multi-mode coherent light. *Opt. Express*, 22(3):3611–3620, Feb 2014. 43

[86] Thiago Ferreira da Silva, Gustavo C. do Amaral, Douglas Vitoreti, Guilherme P. Tempor ao, and Jean Pierre von der Weid. Spectral characterization of weak coherent state sources based on two-photon interference. *J. Opt. Soc. Am. B*, 32(4):545–549, Apr 2015. 43

[87] Yang Liu, Teng-Yun Chen, Liu-Jun Wang, Hao Liang, Guo-Liang Shentu, Jian Wang, Ke Cui, Hua-Lei Yin, Nai-Le Liu, Li Li, Xiongfeng Ma, Jason S. Pelc, M. M. Fejer, Cheng-Zhi Peng, Qiang Zhang, and Jian-Wei Pan. Experimental measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 111:130502, Sep 2013. 43

[88] Zhiyuan Tang, Kejin Wei, Olinka Bedroya, Li Qian, and Hoi-Kwong Lo. Experimental measurement-device-independent quantum key distribution with imperfect sources. *Phys. Rev. A*, 93:042308, Apr 2016. 43

[89] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W.-B. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields. Quantum key distribution without detector vulnerabilities using optically seeded lasers. *Nature Photonics*, 10:312 EP –, Apr 2016. 43

[90] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid. Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. *Phys. Rev. A*, 88:052303, Nov 2013. 43

[91] C. Wang, F. X. Wang, H. Chen, S. Wang, W. Chen, Z. Q. Yin, D. Y. He, G. C. Guo, and Z. F. Han. Realistic device imperfections affect the performance of hong-ou-mandel interference with weak coherent states. *Journal of Lightwave Technology*, 35(23):4996–5002, Dec 2017. 43, 48

[92] T. Ferreira da Silva, G. B. Xavier, and J. P. von der Weid. Real-time characterization of gated-mode single-photon detectors. *IEEE Journal of Quantum Electronics*, 47(9):1251–1256, Sep. 2011. 49

[93] Operation of the Thorlabs Pollarization Controller. 54

[94] Marcos Curty, Feihu Xu, Wei Cui, Charles Ci Wen Lim, Kiyoshi Tamaki, and Hoi-Kwong Lo. Finite-key analysis for measurement-device-independent quantum key distribution. *Nature Communications*, 5(1):3732, 2014. 55

[95] Charles Ci Wen Lim, Feihu Xu, George Siopsis, Eric Chitambar, Philip G. Evans, and Bing Qi. Loss-tolerant quantum secure positioning with weak laser sources. *Phys. Rev. A*, 94:032315, Sep 2016. 55

[96] B. Qi, H. Lo, C. C. W. Lim, G. Siopsis, E. A. Chitambar, R. Pooser, P. G. Evans, and W. Grice. Free-space reconfigurable quantum key distribution network. In *2015 IEEE International Conference on Space Optical Systems and Applications (ICSOS)*, pages 1–6, Oct 2015. 56

[97] G. L. Roberts, M. Lucamarini, Z. L. Yuan, J. F. Dynes, L. C. Comandar, A. W. Sharpe, A. J. Shields, M. Curty, I. V. Puthoor, and E. Andersson. Experimental measurement-device-independent quantum digital signatures. *Nature Communications*, 8(1):1098, 2017. 56

Appendices

Appendix A

Calculation of the H.O.M. Visibility parametrization

We assume that the two detectors have efficiencies $\eta_{c,d}$ and dark count probabilities $d_{c,d}$, respectively, and are blind to the photon number, i.e., a single-photon event cannot be distinguished from a multi-photon event.

Let $P_{mn}^{(out)}$ be the probability that m (n) photons arrive at the detector at port c (d). Since the ports c and d are separate, the output state $|\Psi_{out}\rangle$ eq.(4.5) can be factorized into coherent states:

$$|\Psi_{out}\rangle = |\gamma_H\rangle \otimes |\gamma_V\rangle \otimes |\delta_H\rangle \otimes |\delta_V\rangle \tag{A.1}$$

where the coherent states with parameter γ_i (δ_i) are in output port c (d), $i = H, V$, and

$$\gamma_i = (\alpha t \hat{\varepsilon}_a + \beta r \hat{\varepsilon}_b) \cdot \hat{\varepsilon}_i \ , \quad \delta_i = (\alpha r \hat{\varepsilon}_a - \beta t \hat{\varepsilon}_b) \cdot \hat{\varepsilon}_i \tag{A.2}$$

Therefore, we can write the probability $P_{mn}^{(out)}$ as a product:

$$P_{mn}^{(out)} = P_m^{(out,c)} P_n^{(out,d)} \tag{A.3}$$

where

$$\begin{aligned} P_m^{(out,c)} &= \sum_{m_H + m_V = m} P_{m_H} P_{m_V} \\ P_m^{(out,d)} &= \sum_{n_H + n_V = n} P_{n_H} P_{n_V} \end{aligned} \tag{A.4}$$

The probabilities on the right-hand side are easily deduced from the corresponding coherent states. We obtain

$$P_{m_i} = e^{-|\gamma_i|^2} \frac{|\gamma_i|^{2m_i}}{m_i!} \ , \quad P_{n_i} = e^{-|\delta_i|^2} \frac{|\delta_i|^{2n_i}}{n_i!} \tag{A.5}$$

Using the binomial theorem, we deduce

$$P_m^{(out,c)} = e^{-\mu_c} \frac{\mu_c^m}{m!} \ , \quad P_n^{(out,d)} = e^{-\mu_d} \frac{\mu_d^n}{n!} \tag{A.6}$$

and therefore

$$P_{mn}^{(out)} = e^{-\mu_c - \mu_d} \frac{\mu_c^m \mu_d^n}{m!n!} \tag{A.7}$$

where

$$\begin{aligned} \mu_c &= \sum_{i=H,V} |\gamma_i|^2 = |\alpha t \hat{\varepsilon}_a + \beta r \hat{\varepsilon}_b|^2 \\ &= |\alpha|^2 t^2 + |\beta|^2 r^2 + 2|\alpha\beta| tr \cos\Phi \cos(\theta_a - \theta_b + \phi_0) \\ \mu_d &= \sum_{i=H,V} |\delta_i|^2 = |\alpha r \hat{\varepsilon}_a - \beta t \hat{\varepsilon}_b|^2 \\ &= |\alpha|^2 r^2 + |\beta|^2 t^2 - 2|\alpha\beta| tr \cos\Phi \cos(\theta_a - \theta_b + \phi_0) \end{aligned} \tag{A.8}$$

Notice that ϕ_0 is an irrelevant phase, because we need to average over the phases.

The probability of detection if m (n) photons reach detector c (d) is $1-(1-\eta_c)^m(1-d_c)$ $(1-(1-\eta_d)^n(1-d_d))$. Therefore, the probability of detection given m (n) photons coming out of beam splitter port c (d) is

$$\begin{aligned} P_{mn} &= [1-(1-\eta_c)^m(1-d_c)] \\ &\quad \times [1-(1-\eta_d)^n(1-d_d)]\, P_{mn}^{(out)} \end{aligned} \tag{A.9}$$

The total coincidence probability is

$$\begin{aligned} P^{(coin)} &= \sum_{m,n=0}^{\infty} P_{mn} \\ &= \left(1-e^{-\eta_c\mu_c}(1-d_c)\right)\left(1-e^{-\eta_d\mu_d}(1-d_d)\right) \end{aligned} \tag{A.10}$$

showing that the effective average photon number is the average photon number of the output beam that reaches the detector multiplied by the detector efficiency.

After averaging over the phases $\theta_{a,b}$, we obtain an expression in terms of Bessel functions,

$$\begin{aligned} P^{(coin)} &\rightarrow \int_0^{2\pi} \frac{d\theta_a}{2\pi} \int_0^{2\pi} \frac{d\theta_b}{2\pi} P^{(coin)} \\ &= 1 - \mathcal{C} I_0(2\eta_c \sqrt{\mu_a \mu_b} t r \cos\Phi) \\ &\quad - \mathcal{D} I_0(2\eta_d \sqrt{\mu_a \mu_b} t r \cos\Phi) \\ &\quad + \mathcal{C}\mathcal{D} I_0(2(\eta_c - \eta_d) \sqrt{\mu_a \mu_b} t r \cos\Phi) \end{aligned} \tag{A.11}$$

where

$$\begin{aligned} \mathcal{C} &= e^{-\eta_c(\mu_a t^2 + \mu_b r^2)}(1 - d_c) \ , \\ \mathcal{D} &= e^{-\eta_d(\mu_a r^2 + \mu_b t^2)}(1 - d_d) \ . \end{aligned} \tag{A.12}$$

For the HOM visibility, we also need to calculate the probabilities for one of the two detectors to click. The probability for detector at port \$c\$ to click, after averaging over phases, is

$$\begin{aligned} P^{(c)} &= \sum_{m=0}^{\infty} \left(1 - e^{-\eta_c \mu_c}(1 - d_c)\right) P_m^{(out,c)} \\ &= 1 - \mathcal{C} I_0(2\eta_c \sqrt{\mu_a \mu_b} t r \cos\Phi) \end{aligned} \tag{A.13}$$

Similarly, for the other detector, we obtain

$$\begin{aligned} P^{(d)} &= \sum_{n=0}^{\infty} \left(1 - e^{-\eta_d \mu_d}(1 - d_d)\right) P_n^{(out,d)} \\ &= 1 - \mathcal{D} I_0(2\eta_d \sqrt{\mu_a \mu_b} t r \cos\Phi) \end{aligned} \tag{A.14}$$

We define the HOM visibility by

$$V_{HOM} = 1 - \frac{P^{(coin)}}{P^{(c)} P^{(d)}} \tag{A.15}$$

Notice that $V_{HOM} = 0$, for $\Phi = \frac{\pi}{2}$ (orthogonal polarizations).

In the limit $\alpha, \beta \rightarrow 0$ (small average photon number), and in the ideal case of no dark counts ($d_c = d_d = 0$), the HOM visibility is approximately

$$V_{HOM} \approx \frac{2RT\mu_a\mu_b \cos^2\Phi}{(T\mu_a + R\mu_b)(R\mu_a + T\mu_b)} \tag{A.16}$$

Its maximum value of $\frac{1}{2}$ is attained for $\Phi = 0$, and $\frac{\mu_b}{\mu_a} = \frac{T}{R}$. For a $50:50$ beam splitter, it reduces to

$$V_{HOM} \approx \frac{2\mu_a\mu_b \cos^2 \Phi}{(\mu_a + \mu_b)^2} \tag{A.17}$$

which vanishes for $\Phi = \frac{\pi}{2}$ (orthogonal polarizations), and for $\Phi = 0$ (parallel polarizations), it has maximum $\frac{1}{2}$ at $\mu_a = \mu_b$.

Appendix B

P-RTS Alice's state preparation

We assume that Alice has full knowledge of Bob's detection setup parameters, as summarized in Tables 3.1 & 3.2, she knows that Bob will apply a selection threshold and also she knows the channel's statistics $\{\eta_0, \sigma\}$. For the rest of the section, we follow the notation from Lim *et al.* [76] , where X denotes the rectilinear (computational) basis and Z the diagonal (Hadamard) basis. Alice performs a numerical optimization over the free parameters of her state : $\{q_X, P_{\mu_s}, P_{\mu_w}, \mu_s, \mu_w\}$ where q_X is the proportion of the bits encoded in the X-basis , $P_{\mu_s}$and P_{μ_w} are the proportions of the signal state and weak decoy state respectively, μ_s and μ_w are the photon numbers per pulse for the signal and weak decoy states respectively. For the vacuum decoy state we have fixed $\mu_v = 0.001$ and $P_{\mu_v} = 1 - P_{\mu_s} - P_{\mu_w}$.

The detection probability for $k \in \{signal, weak, vacuum\}$ at the detector $i \in \{H, V, D, A\}$:

$$P^i_{click}(\mu_k) = 1 - (1 - p^i_{bg}) \cdot e^{-\eta^i_{SYS} \cdot \mu_k} \tag{B.1}$$

The error probability

$$E^i(\mu_k) = 1 - (1 - p^{\perp i}_{bg}) \cdot e^{-e_{mis} \eta^{\perp i}_{SYS} \cdot \mu_k} \tag{B.2}$$

where $\eta^{\perp i}_{SYS}$ the total transmission leading to detector i i.e. channel transmittance, Bob's optical instruments and detector efficiency. Also $p^{\perp i}_{bg}$ is the background noise to the detector orthogonal to i. To run the numerical optimization that returns the optimal state we need the number $n_{X,k}$ of detections for which both Alice and Bob choose the rectilinear basis and Alice had used the decoy intensity $k \in \{\mu_s, \mu_w, \mu_v\}$ and the number $m_{X,k}$ of the erroneous detections where both Alice and Bob choose the rectilinear basis and Alice had used the decoy intensity k. We choose to send in total $N = 4 \cdot 10^{10}$ pulses. For the simulation we define the quantities $N_{post} = N \cdot \int_{\eta_T}^{1} p(\eta)\, \mathrm{d}\eta$ as the number of pulses that experience transmittance higher than the threshold, P_k is the proportion of the state k in Alice's sequence, r^i is the

number of available gates i.e. gates not blanked due to the dead-time for each detector $i \in \{H, V, D, A\}$. The fraction r^i can be estimated for each detector given that the average photon number is $\mu_{avg} = P_{\mu_s} \cdot \mu_s + P_{\mu_w} \cdot \mu_w + P_{\mu_v} \cdot \mu_v$. Then it is,

$$r^i = \frac{1}{1 + P^i_{click}(\mu_{avg}) \cdot \ell_g} \tag{B.3}$$

In the above $\ell_g = \dfrac{\text{dead-time}}{\text{trigger period}}$ is the number of blanked gates after each detection. Putting everything together we have,

$$n_{i,k} = N_{post} \cdot P_k \cdot \frac{q_X}{2} \cdot \left(r^i \cdot P^i_{click}\left(\mu_k\right) + E^i \cdot r^{\perp i}\right) \tag{B.4}$$

$$m_{i,k} = N_{post} \cdot P_k \cdot \frac{q_X}{2} \cdot r^{\perp i} \cdot E^i\left(\mu_k\right) \tag{B.5}$$

similar expressions hold for the diagonal basis by replacing $X \to Z$, where $q_Z = 1 - q_X$.

Applying the finite-size key distillation method from [76] we calculate the secure key Rate $R = \dfrac{\ell}{N}$, where ℓ the number of distilled bits,

$$\ell = \left\lfloor s_{X,0} + s_{X,1}\left(1 - h(\phi_X)\right) - n_X \cdot f_{EC} \cdot h(m_X/n_X) - 6\log_2\frac{21}{\varepsilon_{sec}} - \log_2\frac{2}{\varepsilon_{cor}} \right\rfloor \tag{B.6}$$

where $s_{X,0}$ and $s_{X,1}$ are the contributions to the key rate from zero and single photon pulses and ϕ_X the phase error associated with the single photon events. Their expressions stem from the three decoy state method [37] extended to include finite-size effects and are taken directly from [76]. The error correction efficiency was set as $f_{EC} = 1.16$, the secrecy criterion $\varepsilon_{sec} = 10^{-10}$ and the correctness criterion $\varepsilon_{cor} = 10^{-15}$. Given the detection parameters of tables 3.1 & 3.2 , we run a numerical optimization for various turbulence parameters (η_0, σ) that returns the optimal state $\{q_X, P_{\mu_s}, P_{\mu_w}, \mu_s, \mu_w\}$. Based on these parameters we construct the waveforms for Alice's decoy and polarization sequences.

Choosing the appropriate scale for the Weak decoy state.

For out 15bit generator the suitable scales that are converted to Voltage amplitude to modulate vacuum and and signal pulses are trivial. We set the maximum scale 16382 for the signal and 0 for the vacuum state. To choose the scale for the weak decoy we make a test measurement to determine the relation between the scale loaded on the generator and the resulting detection probability. We normalize the data to the signal photon number, 0.527 for the measurements of section 3.5, and we make a polynomial fit to determine the shape of

the function $\mu(scale)$ and calculate the appropriate scale that produces intensity $\mu_w = 0.241$ for the measurements of section 3.5.

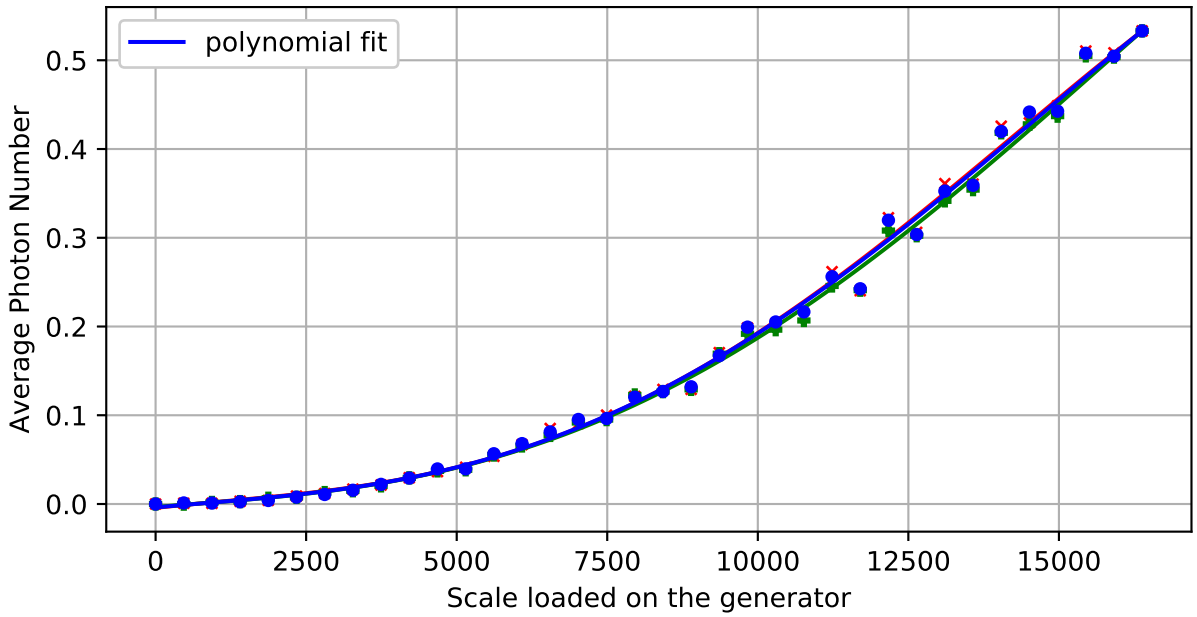

Figure B.1: Polynomial fit to determine the weak decoy scale.
Polynomial fit to determine the generator scale that produces the desired weak decoy intensity.

Vita

Eleftherios Moschandreou obtained his B.S. in Physics with concentration in Theoretical Physics from the Aristotle University of Thessalonika, Greece. He is currently a graduate student at the University of Tennessee focusing on Quantum Optics and experimental Quantum Cryptography.