Integrated Quantum Key Distribution Sender Unit for Hand-Held Platforms

Gwenaelle Mélen

München 2016

Integrated Quantum Key Distribution Sender Unit for Hand-Held Platforms

Gwenaelle Mélen

Dissertation
an der Fakultät für Physik
der Ludwig-Maximilians-Universität
München

vorgelegt von
Dipl.-Ing. Gwenaelle Mélen (geb. Vest)
aus Lyon

München, den 29. Januar 2016

Erstgutachter: Prof. Harald Weinfurter
Zweitgutachter: Prof. Alexander Högele
Tag der mündlichen Prüfung: 11. März 2016

Abstract

Mastering the generation, propagation and detection of electro-magnetic waves has enabled a technological breakthrough that has changed our entire society. World-wide communication through the telephone and the internet has become an integral part of our daily-life, which is expected to grow even further with the emergence of the internet of things. While secure communication was of concern mostly for governmental and financial institutions, digital security has now caught the attention of the general public. The weaknesses of current encryption protocols, such as the existence of back-doors or the predicted breakdown of popular algorithms such as RSA, reveal the need for alternative encryption schemes ensuring unconditional security on all types of devices.

Quantum Key Distribution (QKD) has emerged as a powerful option to ensure a private communication between two users. Based on the laws of quantum mechanics, this class of protocols offers the possibility to detect the presence of a third party trying to intercept the key during its distribution, and even to quantify the amount of leaked information. While most research projects focus on long distance applications, little attention has been devoted to short distance schemes such as wireless payment, network access and authentication, which could highly benefit from QKD-enhanced security.

This thesis focuses on the development of a miniature QKD sender add-on that could be embedded either in mobile devices or in existing optical communication platforms, thus allowing for a secure key exchange with a shared dedicated receiver over a free-space link. The proposed optics architecture ($35 \times 20 \times 8\,\mathrm{mm}^3$) is optimised for BB84-like protocols and uses an array of four Vertical-Cavity Surface-Emitting Lasers with highly similar properties to generate 40 ps long near-infrared faint coherent pulses at 100 MHz repetition rate. Under strong modulation, the polarisation of the pulses is not well defined and enables an external control of each diode's emission by a wire-grid polariser. The four beams are spatially overlapped in a polarisation-insensitive femtosecond laser written waveguide array, and combined with a red beacon laser using an external beamsplitter to ensure a stable, synchronised optical link with the receiver.

The complete module is compatible with current smartphone technology, allowing to run the classical post-processing over WLAN in the future. First tests with a free-space receiver indicate an average error ratio of 3.3 % and an asymptotic secure key rate of 54 kHz under static alignment. For the first time, a secure key exchange between a mobile platform held by a user and a receiver equipped with a dynamic alignment system could be demonstrated with an error ratio of 4.1 % and a secure key rate of 31 Hz. The further optimisation of the experimental parameters and the implementation of a decoy protocol will enhance the key generation rate as well as the general security of the system. The results of this thesis pave the way towards unprecedented security in wireless optical networks, as examplified for the communication between a mobile device and a dedicated receiver.

Zusammenfassung

Die Fähigkeit, elektromagnetische Strahlung kontrolliert zu erzeugen, gerichtet zu emittieren sowie zu detektieren stellte einen technologischen Durchbruch dar, der die ganze Gesellschaft verändert hat. Weltweite Kommunikation und Datenübertragung mittels Radiowellen, dem Telefon und dem Internet wurde zu einem wesentlichen Bestandteil des täglichen Lebens. Es ist zu erwarten, dass durch das Internet der Dinge die übertragene Datenmenge weiter zunehmen wird. Während zunächst vor allem Regierungen und Banken an Methoden für sichere Datenübertragung interessiert waren, wurde die Frage nach digitaler Sicherheit mit der Entwicklung mobiler Geräte, die immer mehr persönliche Daten sammeln und übertragen, in die breite Öffentlichkeit getragen. Die Schwachpunkte aktueller Verschlüsselungstechnologien, wie z.B mögliche Hintertüren in existierenden Implementierungen oder das in absehbarer Zeit erwartete Brechen des weit verbreiteten RSA-Algorithmus, zeigen die Notwendigkeit alternativer Verfahren, deren Sicherheit nicht von zusätzlichen, mitunter nicht überprüfbaren Annahmen abhängt.

Quantenschlüsselübertragung (engl. Quantum Key Distribution, QKD) stellt eine leistungsfähige Alternative dar, um verschlüsselte Kommunikation zwischen zwei Benutzern mithilfe eines gemeinsamen sicheren Schlüssels zu ermöglichen. Aufbauend auf den Gesetzen der Quantenmechanik ermöglicht es diese Klasse von Protokollen, eine dritte Partei beim Abhören des Schlüssels zu detektieren. Ebenso kann die Menge der möglicherweise abgefangenen Daten quantifiziert werden. Die meisten Forschungsprojekte konzentrierten sich bisher auf die Kommunikation über weite Strecken, wohingegen Anwendungen über kurze Entfernungen, wie z.B. handybasierte Bezahlmethoden oder Zugang und Authentifizierung in einem Netzwerk weitgehend vernachlässigt wurden, obwohl auch diese Anwendungen von der verbesserten Sicherheit durch QKD profitieren könnten.

Die vorliegende Arbeit beschäftigt sich mit der Entwicklung einer miniaturisierten QKD Sendeeinheit für den sicheren Schlüsselaustausch über eine Freistrahlverbindung mit einem Empfänger, wie sie als Erweiterung für mobile Geräte oder bestehende optische Kommunikationsinfrastruktur verwendet werden könnte. Das vorgeschlagene Design des optischen Chips ($35 \times 20 \times 8\,\mathrm{mm}^3$) ist für Protokolle, die sich an BB84 anlehnen optimiert und verwendet eine Anordnung von vier praktisch nicht zu unterscheidenden Oberflächenemittern (Vertical-Cavity Surface-Emitting Laser, VCSEL) die schwache, kohärente Pulse mit 40 ps Länge im nahen Infrarotbereich mit einer Wiederholrate von 100 MHz erzeugen. Bei starker Modulation ist die Polarisation der Pulse unbestimmt und kann daher mithilfe eines Gitterpolarisators für jede Diode separat eingestellt werden. Die vier Strahlen werden räumlich in einem optischen Wellenleiter, der mit einem Femtosekundenlaser geschrieben wurde und unabhängig von der Polarisation arbeitet, überlappt. Anschließend werden sie an einem externen Strahlteiler mit einem weiteren Laser im sichtbaren Bereich zusammengeführt. Dieser dient dazu, eine synchronisierte Verbindung zum Empfänger herzustellen.

Das komplette Modul ist kompatibel mit aktueller Smartphonetechnik, wodurch ein klassischer Kanal, der für die Datennachbearbeitung benötigt wird, über LTE oder WLAN zur Verfügung gestellt werden kann. Erste Freistrahltests, bei denen Sender und Empfänger

fixiert waren, ergaben eine durchschnittliche Fehlerrate von 3,3 % und eine asymptotische sichere Schlüsselrate von 54 kHz. Zum ersten Mal konnte auch ein sicherer Schlüsselaustausch zwischen einem vom Nutzer in der Hand gehaltenem mobilen Gerät und einem mit einem dynamischen Justagesystem ausgestatteten Empfänger gezeigt werden. Die Fehlerrate lag hierbei bei 4,1 % und die sichere Schlüsselrate bei 31 Hz. Durch eine weitere Optimierung der experimentellen Parameter sowie der Implementierung eines sogenannten Decoyprotokolls wird sich die Schlüsselrate sowie die Sicherheit des Systems noch deutlich erhöhen lassen.

Zusammenfassend stellen diese Ergebnisse, exemplarisch gezeigt anhand der Kommunikation zwischen einem mobilen Gerät und einem stationren Empfänger, einen ersten Schritt hin zu bisher unerreichter Sicherheit in drahltlosen Netzwerken dar.

Contents

Abstract i

Zusammenfassung iii

1. Introduction 1

2. Design of a Quantum Key Distribution system 3
2.1. Basic notions of quantum communication . . . 3
2.2. Quantum Key Distribution . . . 5
2.3. Realistic devices and side-channels . . . 7
2.3.1. Vulnerabilities on the sender side . . . 7
2.3.2. Vulnerabilities on the receiver side . . . 9
2.4. Design of a hand-held sender unit . . . 9
2.4.1. Existing systems . . . 10
2.4.2. Selection of the components . . . 11
2.4.3. Resulting architecture . . . 14

3. Generation of faint laser pulses with Vertical Cavity Surface Emitting Lasers 17
3.1. General properties of VCSELs . . . 17
3.1.1. Working principle . . . 17
3.1.2. Polarisation behaviour . . . 19
3.1.3. State-of-the-art devices . . . 20
3.2. Manipulation of bare VCSEL chips . . . 20
3.2.1. Testing and mounting . . . 20
3.2.2. Driving Electronics . . . 21
3.2.3. Optical characterisation set-up . . . 24
3.3. Experimental results . . . 26
3.3.1. Continuous-wave regime . . . 26
3.3.2. Pulsed regime . . . 28
3.3.3. Generation of decoy states . . . 32

4. Polarisation control of weak coherent pulses 37
4.1. Theory of wire-grid polarisers . . . 37
4.1.1. TE-Polarisation . . . 38
4.1.2. TM-polarisation . . . 39
4.2. Grating optimisation using Finite Difference Time Domain simulations . . . 42
4.3. Experimental results . . . 44
4.3.1. Wire-grid polariser fabrication . . . 44
4.3.2. Optical characterisation . . . 48
4.4. Refinement of the simulation model . . . 48

5. Ensuring the spatial overlap of the qubits with photonic integrated circuits 53
5.1. Femtosecond laser micromachining . . . 53
5.2. Characterisation of planar waveguide architectures . . . 54
5.2.1. Straight waveguides . . . 55
5.2.2. Directional couplers . . . 57
5.3. Study of three-dimensional waveguide arrays with polarisation insensitive behaviour . . . 59
5.3.1. Architecture optimisation . . . 59
5.3.2. Process tomography . . . 61
5.3.3. Computation of optimal input states . . . 62
5.3.4. Discussion . . . 63

6. Assembly and characterisation of the Alice module 67
6.1. Additional optical elements . . . 67
6.1.1. Collimation optics . . . 67
6.1.2. Visible beacon laser . . . 67
6.1.3. Dichroic beamsplitter . . . 67
6.2. Assembly onto a micro-optical bench . . . 68
6.3. Quality of the assembled Alice module . . . 70
6.3.1. Coupling and collection efficiencies . . . 70
6.3.2. Set of generated output state . . . 71
6.3.3. Phase compensation . . . 72

7. Quantum Key Distribution experiment 75
7.1. Optical setup of the receiver . . . 75
7.1.1. Polarisation analysis of the faint laser pulses . . . 75
7.1.2. Tracking system . . . 76
7.1.3. Synchronisation with the sender . . . 79
7.2. Preliminary tests . . . 80
7.2.1. Characterisation of the optical pulses . . . 80
7.2.2. Evaluation of the dark count rate . . . 81
7.2.3. Test of the dynamic alignment systems . . . 83
7.3. Experimental quantum key distribution . . . 83
7.3.1. Static alignment of the sender unit . . . 84
7.3.2. Dynamic alignment of a hand-held Alice module . . . 84

8. Conclusion and outlook 87

A. Printed Circuit Board layouts 89
A.1. Driving Electronics . . . 89
A.2. VCSEL board . . . 90

B. Tomographic measurement data 91
B.0.1. Tomography of the waveguide chip . . . 91
B.0.2. Tomography of the states prepared by the Alice module . . . 92

List of abbreviations 93

Bibliography 95

Publications **105**

Acknowledgements **107**

Soulever un caillou et ne rien trouver, c'est déjà un progrès.

P.C.

1. Introduction

In modern communication, the information sent from A(lice) to B(ob) is encoded onto a sequence of bits of value 0 or 1 and carried by modulated electro-magnetic waves. As this classical signal can be easily deflected from its initial route, amplified and detected by a third party, the original message is usually encrypted prior to transmission to prevent undesirable readers to retrieve any information from the transferred data.

In the most simple scenario, called *symmetric encryption*, both parties wishing to communicate share an identical key used for both the encryption and decryption processes. Theoretical security based on information theory can be proven only for the so-called One-Time-Pad, where the key consists of a random bit sequence necessarily as long as the message, is only used once. Real implementations, however, use a static key of fixed length repeatedly to reduce the effort the memory and time-consuming key generation process, and to ensure practical security by applying multiple permutation and substitution algorithms, as done in the Advanced Encryption Standard (AES). While the encryption protocol itself is considered secure, the main issue lies in the distribution of the initial secret key among both participants, as interaction of a third party during this process cannot be excluded.

Asymmetric protocols circumvent this problem by allowing each user Alice to generate two keys. The first one, called *public*, can be used by anyone to encrypt the messages intended for her, whereas the content can be decrypted only with the *private* key that she keeps secret. The security of such protocols relies on pseudo one-way functions guaranteeing a computationally hard retrieval of the private key from the public one. The RSA protocol [1] for instance, widely used in all types of communication over the internet, could be cracked by factorising large numbers into prime numbers. While this operation would take about the age of the universe on a classical computer for a 200-digit number, it could be calculated within a reasonable amount of time using Shor's algorithm [2] on a quantum computer. The implementation of such program would make military, political, financial and personal communication vulnerable, and could be critical for our society. Although state-of-the-art experiments are only able to factorise the number 21 using this quantum algorithm [3], the emergence of a fully functioning quantum computer capable of solving such problems is expected in a relatively near future. It is thus of utmost common interest to elaborate alternative encryption schemes before the collapse of the current system.

Quantum Key Distribution (QKD) protocols have attracted a lot of attention since the first proposal in 1984 [4], as they promise a theoretical security [5, 6]. By generating a random key, that can therefore neither be guessed nor calculated, and by securely distributing it among two users, QKD fixes the weakest links of classical encryption schemes. Furthermore, these protocols exploit the quantum properties of the qubits to precisely quantify the information gained by a potential eavesdropper and abort the process if necessary. The created key can then be combined with conventional cryptographic algorithms to ensure security of the full encryption process.

Most efforts have been concentrated on pushing the limits of achievable distances in

order to build secure quantum networks based on trusted nodes. Several metropolitan networks with dedicated "dark" fibres have been installed in Geneva [7], Hefei [8] and Tokyo [9]. The successful integration of a QKD network with a classical Gigabit Passive Optical Network (GPON) has even been reported recently [10]. Additionally, long-distance free-space links [11][12] would offer the possibility to use satellites as trusted relays. Nevertheless, short-distance applications such as card-less payments, network access or the internet of things (IoT) could also benefit from increased security. Miniature add-ons based on photonic nanotechnologies could boost the integration of QKD in mobile devices or in existing optical communication platforms. In order to be attractive and competitive against other less secure alternatives, these QKD devices should ensure a user-friendly operation with fast key generation rates.

This thesis reports on the development of a miniature QKD sender unit capable of generating polarised weak coherent pulses in order to implement BB84-like protocols. To achieve a limited footprint as well as a low power consumption of the optical module, a novel architecture based mostly on passive components has been designed. The size of the first prototype ($35 \times 20 \times 8\,\mathrm{mm}^3$) and the compatibility of the driving electronics with standard smartphone technology allows for future integration of this system into mobile platforms.

Chapter 2 presents a brief theoretical introduction to the implemented QKD protocol and discusses the technical challenges associated with the generation of high quality polarisation qubits with integrated optics components. The suitability of different elements is estimated and a novel design based on four laser diodes is proposed. Chapter 3 deals with the generation of identical faint laser pulses using an array of Vertical Cavity Surface Emitting Lasers. The polarisation properties of these pulses are characterised under continuous-wave and strong modulation operation. Chapter 4 focuses on the optimisation and the fabrication of a wire-grid polariser array enabling the polarisation preparation of the pulses emitted by each diode. The characterisation of a waveguide chip manufactured by femtosecond laser micromachining and ensuring the spatial overlap of the polarised coherent states is presented in Chapter 5. The assembly of the micro-optics unit as well as its performance within a first proof-of-principle QKD experiment involving a free-space receiver equipped with dynamic alignment system are shown in Chapter 6 and 7, respectively.

2. Design of a Quantum Key Distribution system

2.1. Basic notions of quantum communication

Quantum Key Distribution protocols rely on the correctness of quantum mechanics, and are based on Wiesner's original idea [13] that a currency obeying the laws of quantum physics could not be counterfeited. Unlike its classical counterpart, the quantum bit or *qubit* cannot only take the values 0 and 1 but can be in any superposition of the states $|0\rangle$ and $|1\rangle$ such that

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2.1}$$

where α and β are complex quantities satisfying the normalisation condition $|\alpha|^2+|\beta|^2 = 1$. The qubit states span a two-dimensional Hilbert space and can be represented by a vector in polar coordinates

$$|\psi(\theta,\varphi)\rangle = cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\, sin\left(\frac{\theta}{2}\right)|1\rangle \tag{2.2}$$

with $\varphi \in [0, 2\pi]$ and $\theta \in [0, \pi]$ and visualised onto the Poincaré sphere, as depicted in Fig. 2.1.

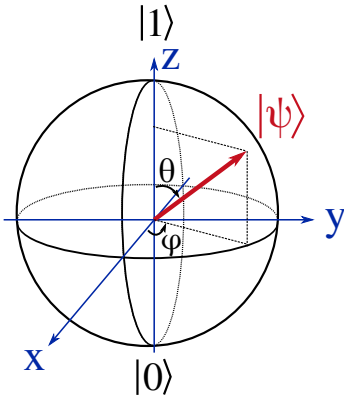


Figure 2.1.: Visualisation of a qubit $|\psi\rangle$ on the Poincaré sphere. The states $|0\rangle$ and $|1\rangle$ represent the computational basis of $|\psi\rangle$.

In principle, any two-level system can be used as qubit. Most textbooks consider a spin-1/2 particle where the spin-up state $|\uparrow\rangle$ corresponds to $|1\rangle$ and the spin-down state $|\downarrow\rangle$ to $|0\rangle$. In quantum communication applications, the qubits have to be distributed efficiently among different parties separated by a long distance. Photons are easily transferable and therefore suitable as *flying qubits* in this sense. As further advantage they offer the possibility to encode information onto different Degrees Of Freedom (DOF) such as the

Spin Angular Momentum (SAM, or polarisation), Orbital Angular Momentum (OAM), phase, frequency or spatial mode, therefore allowing for high-dimensional encoding [14].

In the following we will focus on one qubit systems with information encoded onto the polarisation of photons, and define the eigenstates $|0\rangle$ and $|1\rangle$ as $|H\rangle$ and $|V\rangle$, respectively. Photonic qubits are sometimes also written in a different computational basis such as $X = \{|D\rangle, |A\rangle\}$ and $Y = \{|R\rangle, |L\rangle\}$. The correspondence between the usual states used in quantum communication, their linear polarisation and the bit value they encode is given in Table 2.1.

Basis	State	Linear polarisation	Bit value
Z	$\|H\rangle$	0^o	0
	$\|V\rangle$	90^o	1
X	$\|D\rangle = \frac{1}{2}(\|H\rangle + \|V\rangle)$	45^o	0
	$\|A\rangle = \frac{1}{2}(\|H\rangle - \|V\rangle)$	-45^o	1
Y	$\|R\rangle = \frac{1}{2}(\|H\rangle + i\|V\rangle)$	–	0
	$\|L\rangle = \frac{1}{2}(\|H\rangle - i\|V\rangle)$	–	1

Table 2.1.: Definition of the common computational bases used in quantum information processing of polarisation qubits. The states $|D\rangle$,$|A\rangle$ are called diagonal and anti-diagonal, respectively, while $|R\rangle$ and $|L\rangle$ refer to circularly polarised light with right or left handedness.

A measurement on the state $|\phi\rangle$ can be mathematically described by a self-adjoint operator which projects the qubits onto one of its eigenstates $\{|\psi_1\rangle, |\psi_2\rangle\}$ with a probability

$$P(|\psi_i\rangle) = |\langle\phi|\psi_i\rangle|^2 \tag{2.3}$$

When the preparation and measurement bases coincide, the qubit information is perfectly transferred, provided that the quantum communication channel does not change the state. For example, if Alice encodes the bit 0 in the Z-basis ($|\phi\rangle = |H\rangle$), Bob can perform a σ_z measurement that leads to

$$P(|H\rangle) = |\langle H|H\rangle|^2 = 1 \qquad P(|V\rangle) = |\langle V|H\rangle|^2 = 0 \tag{2.4}$$

from which he can deduce which state Alice sent if he knows the basis she used. If he does not know in which basis he should measure and decides to analyse the qubit in a so-called *conjugated* basis, *e.g.*, X he will not gain information about the state, as both possible states from the Z-basis lead to equally probable outcomes:

$$P(|D\rangle) = |\langle D|H\rangle|^2 = \frac{1}{2} \qquad P(|D\rangle) = |\langle D|V\rangle|^2 = \frac{1}{2} \tag{2.5}$$

$$P(|A\rangle) = |\langle A|H\rangle|^2 = \frac{1}{2} \qquad P(|A\rangle) = |\langle A|V\rangle|^2 = \frac{1}{2} \tag{2.6}$$

Due to the impossibility to clone the state of a single quantum system [15], the receiver cannot generate copies of the qubit prior to measurement and therefore retrieve the qubit

value by applying several operators, *e.g.*, σ_x and σ_z. This indistinguishability of non-orthogonal states can be used in quantum communication protocols, as presented in the following section.

2.2. Quantum Key Distribution

We focus on the first Quantum Key Distribution (QKD) protocol [4] proposed by Bennett and Brassard in 1984 (BB84), not only due to its historical importance, but also due to the simplicity of its experimental implementation. The essential concept and notions based on this example are easily transferable to the more elaborate schemes mentioned later on. The BB84 protocol belongs to the *prepare-and-measure* schemes, where the sender, usually called Alice, prepares the single qubits states and sends them to a receiver, usually called Bob, over a dedicated *quantum* channel. As the information is encoded onto the polarisation of single photons, the BB84 protocol is also qualified as *discrete variable encoding* protocol. The different steps are detailed below.

1. The sender Alice and the receiver Bob agree on two conjugated bases, *e.g.*, $Z = \{|H\rangle, |V\rangle\}$ and $X = \{|D\rangle, |A\rangle\}$ and a corresponding coding scheme, as presented in Table 2.1.

2. Alice chooses at each step a random basis and a random bit value. She prepares a single photon accordingly and sends it over to Bob via a (polarisation) preserving channel. Bob detects each photon in a randomly chosen polarisation basis, obtaining a meaningful result only when both preparation and detection bases coincide. This procedure is repeated until the appropriate number of bits have been exchanged.

3. From this stage on, the post-processing of the key remains purely classical. Bob announces over a public channel the times of his detection events, and all the bits lost during transmission are discarded from both sides. According to the coding scheme they agreed upon, Alice and Bob now both possess a binary string of data sometimes referred to as *raw key*.

4. During *basis reconciliation* or *sifting*, Bob broadcasts the basis he used for each detected photon, without ever communicating the corresponding outcome. Alice reports the time where the basis choices coincide. They both remove the other bits (about 50 %) and obtain the so-called *sifted key*.

In the absence of an eavesdropper (Eve) and for perfect transmission through the quantum channel, the sifted keys on Alice's and Bob's side should be identical. Eve can try to gain information about the key by tampering with the quantum channel, for example by performing a so-called *intercept-resend attack*. She diverts all qubits to her own measurement setup similar to Bob's and prepares new states according to her outcomes. Because she does not know which of both encoding bases she should use, she chooses at random. Among the bits that are kept during the sifting procedure, *i.e* when Bob's and Alice's basis choice coincide, she will introduce a fraction of flipped bits called Quantum Bit Error Ratio (QBER) $\delta = 25\,\%$, as highlighted in Table 2.2. Fifty percent of the time, she chooses the right basis and introduces no error. Otherwise, she prepares the wrong state, but has 50% chance that Bob's measurements still yields the right result. Alice and

Alice	Basis	Z	Z	X	Z	X	X
	Prepared state	$\|H\rangle$	$\|V\rangle$	$\|A\rangle$	$\|H\rangle$	$\|A\rangle$	$\|D\rangle$
Eve	Basis	X	X	Z	Z	X	Z
	Detected state	$\|D\rangle$	$\|A\rangle$	$\|H\rangle$	$\|H\rangle$	$\|A\rangle$	$\|V\rangle$
Bob	Basis	Z	X	X	Z	Z	X
	Detected state	$\|H\rangle$	$\|A\rangle$	$\|D\rangle$	$\|H\rangle$	$\|D\rangle$	$\|H\rangle$
	Sifted key	0		1	0		0

Table 2.2.: Security of the BB84 protocol against eavesdropping in case of an intercept-resend attack. Eve detects each qubit in a random basis and prepares a new qubit state according to the outcome of her measurement. The 25 % of errors she will have introduced on average in the sifted key reveals her presence.

Bob can therefore detect Eve by evaluating δ.

In practice, some bits are flipped due to imperfect optical systems, environmental fluctuations or to Eve's presence. Because it is not possible to discriminate between the potential sources of error, only the worst case scenario, where all wrong bits are attributed to Eve's doing, is considered. In order to evaluate the fraction of flipped bits called Quantum Bit Error Ratio (QBER) δ, and rectify these errors, Alice and Bob have to perform classical error correction. The CASCADE protocol [16], developed specifically for QKD, executes a binary search using parity bit checks for different block sizes. Alternatively, the Winnow protocol [17] based on Hamming codes offers faster agreement between both keys with limited information exchange over the classical channel. This algorithm has also been proven more efficient over a wide range of error rates, thereby exhibiting more flexibility than Low Density Parity Codes (LDPC).
If the QBER does not exceed a threshold value above which the security is not guaranteed any more and the QKD protocol aborts, error correction is performed. The number of bits discarded during a perfect correction process is given by the binary entropy function [18]

$$H_2(\delta) = -\delta \; log_2(\delta) - (1-\delta) \; log_2 \, (1-\delta) \tag{2.7}$$

In practice a slightly larger number of bits $f(\delta)\, H_2(\delta)$ is consumed, where $f(\delta) \gtrsim 1$ characterises the imperfection of the correction.

Given the QBER δ, the information potentially gained by Eve is also upper bounded by $H_2(\delta)$. In order to reduce this information to a negligible amount ε, the number of bits that can be used in the final key has to be decreased to

$$N = N_{sift} \, [1 - \; H_2(\delta) - f(\delta)\, H_2(\delta)] \tag{2.8}$$

A secure key of N bits can be distilled when N is strictly positive, *i.e.*, for $\delta < 11\,\%$ (assuming $f(\delta) = 1$). In this last step, called *privacy amplification* or *randomness extraction*, the sifted key of length N_{sift} is shrunk down to N bits and maximally scrambled via multiplication with a $N \times N_{sift}$ matrix belonging to the U_2-Hash function class. Diagonal-constant (Töplitz) matrices [19] are suitable for this task as their structure guarantees low memory requirements as well as efficient multiplication via Fast Fourier Transform (FFT).

It should be mentioned that N is asymptotically reached for very large numbers of bits, typically well above 10^6. For smaller samples, this number is decreased due to insufficient statistics and therefore larger uncertainty on Eve's information. Finite-key analysis of QKD protocols can be found in [20, 21].

Finally, an authentication step is required to avoid a *man-in-the-middle* attack. Alice and Bob should possess an initial pre-shared key, that is hashed with the generated key and compared by both parties. The secret seed required for QKD protocols is responsible for the alternative and more appropriate name of quantum key growing. An exhaustive review of the theory and practical implementations of QKD protocols is presented in [22].

A number of variations of this protocol have been proposed. The *efficient BB84* protocol [23] uses an unbalanced basis choice where the most probable basis, *e.g.*, Z is used to generate a key while the other only serves for the computation of the phase error ratio. The optimal relative frequency is dependent on the error rate, and although this method guarantees higher key generation rates, the use of X cannot asymptotically go down to 0 to gather enough statistics to evaluate Eve's information. The BB84 protocol has also been implemented with phase encoding [24] to allow the use of birefringent quantum channels such as fibres. The main technical difficulty associated with this scheme is the requirement of at least one stable Mach-Zehnder interferometer on the receiver's side.

2.3. Realistic devices and side-channels

QKD aroused interest in the scientific community for guaranteeing *theoretical security* against intercept-resend attacks. Unfortunately, technical imperfections present in real devices have opened back-doors to more elaborate attacks, where Eve can reconstruct the key almost entirely without being detected. An actual and exhaustive list of the discovered vulnerabilities is presented in Ref. [25]. Although a successful patch could be implemented for each of them, the emerging field of *quantum hacking* regrettably led the communities outside of quantum physics to believe that QKD is not secure and therefore does not bring any improvement with respect to classical cryptographic systems. We present some of the known practical imperfections that are relevant for the design of our hand-held QKD sender unit and its dedicated free-space receiver. The associated security analysis can for most cases be found in the famous contribution by Gottesman, Lo, Lütkenhaus and Preskill (GLLP) [26] or in more recent work [27].

2.3.1. Vulnerabilities on the sender side

Photon distinguishability

One pre-requisite for the BB84 protocol is that the qubits only differ by their polarisation states. The other degrees of freedom such as the spatial modes, the spectral properties and temporal shapes have to be identical and should not in any way be correlated to benefit from the indistinguishability of non-orthogonal states responsible for the underlying security. Eve can also benefit from the imperfect preparation of the qubits [20] if they do not form perfectly conjugated bases. The overlap between the formed bases can be quantified by device quality $q \leq 1$ defined as

$$q = -log_2 \left[\max_{(\psi_x, \psi_z)} \left(|\langle \psi_x \mid \psi_z \rangle|^2 \right) \right] \tag{2.9}$$

and leading to a reduction of the secret key rate by this amount. The value $q = 1$ is obtained only for mutually unbiased bases, and $q = 0$ is achieved only if $X = Z$, leading to a secret key rate of 0, due to the possibility given to Eve to retrieve the state with a single measurement using an intercept-resend attack.

Photon-Number-Splitting (PNS) attack

The first proposal for QKD relied on the existence of a single-photon source that had not been developed yet. Despite recent progress towards efficient on-demand sources, the achieved photon generation rate is not sufficient to guarantee a fast key exchange process, and the use of most systems is cumbersome due to the requirement of cryogenic temperatures. Alternatively, attenuated laser pulses, also known as Weak Coherent Pulses (WCP), have emerged as a more practicable approach. The photon statistics of a pulse containing on average μ photons is known to follow a Poissonian distribution, *i.e.*, the probability of having n photons in a pulse is defined as

$$P_\mu(n) = \frac{\mu^n}{n!} e^{-\mu} \tag{2.10}$$

For instance, a pulse with a mean photon number $\mu = 1$ has equal probability $P_1(0) = P_1(1) = e^{-1} = 0.37$ to contain either zero or one photon, an a non-negligible probability $P_1(n \geq 2) = 1 - e^{-\mu} - \mu\, e^{-\mu} = 0.26$ to contain multiple photons. In the Photon-Number-Splitting (PNS) attack (also *storage* or *beamsplitter attack*) [28] [29], Eve is able to count the number of photons within the pulse, using *e.g.* a Quantum Non-Demolition (QND) technique. She prevents single photon pulses to be transmitted and extracts at least a photon from multi-photon pulses. Provided that she has access to a quantum memory, she can wait until the basis reconciliation to measure her photons in the right basis. If she gets more than two photons for one bit, she can also measure in both bases simultaneously and therefore also retrieve the full information. In this scheme Eve does not introduce any error and therefore stays unexposed, although Bob might become suspicious if its detection rate is surprisingly low.

A secret key can still be obtained with WCP by eliminating the so-called *tagged bits* Δ, representing the portion of bits Eve can retrieve using this strategy. This quantity corresponds to the probability for Bob to obtain a detection event when a multi-photon pulse was sent:

$$\Delta = \frac{P_\mu(n \geq 2)}{P_\mu(n \geq 1) \cdot \eta_{tot}} \tag{2.11}$$

with η_{tot} the total detection efficiency. The number of extracted secret bits is then reduced to

$$N = N_{sift} \,.\, \left[(1 - \Delta) - f(\delta) \,.\, H_2(\delta) - (1 - \Delta) \,.\, H_2\left(\frac{\delta}{1 - \Delta}\right) \right] \tag{2.12}$$

Several countermeasures were proposed in order to improve the security against PNS attacks. The *SARG04* [30] protocol applies a different sifting procedure that does not require the public announcement of the encoding basis, thus preventing Eve to perform the right measurement. A more universally adopted extension to the BB84 protocol is the decoy state protocol [31, 32]. In addition to the BB84 signal states with mean photon numbers μ_s, Alice also sends decoy states, which only differ from the signal states by their

intensity μ_d such that $|\langle\mu_s|\mu_d\rangle|^2 \neq 0$. Eve can therefore not distinguish between these non-orthogonal states, and by performing a PNS attack she will change the statistics of both states by a different amount. By evaluating the transmission probability of the signal and decoy states, Alice and Bob can detect Eve's presence and abort the protocol if necessary. This method is convenient as it allows to use weak coherent states with high mean photon numbers, thereby increasing the key generation rate.

Trojan-Horse attacks

This category of attacks consists in injecting a bright optical pulse into the sender and to analyse the reflected signal. Information about the current state of the different components [33] can reveal which state had just been prepared. An upper-bound on Eve's extractable information was recently established [34], and countermeasures including the addition of optical isolators and narrow spectral filters have been proven efficient against such attacks.

2.3.2. Vulnerabilities on the receiver side

Most of the reported vulnerabilities of commercial and research platforms are directly related to imperfections of the single-photon detectors. Avalanche Photodiodes (APD) operated in Geiger mode, *i.e.*, with a reverse voltage above the breakdown voltage, have become standard components for QKD applications, as they can achieve low noise, high temporal resolution and high-efficiency, especially between 500 nm and 900 nm. Several flaws such as intrinsic efficiency mismatch between different detectors [35], dead-time [36] or saturation using bright pulses [37] can be exploited by an eavesdropper to know which of the detectors recorded the photon. A possible attack related to the free-space property of our system is identified and presented in Chapter 7.

A recent protocol named Measurement-Device-Independent QKD (MDI-QKD) [38] proposes that the detection of the qubits sent by Alice and Bob takes place at a third location associated to Charlie. The latter performs a Bell state measurement and broadcasts publicly the outcome. Alice and Bob can conclude about his fairness by comparing a subset of their keys. As long as Alice and Bob trust their apparatus, no assumption needs to be made on the security of the detection process, thereby making any attack on the detectors inefficient. This convenient untrusted-relay architecture can be used for weak coherent pulses in combination with decoy state protocol, and constitutes an important element towards secure quantum networks.

Another promising approach is the *Continuous Variable* encoding (CVQKD) based on the simultaneous phase and intensity Gaussian modulation of macroscopic pulses. This method takes advantage of standard high-speed components such as modulators and detectors developed in the telecommunication industry for a wavelength of 1,550 nm and not inclined to the aforementioned attacks. In contrast to BB84, losses are more critical for this protocol and classical error correction is harder to perform. A MDI-QKD version was also demonstrated recently [39].

2.4. Design of a hand-held sender unit

In this thesis we focus on an asymmetric client-server scenario, where a user owns an integrated QKD sender (Alice) unit allowing him to perform a secure key exchange with a

shared dedicated receiver (Bob) over short distances ($0.5 - 1\,\mathrm{m}$). The generated key could either be stored for future or remote use (*e.g.* on the internet), or could be consumed directly to communicate with the receiver. In the case where the latter is a trusted node of a quantum network, the integrated sender unit can be seen as a quantum access device that allows the user's data to be securely uploaded. In a more down-to-earth approach, the receiver could be a Point-Of-Sale (POS) or an Automated Teller Machine (ATM), where the additional use of a QKD protocol would allow to detect a *man-in-the-middle* or *skimmer* attack, to which the widely used magnetic stripe credit cards are prone. Several countermeasures including the development of the so-called *smart-cards* by the Europay Mastercard and Visa (EMV) consortium have been implemented but still suffer from other flaws that allow a third party to obtain the user's credit card data and even simulate an authorised debit quite easily [40].

In order for our system to compete with classical communication devices based on *e.g.* Near-Field Communication (NFC) or credit cards in terms of practicality and user-friendliness, we impose the following specifications:

- The optical part of the hand-held transmitter unit should be ultra-flat in order to fit in *e.g.* a smartphone case. The dedicated electronics should be compatible with current mobile technology and consist of relatively low-cost, standard components. While the optics is optimised for short distance operations, it should be possible to integrate this QKD add-on into telescope-based systems to bridge the gap to longer distances.

- The free-space receiver should be equipped with a dynamic alignment system to ensure (a) a stable optical link with easy aiming procedure despite the possible shaking of the user and (b) a continuous reference-frame alignment with the sender.

- The system should run at 100 MHz in order to guarantee high key generation rates exceeding 10^6 sifted bits within a few seconds. With this design rule, strong reduction of the key due to finite-size effects can be avoided, and processing times of a few seconds can be achieved.

This work is mainly related to the design and characterisation of the miniature Alice module. The corresponding receiver has been developed separately [41][42] and is briefly presented in Chapter 7. From this perspective, we first review the current state of the few projects reported in the literature at the beginning of this work and which concentrate on the miniaturisation of the sender unit. We discuss the advantages and drawbacks of the different concepts and components involved and finally present the adopted architecture.

2.4.1. Existing systems

In the following we review and compare practical QKD systems implementing the BB84 protocol with polarised WCP (see Table 2.3). The main advantage of this scheme is the simplicity of the optical setup on the sender side. In a realistic application, the latter should only include scalable, low-cost components while expensive and demanding devices in terms of energy and hardware such as single-photon detectors are reserved to the shared receiver.

The first project towards a hand-held Alice module was reported by the University of Bristol and Hewlett-Packard Laboratories in 2006 [43]. In this experiment, the pulses are

generated at 5 MHz by four Light-Emitting Diodes (LED) , polarised by sheet polarisers and and spatially combined into one mode using a grating couplers. Spectral indistinguishability of the states is obtained by a narrow filtering of the broadband emission. The size of the module is about $15\times15\times4\,\mathrm{cm}^3$, and a static alignment with the receiver allowed secret key rates of 4 kHz. A similar system based on Edge-Emitting Laser diodes (EEL) and achieving comparable key rates was announced a few years later by Qinetiq [44].

Architectures based on a single Distributed Feedback laser diode (DFB) source have also been proposed. In Ref. [45], the pulses emitted at 100 MHz repetition rate are equally distributed among four fibre-coupled Semiconductor Optical Amplifiers (SOA) that act as fast switches. The output beams are each polarised by a $2.5\times2.5\,\mathrm{mm}^2$ free-space polariser and are coupled into a bare fibre for spatial filtering. High key rates exceeding 3.6 MHz with a QBER of 1.14 % were experimentally obtained.

After the beginning of this work, Los Alamos National Laboratory announced their fibre-based sender unit named *QKarD* [46]. The compact optical architecture developed for telecommunication wavelengths fits into a butterfly package of a few cubic centimetres. Unfortunately, the publication only mentions that the device includes a DFB laser modulated at 10 MHz repetition rate, without giving further technical details or experimental results. For sake of completeness we should also mention that the first on-chip Alice platform has been demonstrated at 1,550 nm during the redaction of this thesis [47].

	Source	Type	Polarisation selection	R_{rep}	QBER	R_{sec}	Reference
1	LED	Free-space	Sheet polarisers	5 MHz	2.7 %	4 kHz	[43] (2006)
2	EEL	Free-space	$\lambda/2$ + PBS	20 MHz	< 4 %	3 kHz	[44] (2010)
3	DFB	Fibred	Sheet polariser	100 MHz	1.1 %	3.6 MHz	[45] (2011)
4	DFB	Fibred	?	10 MHz	?	?	[46] (2013)

Table 2.3.: Performance of the QKD systems reported in the literature which include a small Alice unit. Package sizes range from approximately $15\times15\times4\,\mathrm{cm}^3$ (1) to $5\times1\times1\,\mathrm{cm}^3$ (4).

2.4.2. Selection of the components

Generation of polarised WCP

We choose to implement the BB84 protocol with polarisation encoding onto weak coherent states. In order to close the previously discussed side-channels, they should exhibit spectral, spatial as well as temporal indistinguishability. Working with only one source and actively rotating the polarisation of each pulse using an EOM is therefore the most natural strategy in this regard. However, EOMs often induce an elliptical component, thereby limiting the achievable QBER, and their footprint of a few square centimetres does not fulfil our design guidelines. We therefore adopt an approach where each BB84 state is generated by a dedicated laser, and which has already been proven successful in other QKD experiments [11, 48]. Different types of light sources with a high integration potential, *i.e.*, bare semiconductor chips without additional packaging, have been considered. LEDs emit unpolarised light and allow for external selection of the polarisation state. The

broadband emission guarantees a good spectral overlap between different diodes, which can be further enhanced by a narrow spectral filter. Nevertheless, the collection efficiency of the light is limited by the low directionality of the emission ($\Theta \simeq 90^o - 120^o$), and the temporal response of LEDs is restricted to about 2 ns by the spontaneous emission rate. This solution may be viable at lower repetition rates but is not suitable for a system running at 100 MHz, where subnanosecond optical pulses have to be generated to allow for efficient temporal filtering. Laser diodes, on the other hand, can be modulated with gigahertz frequencies and are in this regard better candidates. QKD experiments have been mostly implemented with EEL as they emit polarised light with a typically high contrast above 1:100. While precise positioning of the diode to adjust the polarisation direction is convenient with a TO-package, the alignment and bonding procedures would become extremely cumbersome with the bare chips. Additionally, the elliptical profile of the output beam limits the coupling efficiency into an integrated spatial mode filter supporting circular modes. DFB lasers exhibit the same issues, and are furthermore not suited for our application as their narrow spectral width of several tens of megahertz strongly limits the overlap probability of separated chips. Vertical-Cavity Surface-Emitting Lasers (VCSEL), on the other hand, fulfil all the requirement imposed by the BB84 protocol and our design rules simultaneously. Here four top-emitting diodes fabricated on the same substrate can be used to generate the four different states and are likely to exhibit uniform emission properties due to highly similar growth conditions. Most VCSEL arrays are designed with a standard pitch of 250 µm, thereby offering compatible integration with other micro-optics components. Their low energy consumption on the order of a few milliwatts combined with high modulation speeds up to 40 GHz [49, 50] is a particularly attractive feature for optical interconnects and embedded systems. Finally, the circular Laguerre-Gauss profile of the laser beam enables efficient coupling into fibres for, *e.g.*, Local Area Networks (LAN) applications or into waveguides for more compact architectures. We therefore opt for this solution, and agree upon an emission wavelength of 850 nm to take advantage of state-of-the-art VCSEL architectures while guaranteeing a low absorption in air and high detection probability with standard Silicon-APDs on Bob's side.

Unlike other aforementioned solid-state lasers, VCSELs usually exhibit a quite complex polarisation behaviour related to the lack of intrinsic polarisation selection mechanisms. As the emitted light is not strongly polarised along a particular direction, a passive device such as a micro-polariser array with 250 µm pitch is sufficient to control the state generated by each diode. The strategy consisting in assembling different polariser sheets results in relatively low orientation accuracy, and can hardly be extended to the sub-millimetre scale. Here we take advantage of nanotechnology fabrication techniques such as Electron-Beam Lithography (EBL) or Focused Ion Beam (FIB) milling to directly produce an array of components preparing the right quantum states. A relevant option is provided by wire-grid polarisers [51, 52]. These sub-wavelength metal gratings act as perfect reflectors for s-polarisation (*i.e.*, parallel to the stripes) whereas extraordinary transmission occurs for p-polarisation due to Surface Plasmon Polariton (SPP) excitation and Fabry-Pérot cavity effects at the slit ends. As the filtered polarisation is completely reflected, special attention needs to be devoted to avoiding scattering at the interfaces between the optical components or retro-injection into the laser diode.

Spatial overlap of the WCP

As the different polarisation states are generated by dedicated diodes, spatial filtering methods should also be investigated. In previous experiments, the beams have been overlapped either at a beamsplitter, leading to a rather bulky architecture, or in a single-mode fibre. The second solution is not adapted to our miniaturised module for two reasons. First of all, the length of the fibre should be long enough to provide sufficient attenuation of higher-order modes. Second of all, fibres feature a relatively high birefringence, which is strongly influenced by mechanical and thermal stress and leads to a random and unstable rotation of the $\pm 45^o$ states. For an outdoor application, the fibre should be thermally stabilized to cope with the ambient temperature and with the heating of the device itself in the hand or pocket of the user. In view of compactness and stability we thus focus on single-mode, low birefringence waveguide arrays rather than optical fibres. Lithographically fabricated Photonic Integrated Circuits (PIC) benefit from the mature industrial development of the semiconductor technology, reaching high integration density and low propagation losses. Whereas they have been used to demonstrate the first on-chip qubit manipulations [53, 54], they do not sustain polarisation encoding due to waveguide birefringence and their layout is restricted to planar configurations. These limitations can be overcome by the femtosecond laser writing technique [55, 56], which has recently emerged as a fast, single-step alternative fabrication method allowing three-dimensional classical [57] and quantum [58, 59] photonics architectures. The low birefringence $\Delta n < 10^{-5}$ enables the propagation of polarisation qubits and their combination into one spatial mode using directional couplers.

Collimation optics

The light emerging from the waveguide chip has a divergence angle of a few degrees and should be collimated by a miniature lens to allow reasonable operation distance between Alice and Bob. The receiver is typically equipped with two entrance apertures of diameter $d = 1\,\text{mm}$ and separated by 10 cm in order to facilitate the aiming and filter the background light. A compromise has to be found between low divergence of the output beam and the diameter of the lens. The influence of the focal length onto the beam radius is shown in Fig. 2.2.

GRadient INdex (GRIN) lenses offer small diameters below 2 mm but a length of one to two centimetres. Unlike conventional lenses, the light is focused using continuous Total Internal Reflection in a smooth refractive index gradient with cylindrical symmetry. The latter is achieved either by implantation or diffusion of impurities. Experimental observation of birefringence effects have nevertheless been reported due to anisotropic dopant concentration [60, 61]. Unfortunately, the focal length of commercial GRIN lenses is limited to 4 mm, such that the maximal operation distance between Alice and the first aperture of the receiver is about 30 cm. Commercial aspheric lenses with an outer diameter of $d' \leq 3.6\,\text{mm}$ can deliver longer focal lengths up to $f = 6\,\text{mm}$, which are sufficient to extend the practical communication range to about 60 cm.

Synchronisation and reference-frame alignment with the receiver

The secure key rate provided by the BB84 protocol is strongly influenced by experimental parameters such as the precise alignment of the reference polarisation between Alice and Bob. For moving platforms, this represents an enormous exchange of information.

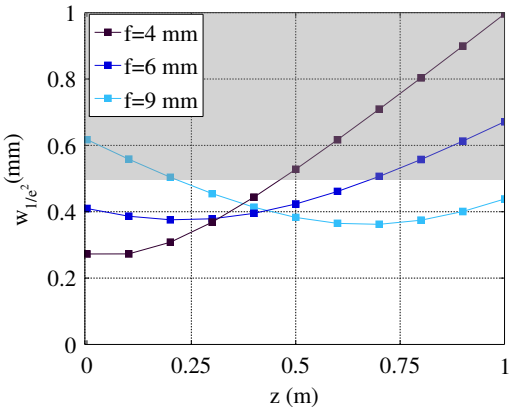


Figure 2.2.: Evolution of the infrared beam diameter for collimation lenses with different focal lengths. The grey area indicates the region where the signal would be blocked by the entrance aperture on the receiver's side.

Slow rotations of the bases can be compensated by implementing the Reference-Frame-Independent QKD (RFIQKD) [62, 63], which nevertheless requires the preparation of additional circularly polarised states. Another elegant solution consists in mapping the polarisation onto a rotation-invariant state, *e.g.*, the Orbital Angular Momentum (OAM) on Alice's side and to perform the inverse operation after the quantum channel [64]. The area of the liquid-crystal device called *q-plate* in the original paper is unfortunately not suited for our flat architecture. We will therefore rely on a live-basis alignment procedure involving a motorised wave plate on Bob's side.

As a temporal filtering process is applied to the detected events, synchronisation is primordial to obtain a meaningful sifted key. The detection window on Bob's side should be perfectly matched to the firing times of the laser, implying the requirement of a shared clock. Here we use an additional visible beacon laser modulated at Alice's repetition rate to perform this task. This beam is overlapped with the infrared signal using a miniature beamsplitter and can therefore also help the user aiming into the receiver.

2.4.3. Resulting architecture

The resulting sender architecture is shown in Fig. 2.3. The beams emitted by the VCSELs are focused onto the entrance facet of the waveguide chip using a Micro-Lens Array (MLA) with 250 µm pitch and polarised on their way by a micro-polariser array. A Neutral Density Filter (NDF) attenuates the light reflected from the gold polariser to avoid unstable emission of the VCSEL due to retro-injection. To facilitate the assembly and to increase the stability of the module, the micro-optical elements are separated by a combination of commercial glass spacers with standard thicknesses, in which a hole was etched via micro-powder blasting. The module has a size of $35\times20\times5\,\mathrm{mm}^3$.

In order to guarantee high coupling efficiencies into the waveguide chip, the optimal distance between the components was first simulated with *Zemax OpticStudio 14* using the specifications provided by the suppliers, and were refined later using the experimental values given in Table 2.4. When possible, the thickness of each element was measured using a 1:100 indicating calliper with an accuracy of 10 µm.

The results of the simulations are presented in Fig. 2.4, where the distance between

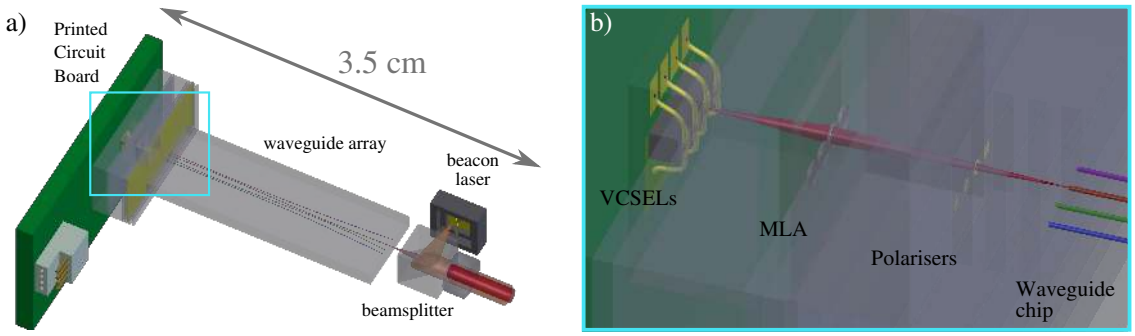


Figure 2.3.: 3D modelling of the resulting architecture. (a) View of the complete Alice module emitting polarised faint laser pulses at 850 nm. An additional red beacon laser is overlapped with the infrared signal to allow for convenient aiming into the detectors and synchronisation with the receiver. (b) Close view on the micro-optical elements.

Element	Length l	Material	Additional information
Conductive glue	15 ± 5 µm	Silver epoxy	
Single-mode VCSEL array (*VS*)	250 µm	GaAs	250 µm pitch Beam waist $w_{0,1/e^2}$=1.8 µm
Spacer 1	$1,140 \pm 10$ µm	Fused silica	Square hole a=2 mm
Spacer 2	185 ± 10 µm	Fused silica	Square hole a=1 mm
NDF	100 µm	Gelatin	
Micro-lens array	960 ± 10 µm	*BK7 & SU8*	250 µm pitch, f = 890 µm at 850 nm
Waveguide chip	1.8 cm	*Eagle2000*	Mode size: w_x=3.36 $\pm$ 0.05 µm, w_y=3.76 $\pm$ 0.05 µm

Table 2.4.: Summary of the selected components and relevant parameters used in the Zemax simulation. The length l of the components is defined along the beam direction.

the VCSEL array and the NDF is referred to as L, and D corresponds to the separation between the waveguide and the last spacer. High coupling efficiencies exceeding 50 % can be achieved, even for small deviations of the thickness of the different elements. Figure 2.4c shows that the lateral displacement of the waveguide is much more critical than the longitudinal shift. Mounting precisions below one micrometre are required to achieve efficient coupling into the four waveguides simultaneously.

Zemax simulations evaluated the back-coupling efficiency into the VCSELs to 0.4 % due to the high reflectivity of the micro-polariser. The NDF was therefore embedded to be on the safe side but could be removed in future versions. As the beam at the gold surface has a radius $w = 28$ µm, the size of the polariser was fixed to 120×120 µm in order to avoid diffraction effects.

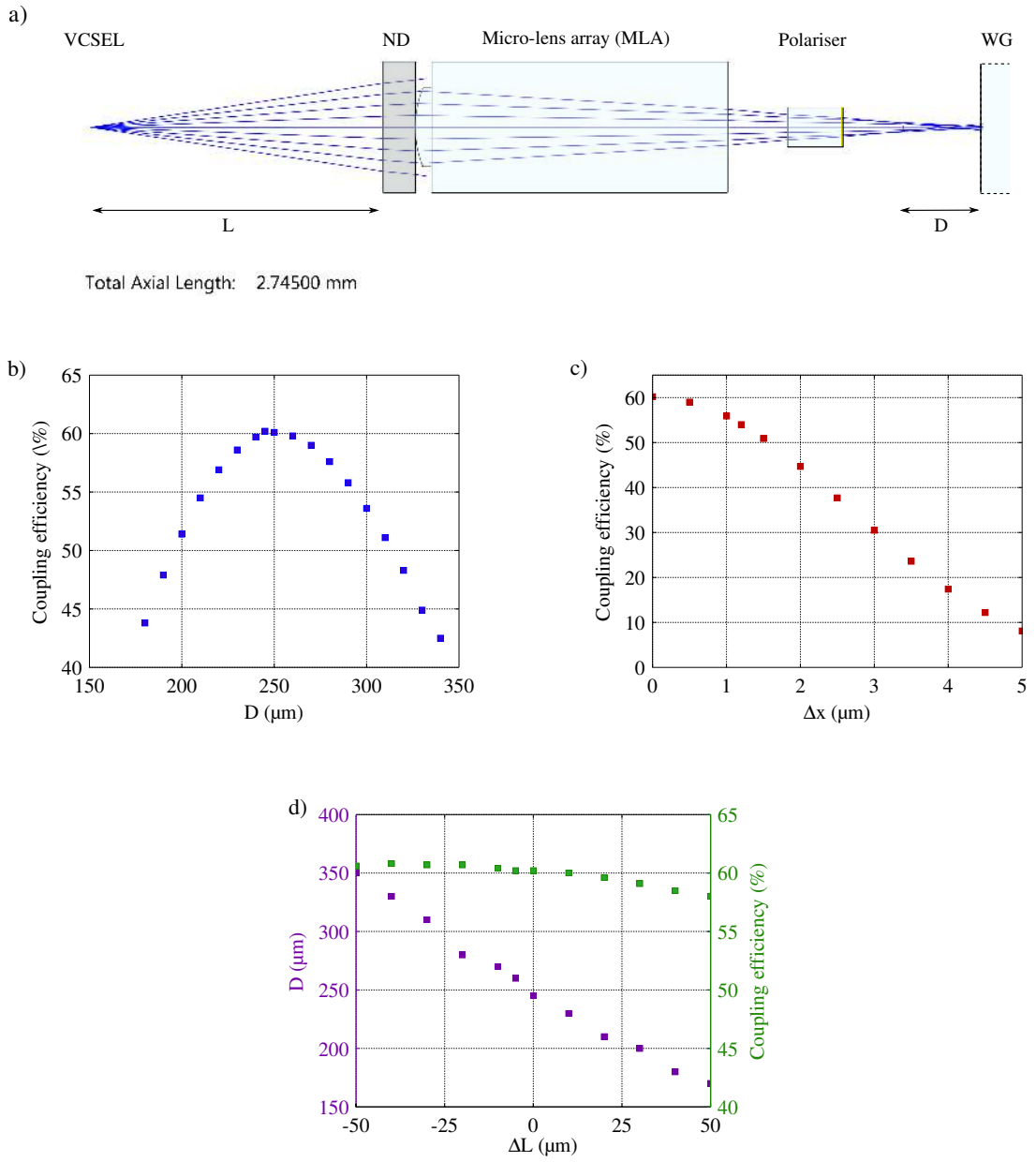


Figure 2.4.: Simulated coupling efficiency into the waveguide and position tolerance of the different elements obtained with Zemax. (a) Light propagation through the micro-optical architecture, computed by ray tracing. (b,c) Evolution of the coupling efficiency into the waveguide with its longitudinal and lateral displacement, respectively. The calculations are based on the physical beam propagation algorithm. (d) Influence of the tolerance of the different elements onto the total coupling efficiency. The deviation of L can be compensated by adapting D to ensure maximal coupling into the waveguide.

3. Generation of faint laser pulses with Vertical Cavity Surface Emitting Lasers

This section introduces the main properties of Vertical Cavity Surface Emitting Lasers (VCSELs) and investigates their suitability to generate indistinguishable short polarised pulses. Several arrays with either single-mode or multi-mode emission at $\lambda = 850\,\mathrm{nm}$ are compared. The evolution of the optical properties as a function of the current parameters is analysed in both Continuous-Wave (CW) and pulsed regimes, with a particular emphasis on the polarisation behaviour. We show that, despite the constant linear polarisation observed for all chips under continuous operation, unpolarised emission can be obtained under strong signal modulation for sub-nanosecond pulses, allowing for an external selection of the polarisation.

We additionally discuss the design of the driving electronics enabling an excellent temporal overlap between the different channels and examine other sources of indistinguishability that could open a side-channel in a quantum key distribution application.

3.1. General properties of VCSELs

3.1.1. Working principle

A VCSEL is a solid-state laser consisting of a direct band-gap semiconductor as active medium embedded in an vertical optical cavity. The device is designed in such a way that either optical or electrical pumping leads to a population inversion and thus to stimulated radiative recombination of electron-pair holes. High carrier densities are obtained by turning the gain medium into a potential well for the carriers. This spatial confinement is achieved by sandwiching this layer between two cladding films from a higher band gap material, as shown in Fig. 3.1a. This heterostructure has an optical thickness of λ, such that the standing wave building up in the surrounding cavity has an anti-node at the position of the well. In modern VCSELs, higher carrier densities and therefore better conversion efficiencies have been obtained by reducing the thickness of the active layer down to a few nanometres, resulting in a Quantum Well (QW) structure, in which electrons behave like a two-dimensional gas. Experience has shown that the optimal performance in terms of energy requirements is obtained for a succession of three QW separated by slightly thicker barriers. Strain engineering of the QW allows to maximise the gain for one crystal orientation by lifting the degeneracy of the valence-band and thereby optimising the band-gap and the band-offset [65].

The cavity is formed by two Distributed Bragg Gratings (DBR), which consist of alternating layers of different refractive indices n_i with a thickness $t_i = \lambda_0/(4n_i)$ to ensure constructive interference of the beams reflected at each interface. Typically more than 20 pairs are required at the bottom to reach a reflectivity of 99.9 %, while the upper DBR consists of less layers to allow top emission. The doping of the DBR has to be optimised to decrease their electrical resistance, but to avoid critical optical losses caused by free-carrier

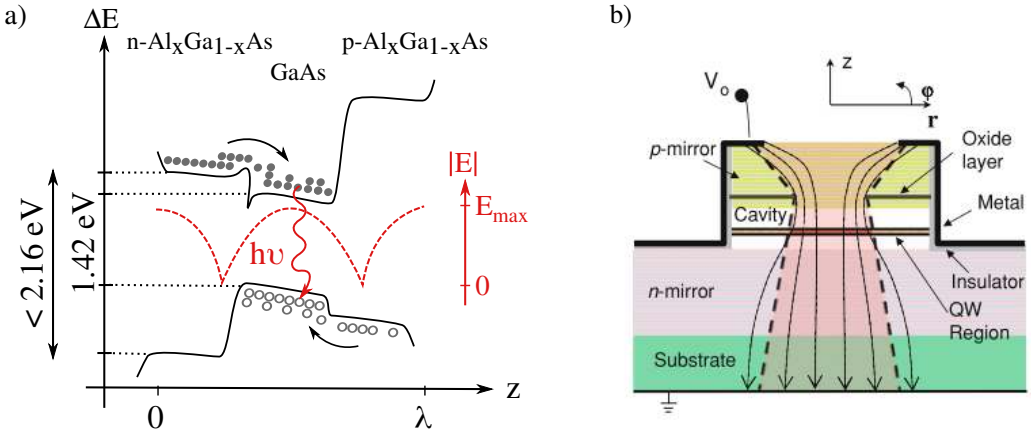


Figure 3.1.: Working principle of a Vertical-Cavity Surface Emitting Laser (VCSEL). (a) Simplified band structure of a forward biased GaAs/$Al_xGa_{1-x}As$ heterostructure emitting at $\lambda = 850\,\text{nm}$. Both injected holes and electrons are trapped in the potential well of the active material to ensure population inversion and therefore stimulated emission. The red curve shows the electric field distribution within the λ-cavity. (b) Schematic cross-section of an electrically pumped oxide-confined VCSEL (taken from [66]).

absorption.

The carriers are injected from both sides of the DBRs to reach population inversion. Lasing starts above a certain threshold current I_{th} (typically a few milliamperes) for which the optical gain exceeds the overall optical losses. At low injection currents, the refractive index increases at the center of the aperture due to higher photon and carrier concentration. Thermal lensing results in a self-focusing effect which decreases the losses for the guided fundamental mode. As the current is ramped up, this effect is slowly counterbalanced by optical Free-Carrier Absorption (FCA) in the DBR and Spatial Hole Burning (SHB) in the active medium, where high and inhomogeneous optical density leads to spatially dependent stimulated recombination. Both effects lead to higher losses for the fundamental mode, favouring higher-order (doughnut-shaped) modes with less intensity at the center. Higher currents also yield to higher losses due to Joule heating and current leakage. As the material gain curve is red-shifted several times faster than the cavity gain with intrinsic temperature, their misalignment results in a gain decrease at high currents referred to as *thermal roll-over*.

High conversion efficiencies around 60 % are achieved by focusing the injected carriers into a limited volume of the active medium. The device architecture is optimised to create a cylindrically symmetric distribution profile of both the carriers and the photons in order to obtain a Gaussian laser beam (see Fig. 3.1b) . The current flows from the top electrode ring electrode, and is further guided through an aperture of several micrometres etched in a thin oxide layer, which has replaced earlier confinement methods based on proton implantation or mesa-etching. Both apertures also serve to confine the generated photons, and their diameter determines if single-mode or multi-mode emission occurs. The latter is advantageous for many applications as it is connected to low thermal resistance, high output power and small beam divergence. While we mainly discuss electrical pumping of VCSELs, optical pumping from a shorter wavelength can sometimes be preferred as it

guarantees a more uniform carrier injection and a higher spatial quality of the output beam by preventing spatial hole burning. Although this operation mode is not considered in this thesis, we bear in mind that an optical field can strongly influence the emission properties of the VCSELs and that special care has to be devoted to avoiding retro-injection.

3.1.2. Polarisation behaviour

Standard edge-emitting diodes emit linearly polarised light, with a suppression of the orthogonal polarisation typically exceeding 1:100. The Transverse Electric (TE) mode, which lies within the plane of the active region, experiences at the same time higher reflectivity at the edges of the chip and higher gain due to better field confinement than the Transverse-Magnetic (TM) mode. VCSELs, on the other hand, do not possess any intrinsic polarisation selection mechanism. The emission is perpendicular to the active layer, thus ensuring an identical gain for all linear polarisations. Moreover, the gain medium GaAs as well as the DBR materials, has an isotropic zinc blende structure, *i.e.*, a cubic face centred As lattice with Ga atoms placed in the tetrahedral sites, as depicted in Fig. 3.2.

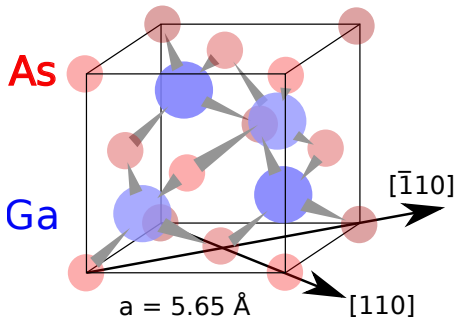


Figure 3.2.: Cristallographic structure of GaAs.

Experimental studies have nevertheless demonstrated that VCSELs emit linear polarisations oriented along either the [110] or the $[\bar{1}10]$ direction. This symmetry breaking can find its origin in the strain induced birefringence arising during the thin film growth, *e.g.* due to lattice mismatch, and that can be further enhanced during lasing due to both electro-optic and elasto-optic effects. As aforementioned, compressive strain is sometimes introduced on purpose in the quantum wells to enhance the gain. The quality of the QW interface can also have an influence onto the polarisation selection. All these effects contribute to a birefringence splitting $\Delta\nu = |\nu_{\bar{1}10} - \nu_{110}|$ typically in the order of a few gigahertz.

The polarisation dynamics of VCSELs is complex and often unpredictable, and we refer the reader to [66] for an exhaustive review of these properties. The dominant polarisation is mainly dependent of the injected current under continuous operation, and spin-flip relaxation models have been developed to explain the occurrence of polarisation switching. So far the polarisation behaviour has not been characterised in the strong modulation regime. When a precise control of the linear polarisation is required, a High Contrast Grating (HCG) with subwavelength dimensions can be placed on the top aperture. Such structures exhibit polarisation dependent reflection, and can therefore enhance one of the

linear mode and force the other to vanish. The working principle of the HCG is presented in Chapter 4.

3.1.3. State-of-the-art devices

The first double heterostructure exhibiting vertical emission at 1.2 µm was demonstrated at cryogenic temperature almost 40 years ago [67]. In the mean time, VCSELs have benefited from intensive development of new ternary and quaternary compounds as well as optimised device architectures to achieve stable operation at room temperature and over large temperature range ($\Delta T = 100\,^o$), wavelength tuning from the NIR [68] to the UV [69], low power consumption and high modulation speeds up to 40 Gbit/s [49, 50]. State-of-the-art VCSELs are developed for an emission wavelength around 850 nm, taking advantage of the Gallium Arsenide (GaAs) based materials that allows high quality epitaxy on GaAs substrate, low thermal resistance, low optical absorption and high reflectivity Distributed Bragg Mirrors (DBR) simultaneously.

While GaAs allows lasing between 650 nm and 1,300 nm, new active materials such as InGaAlAs [70, 71] have to be considered for telecommunication wavelengths, forcing the switch to Indium Phosphide (InP)-based technology. A major issue associated with the corresponding DBRs is their low thermal conductivity, which leads to overheating and limited efficiencies. Recent progress has been made at $\lambda = 1,550$ nm by modifying the complete architecture, *e.g.*, by fusing wafers based on different materials or by using Buried Tunnel Junction (BTJ) devices, where both DBRs are n-doped and therefore exhibit better conductivity than their p-doped counterpart. Such considerations have even enabled the integration of VCSELs onto Silicon-On-Insulator (SOI) platforms with direct coupling into a silicon waveguide [72], thereby proving the potential of VCSELs for high-speed optical circuits [73].

3.2. Manipulation of bare VCSEL chips

3.2.1. Testing and mounting

Several samples have been characterised in this work, starting with commercial multi-mode VCSEL arrays from VI-Systems (thereafter referred to as *VM*) featuring data rates up to 28 Gbit/s. While single VCSEL dies exhibiting single-mode emission are widely spread, arrays were not commercially available at the beginning of this study. Later on, VI-System kindly provided a 12-channel research sample (*VS*), with properties similar to its multi-mode counterpart. Finally, another matrix (*RS*) developed by the company RayCan and optimised for 2.5 Gbit/s transmission rates was also investigated. The main properties of the different Devices Under Test (DUT) are summarised in Table 3.1.

The VCSEL arrays are first tested with a probe station equipped with a top microscope and an infrared camera (Prof. Kotthaus' chair). The dies are placed onto an insulating substrate and electrically connected by two tungsten needles. An appropriate power source with a dedicated driver has to be used (see Section 3.2.2) in order to prevent electrostatic discharge and voltage peaks leading to irreparable damage of the active medium, as shown in Fig. 3.3d. If all lasers work properly, the array is glued with a conductive silver epoxy onto a small gold-plated Printed Circuit Board (PCB). Each diode is electrically connected

	Model	Emission	Data bit rate	Rise time	$I_{b,max}$	Θ_{1/e^2}	SMSR
VM	V25-850C4	MM	28 Gbit/s	14 ps	12 mA	17 ^{o}	–
VS	V25A -850C12SM	SM	28 Gbit/s	14 ps	5 mA	8.5 ^{o}	30 dB
RS	RC12xxx1-S	SM	2.5 Gbit/s	NC	5 mA	12 ^{o}	30 dB

Table 3.1.: Specifications of the 850 nm VCSEL arrays under test. MM: multi-mode, SM: single-mode, $I_{b,max}$: maximum bias current, SMSR: side mode suppression ratio. The rise time is calculated using the 20 % and 80 % reference levels.

to the PCB pads either via the back-side cathode or via a gold wire bonded on the top contact using a cross-groove needle.

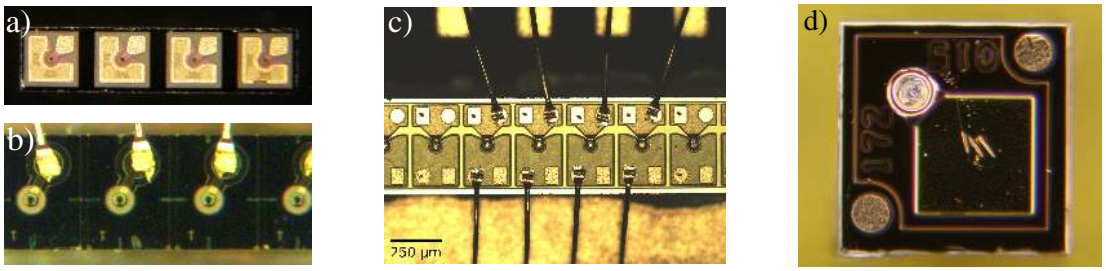


Figure 3.3.: Pictures of the different VCSEL arrays characterised in this section. (a) Multi-Mode Array from VI-Systems (VM) and (b),(c) Single-Mode Array from Raycan (RS) and VI-Systems (VS), respectively. (d) Image of a test VCSEL with melted active area, as the result of an electrostatic discharge.

3.2.2. Driving Electronics

While the driving electronics should provide a reliable current source for the VCSELs, it should also fulfil several requirements imposed by the QKD protocol. For instance, the four states generated by the four diodes should be completely identical, except for their polarisation. Precise and independent control of the pulse parameters is therefore crucial to obtain a perfect temporal overlap between the channels. Moreover, we set additional conditions such as a 100 MHz repetition rate to ensure a fast key generation process and an integration of all the required components onto a single Printed Circuit Board (PCB) to limit the footprint of the Alice module.

As a starting point we consider the electronics board designed for previous laser-based QKD experiments [11] capable of generating 1 ns electrical pulses at 10 MHz repetition rate. The pulse parameters such as length and amplitude are sent from a bash script to the board using a USB connection. A USB/UART transreceiver (*FT232r*, FTDI) first transfers the information to a microcontroller (*ATmega324p*, Atmel) which interprets the data and communicates the values to the dedicated components over a Serial Peripheral Interface (SPI). In particular, the pulse length n (8-bit word) is sent to an FPGA (*SPARTAN-3E*, Xilinx) which generates short pulses as follows: the embedded digital clock manager (DCM) first splits the external clock signal into two signals A and B, and delays the latter by a phase of $2n\pi/2^8$. The signal pair is further split into four different

doublets, one for each channel. Each pair is independently recombined into short pulses by appropriate logic operation performed by a look-up table, as depicted in Fig. 3.5b. One of the issues that have to be addressed is the disparity in phase and length of the resulting electrical pulses due to the different paths taken by the signals within the FPGA. As FPGA routing is not a trivial task for non-experts, the first solution consisted in trying to shift the clocks A_i and B_i by randomly switching additional logical components along the path of each pair. The electrical signals can be measured at the output of the FPGA using a 1 GHz probe tip connected to a storage oscilloscope. Although this method brought some improvement, temporal overlap of the resulting pulses could not be obtained (Fig. 3.4).

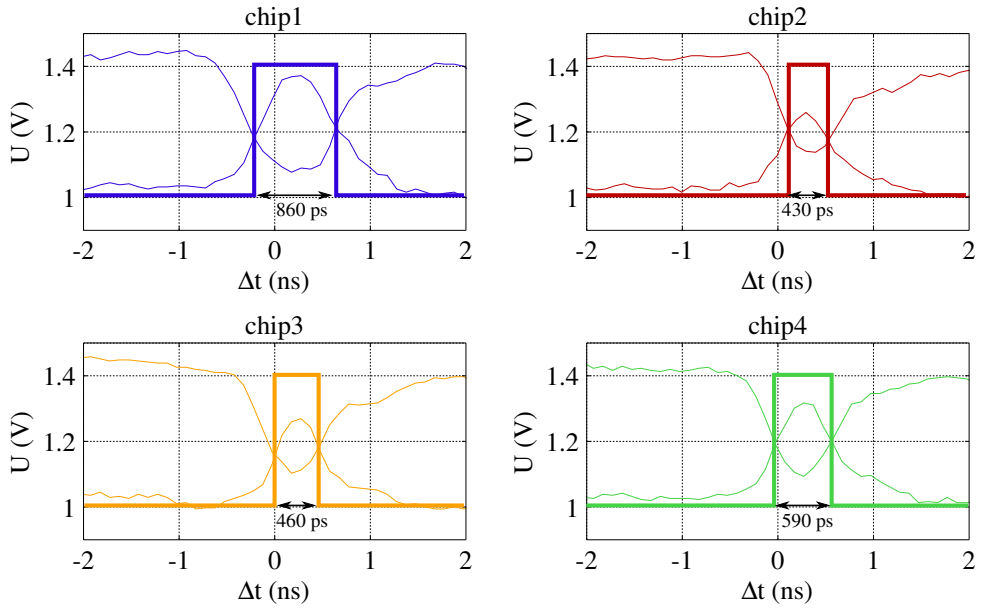


Figure 3.4.: Differential electrical pulses (LVDS) generated by the FPGA and measured with a 1 GHz voltage probe. The bold line shows the interpretation of the VCSEL driver. Successful synchronisation between the channels could not be achieved with this architecture.

In the next approach, the pulse generation is implemented according to the same principle but with discrete elements. Because repetition rate has to be simultaneously upgraded to 100 MHz, components based on differential signaling (either Emitter-Coupled Logic, ECL or Current-Mode Logic, CML) were preferred over Transistor-Transistor Logic (TTL) for their higher achievable bandwidth. The repetition rate increase to 100 MHz also entails a faster communication with the board for post-processing purposes (2 bits of information have to be retrieved for each qubit). The previously achievable baud rate of 115,200 bps imposed by the microcontroller is not suited for our application. The interface between the PCB and the computer is therefore replaced by a ready-to-use FPGA board equipped with a high-speed USB 2.0 transreceiver designed for 480 Mbps transfer rates.

A single dual-channel delay chip shifts two clock entries with 5 ps resolution to control both their absolute and relative phases. An *enable* pin allows to turn on or off the chip and thefore the pulse generation at each clock edge. This feature is used during the key distribution to select the outgoing qubit. A high-speed AND-gate then combines

the shifted clocks to generate the short pulse. The electrical and optical pulses have to reach the sub-nanosecond regime to ensure narrow time filtering and therefore high signal-to-noise ratios. The bandwidth of the laser driver has to be increased, and due to the lower power consumption of VCSELs compared to the edge-emitting diodes used in the prior experiment, the delivered currents have to be decreased. Among the tested VCSEL drivers, the model *ONET4291VA* from Texas Instruments demonstrated the best performance, with a bandwidth of 4.25 GHz and a bias and modulation output currents defined as:

$$I_{b,m} = 0.1 + s_{b,m} \cdot i_{b,m} \ \ (mA) \tag{3.1}$$

where $s_b = 0.047\,\text{mA}$, $s_m = 0.06\,\text{mA}$ are the step sizes and $i_{b,m}$ is a 8-bit value. The modulated signal is AC-coupled, and recombined over a bias-tee with the DC signal at the output of the driver to yield a pulse as depicted in Fig. 3.5c. The relatively slow Serial Peripheral Interface (SPI) between the FPGA and the driver prevents the intensity of the pulses to be changed at each clock cycle. In order to implement the decoy protocol, an alternative approach is proposed and detailed in Section 3.3.3.

Besides the choice of the electronics components, special care has to be devoted to the design of the printed board. The power consumption of the delay lines is quite high and is mostly responsible for the 3.5 A flowing through the circuit. Due to the lack of compact, stable 5 V power supply or battery with sufficient throughput, the PCB is supplied with 12 V. This voltage is then converted by a buck to the 3.3 V needed by the chips, dissipating about $\Delta U \cdot I \simeq 30\,\text{W}$. The PCB composite material $FR4$ contains glass fibres embedded in an epoxy matrix and exhibits therefore poor thermal conductivity ($0.5\,\text{W.m}^{-1}\text{.K}^{-1}$, 800 times smaller than copper). The heat builds up after turn-on of the board and results in a thermal gradient both in space and time, shifting the pulses of each channel due to the temperature dependence of the delay lines. To minimise this effect, different design rules were applied. First, a four-layer PCB with an internal copper layer connected to the ground is used, such that the heat generated by each chip is well drawn from its back-side and distributed among the whole surface. To allow for fast signals, the ground plane should be as close as possible to the surface, but is necessarily sandwiched between other layers, as top and bottom planes are reserved for soldering. In order to extract the heat from this internal plane, a certain number of thermal vias were integrated into the design, below and around each component. The walls of these holes are covered with copper, and electrically connected to the ground plane only. As the thermal conductivity directly scales with the copper surface, more vias with small diameters are more efficient for extraction than a larger one. Moreover, small radii prevent penetration of the tin within the hole that reduces the heat extraction by decreasing the convection area. The vias have to be carefully positioned onto the PCB to avoid creating a maze for the electrons on the ground plane. Once the heat is redirected to the back-plane of the PCB, it is efficiently removed via anodised heat sinks, glued with thermally conductive adhesive. The resulting CAD design is presented in Appendix A.

Due to the small diameters of the vias, the backside of the chips cannot be soldered manually from the other side of the PCB. To circumvent this problem, and also to obtain better soldered interfaces, a reflow soldering oven was acquired.

3.2.3. Optical characterisation set-up

For the optical characterisation, the VCSEL board is clamped onto a mirror mount and fixed onto a translation stage to select the diode to investigate. An aspheric lens with

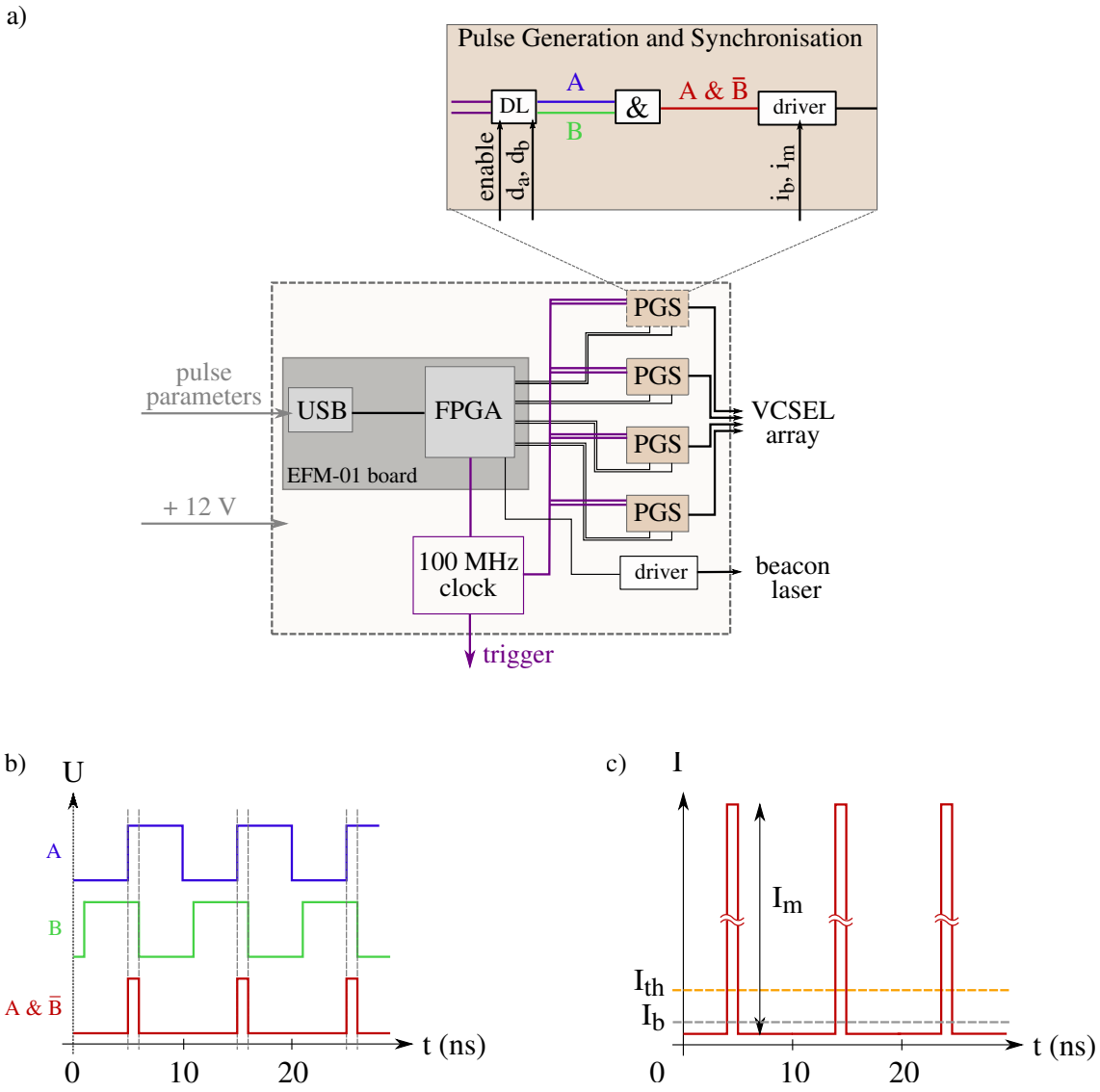


Figure 3.5.: Generation of short electrical pulses. (a) Simplified diagram of the driving electronics. (b) Generation of a short pulse using two delayed clocks A and B and an AND-gate. (c) Driver's interpretation of the modulation and bias currents.

a focal length of $f_1 = 4.5\,\text{mm}$ mounted onto a 3D-stage collimates the beam, which is efficiently focused onto the detector via two mirrors and a second aspheric lens with $f_2 = 11\,\text{mm}$, respectively.

For continuous-wave measurements, the intensity of the collimated beam is measured by a standard power-meter equipped with a silicon chip (*PM100* with sensor *S120C*, Thorlabs). In the pulsed regime, the photons are detected by an Avalanche PhotoDiode (APD) operated in Geiger mode and able to resolve single photons. Each photon creates an electron-pair hole in the active area, and can ionise other atoms due to the high ambient

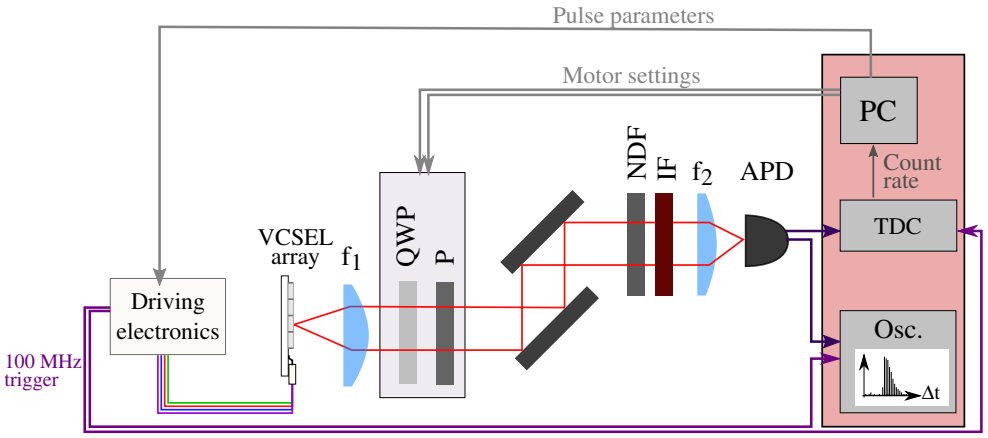


Figure 3.6.: Setup used for the characterisation of the optical pulses. DL: Delay Line; &: AND-gate; QWP: Quarter-Wave Plate; P: Polariser; NDF: Neutral Density filter; IF: Interference Filter; APD: Avalanche PhotoDiode; TDC: Time-to-Digital Converter. $f_1 = 4.5\,\text{mm}$, $f_2 = 11\,\text{mm}$.

electric field, thus generating a macroscopic current. The voltage is either decreased actively or passively over a RC-circuit to quench the avalanche. As long as a current circulates, no further photon can be detected and the APD is considered as *dead*. This *dead time* τ_d caused by the avalanche limits the number of detection events and prevents photon number sensibility within one optical pulse. However, the shape of the optical pulse can be reconstructed by statistically analysing the arrival time of the photon with respect to the corresponding electrical pulse. Such a time-difference histogram is a faithful image of the pulse shape provided that the average photon number per pulse is low enough ($\mu < 1$), in order to guarantee a non-zero detection of the trailing edge. The histogram is computed directly by a 4 GHz storage oscilloscope (Lecroy).

The average photon number impinging on the APD is measured using a Time-to-Digital Converter (TDC) with 81 ps resolution and adjusted via Neutral Density (ND) filters placed in the beam path. Given the repetition rate of the source ($R_{rep} = 100\,\text{MHz}$), the dark count rate R_{dark} of the APD, its efficiency η and the transmission T of the filters, the detection rate R_{det} is given by:

$$R_{det} = R_{rep} \cdot \eta \cdot P_\mu(n > 0) + R_{dark} \tag{3.2}$$

where $P_\mu(n > 0) = 1 - e^{-T \cdot \mu}$ represents the probability to have at least one photon in a pulse under assumption of a Poissonian distribution. The mean photon number μ can be therefore calculated as follows:

$$\mu = -\frac{1}{T}\, ln\left(1 - \frac{R_{det} - R_{dark}}{R_{rep} \cdot \eta}\right) \tag{3.3}$$

The experimental set-up includes a silicon APD (*PDM series*, MPD) with an active area of 50 µm, a resolution of 30 ps (jitter), low dark count rate below 40 Hz and saturation rate around 11 MHz. Alternatively, rather strong pulses can be visualized directly with a 10 GHz free-space GaAs photodiode (Newport) connected to a 20 GHz sampling oscilloscope (Agilent).

Using this set-up, the polarisation analysis can also be performed for both CW and pulsed modes. A polarisation state is completely defined by the Stokes vector

$$\overrightarrow{S} = \begin{bmatrix} S_0 = 1 \\ S_1 = \dfrac{I_H - I_V}{I_H + I_V} \\ S_2 = \dfrac{I_D - I_A}{I_D + I_A} \\ S_3 = \dfrac{I_R - I_L}{I_R + I_L} \end{bmatrix} \tag{3.4}$$

and can be represented onto a Poincaré sphere where the three axis correspond to the three components S_1, S_2 and S_3. The associated Degree Of Polarisation (DOP) is defined as

$$D = \sqrt{S_1^2 + S_2^2 + S_3^2} \tag{3.5}$$

and is equal to zero for unpolarised light and to one for fully polarised light. To determine $\overrightarrow{S}$ and D, it is sufficient to measure the light intensity in the three bases $\{H, V\}$, $\{D, A\}$ and $\{L, R\}$ using a quarter-wave plate and a polariser in the setup. To achieve high precision, high quality elements [1] are mounted onto stepper motors with 0.1^o step size. Using a bash routine, a full map of the polarisation behaviour as a function of of the electrical pulse parameters such as I_b, I_m or the length t_p can be established in a single measurement.

Additionally, the spectrum of the DUT can be finely measured with a free-space Fourier Transform Infra-Red (FTIR) spectrometer. Here the beam goes through a Michelson interferometer and the resulting interference fringes are Fourier-transformed to retrieve the spectral properties of the incoming light. The following measurements are realised with a spectrometer from Brucker (*Vertex 70*) exhibiting 0.014 nm spectral resolution kindly provided by the laser spectroscopy group led by Dr. Nathalie Picqué at the Max Plank Institute of Quantum Optics in Garching, Germany.

3.3. Experimental results

3.3.1. Continuous-wave regime

In this section the behaviour of the different VCSEL arrays is investigated under continuous-wave operation ($I_m = 0$). The power and the polarisation of the emitted light are first evaluated as a function of the injected bias current I_b, yielding the so-called LI-curve presented in Fig. 3.7. The extracted conversion efficiencies and threshold currents are shown in Table 3.2.

The multi-mode array *VM* exhibits very homogeneous properties, with threshold currents around 0.9 mA. The polarisation is stable across the whole current range with a DOP of about 90 %. The light exhibits an elliptical polarisation, with a ratio I_H/I_V slightly different for each diode. Their single-mode counterparts exhibit lower output power and

[1] The contrast of two crossed polarisers (Coddix) is above 1:10,000 and still reaches 1:5,000 with an additional wave plate (B. Halle) placed between them.

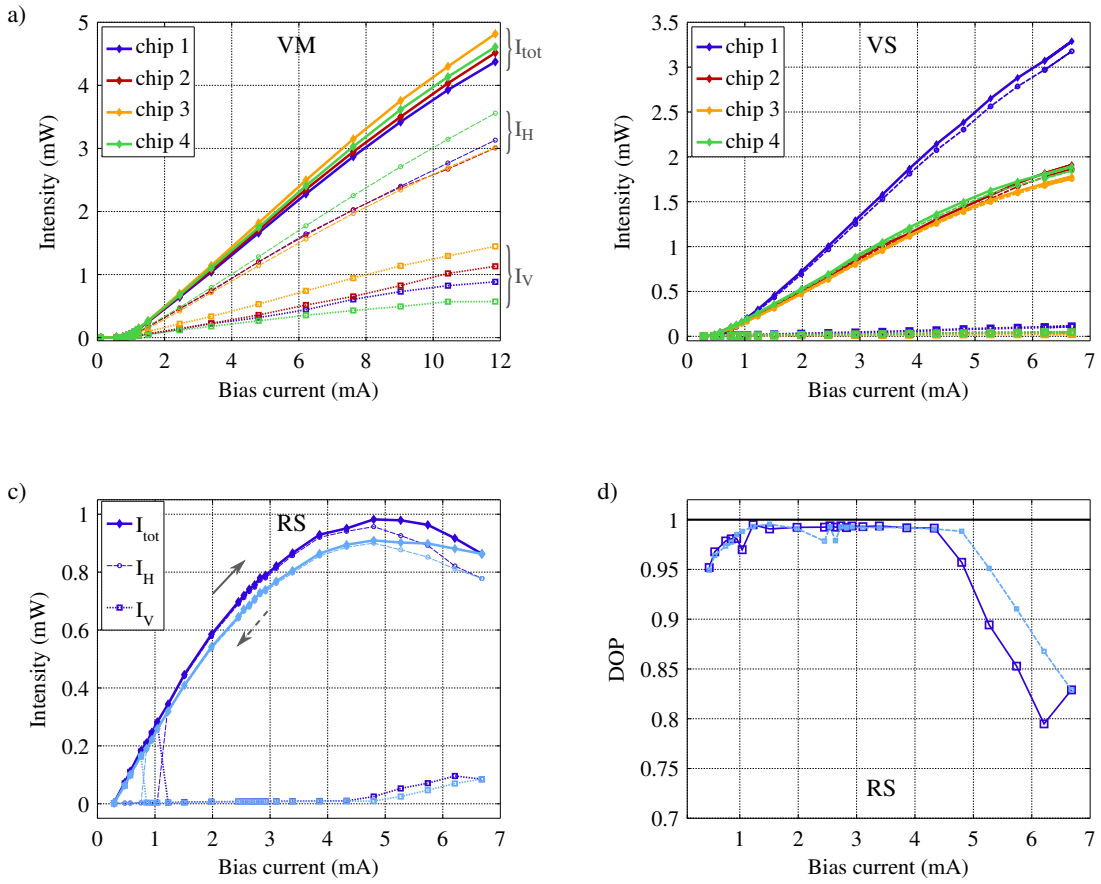


Figure 3.7.: Polarisation-resolved Light-current (LI) curves and resulting degree of polarisation obtained for the different arrays: (a) VM, (b) VS, (c),(d) RS. The dashed line with circle markers corresponds to the horizontal component, while the vertical component is represented by a dotted line with square markers.

Array	VM				VS				RS			
Chip	1	2	3	4	1	2	3	4	1	2	3	4
I_{th} (mA)	0.90	0.90	0.92	0.89	0.71	0.40	0.43	0.41	0.38	0.27	0.28	0.30
η (W/A)	0.42	0.43	0.47	0.44	0.59	0.29	0.27	0.31	0.28	0.37	0.37	0.38

Table 3.2.: Uniformity of the electrical and optical properties of the VCSELs accross the array. I_{th} and η denote the threshold current and the conversion (or slope) efficiency, respectively.

threshold current due to the limited active volume, except for the first chip which features an unexpectedly high conversion efficiency. The polarisation is mainly aligned along the H-axis also stable with an average DOP of 96 %. The optical properties of the last array (RS) exhibit a more complex dependency on the injected current (see Fig. 3.7c). First, the thermal roll-over is clearly visible from $I_b = 4\,\mathrm{mA}$, where the intensity saturates and starts decreasing, limiting the output power to 1 mW. Second, the LI-curve shows a hysteresis

for a scan speed of about 10 µA/s, which was not observed in the other VCSELs. Third, the linear polarisation mode suppression is stronger, with $D > 99\,\%$. A polarisation switch occurs around $I_b = 1\,\mathrm{mA}$ from V to H for increasing currents, also associated with a slight decrease in the DOP.

Generating the four different states $\{|H\rangle, |V\rangle, |D\rangle, |A\rangle\}$ with one VCSEL array seems compromised, as each of the neighbouring diodes exhibits the same linear polarisation under CW operation. The next section is dedicated to a deeper study of the polarisation behaviour in the pulsed regime.

3.3.2. Pulsed regime

For typical telecommunication applications, the VCSEL is always lasing, and the different intensity level required to encode a 0 or a 1 are obtained by a small signal modulation, with an Signal-to-Noise Ratio (SNR) of about 1:5. This operation mode allows for a fast optical response of the system, as the population inversion is already built up, and only a small fraction of additional carriers have to be injected in each pulse to observe a macroscopic change in intensity. In order to perform a QKD experiment with weak coherent pulses, optical pulses with high SNR have to be generated and then attenuated, such that the probability to observe a parasitic single-photon in the detection window around the weak pulses is close to zero. This is achieved by maintaining the bias current I_b as low as possible below the threshold current to limit background spontaneous emission, and by superimposing a large modulation signal I_m. Nevertheless, the number of carriers within the electrical pulse is limited by $I_{m,max} = 15\,\mathrm{mA}$ and by the pulse length, while their dynamics is restricted by diffusion through the resistive Bragg mirrors. Population inversion cannot be reached for bias-free operation, or experimentally not even with the bias offset supplied by the driver ($I_{b,min} = 0.1\,\mathrm{mA}$), even at maximum modulation current. An optimal bias current has therefore to be found to maximise the SNR while guaranteeing the generation of short optical pulses.

Polarisation properties

As a starting point, we consider the 1 ns optical pulse measured with the 10 GHz free-space photodiode and the sampling oscilloscope depicted in Fig. 3.8a. The strong modulation current forces the carrier density within the active medium to increase rapidly and to relax into a steady state with a characteristic period. Due to the fast response of the VCSEL, the relaxation oscillations are also observable in the optical domain. After 0.5 ns, corresponding to three oscillations, the light is polarised along the H-axis with the same DOP as in the CW regime. In contrast, the contribution of the H and V axes seem to be identical within the first oscillation. By adjusting the length of the electrical pulse with the delay lines, the optical pulse can be restricted to this region of interest. Unfortunately, this photodiode behaves non-linearly around its bandwidth limit. While the resulting optical trace is identical for both polarisations with this detector, a factor of at least two in intensity is detected by a power-meter. To circumvent this problem we reconstructed the pulse shape by recording a Time-Difference Histogram (TDH) between the detection signal from a free-space APD and the electrical pulse driving the VCSELs using a storage oscilloscope. The TDH is normalised by the number of clicks in the histogram to obtain the temporal probability distribution of the detection events. To be able to take into account the real intensity of the pulses, the probability distribution is multiplied by observed count

rate averaged over 30 seconds. The contrast C is defined as the probability that an event detected within a certain time window t_w is a signal photon. Due to AC-coupling at the output of the driver, the DC current flowing through the diode between two consecutive pulses is lower than in the continuous-wave regime (see Fig. 3.5c), resulting in a lower background emission. C is therefore evaluated by comparing the number of events within t_w around the pulse and a few nanoseconds away. A detection window of $t_w = 400\,\text{ps}$ is used to allow realistic temporal filtering with the commercial APDs that are integrated in Bob's setup.

Figure 3.8c shows the Stokes analysis of a 50 ps pulse with a reduced DOP of 33 %. The shape is now independent of the projection direction, and the amplitude along H and V differ only by a factor of 2 that can be easily compensated by current tuning. As illustrated in Fig. 3.8d, similar DOP and contrasts around 1:650 can be achieved for different current sets $\{I_b, I_m\}$. For sake of clarity only the minimum contrast, obtained for vertical polarisation, is shown.

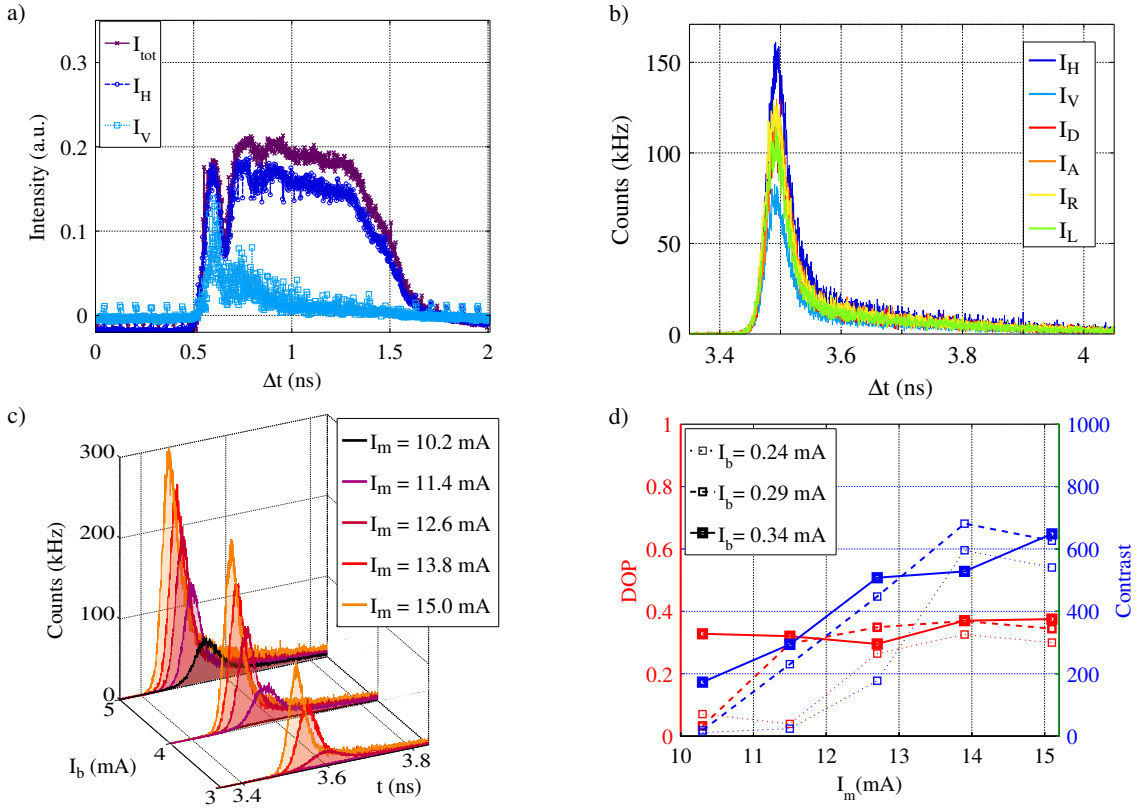


Figure 3.8.: Evolution of the pulse characteristics of the multi-mode VCSEL array. (a) Optical pulse trace measured with the 10 GHz free-space photodiode showing a change of polarisation within the pulse. (b) Time-difference histogram obtained with a free-space APD for short excitation pulses. Low DOP and therefore low dependency of the pulse shape and intensity with the polarisation. (c,d) Influence of the bias and modulation currents onto the optical pulse shape, DOP and signal-to-noise ratio ($t_w = 400\,\text{ps}$) for the fixed electrical pulse length defined in (b).

A similar behaviour was observed for both single-mode arrays, ruling out the possibility that an incoherent superposition of different spatial modes leads to an apparent *unpolarised* character of the pulse at the considered time scale. Pulses down to 40 ps FWHM with DOP down to 5 % have been observed for the central VCSELs of the 12-channel *VS* array. Unfortunately these diodes have been damaged during their characterisation, and the following measurements have been performed on the four VCSELs on the edge of the array. They exhibit much higher DOP around 50 % in pulsed regime. We conjecture that the additional mechanical strain induced by the dicing procedure is responsible for this disparity. As for the *RS* lasers, they exhibit DOP below 30 %, but much longer pulses of 200 ps with significantly lower count rates.

Although the optical pulses emitted by the *VM* array are very bright, as shown in Table 3.3, only a small fraction of the photon are in the fundamental spatial mode and can be efficiently coupled into the waveguide chip. From the free-space spectral measurements presented in Fig. 3.10a, only 3 % of the intensity is concentrated in this mode, leading to an exploitable mean photon number of about 300 per pulse. The *VS* array was therefore chosen as most suitable for the Alice module. The phase and intensity of each pulse was finely tuned in order to obtain excellent temporal overlap between the different channels, as shown in Fig. 3.10d

Array	*VM*	*VS*	*RS*
μ_{max}	9,000	550	80

Table 3.3.: Approximate mean photon number μ achievable for all polarisation states with the bare VCSEL diodes.

Spectral properties

The influence of the electrical pulse parameters onto the spectral properties of the emitted light was also investigated. Figure 3.9 shows the normalised FTIR spectra of pulses emitted by the *VS* array as a function of the length specified to the delay lines. The fundamental mode has a wavelength of 853.2 nm, while the first higher order mode is located around 851.9 nm. Although side-mode suppression ratio above 30 dB is achieved under CW operation, the losses experienced by the higher-order modes during a single pulse are not sufficient to lead to their complete extinction. The short rather unpolarised pulses that are intended to be used in the QKD experiment (black curve) exhibit a narrow emission line superimposed with a broader background that might be related to (amplified) spontaneous emission. Both contributions of the V polarisation and of the parasitic background decrease with increasing pulse length, suggesting a close correlation between them that will be further explored in the photon statistics analysis.

Due to the birefringence splitting of 26 GHz observed between orthogonal polarisations, the four combinations of H and V required by the BB84 protocol cannot be spectrally indistinguishable. On average, smaller splittings were observed for pulses exhibiting lower DOP, although the most valuable samples to confirm this hypothesis could not be measured before their breakdown. The resulting wavelength mismatch of the different VCSELs within the three arrays, potentially opening a side-channel in the final QKD experiment, is illustrated in Fig. 3.10.

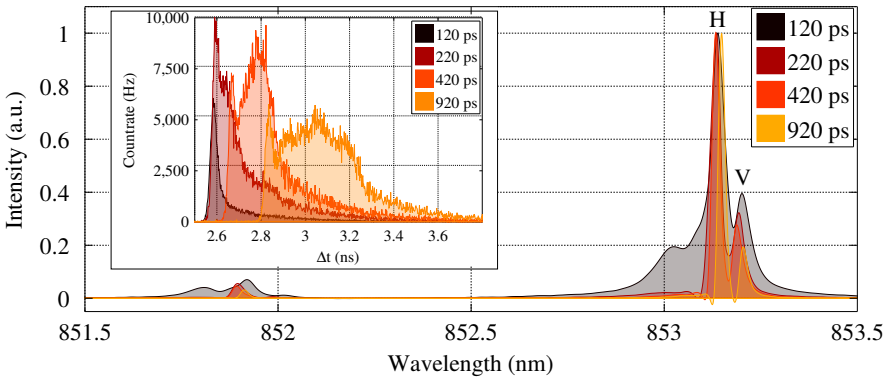


Figure 3.9.: Evolution of the optical pulse spectrum with the programmed electrical pulse length. The intensity is normalised for easier comparison and the corresponding temporal shape is shown in the inset.

The different channels of the *RS* array (Fig. 3.10b) exhibit relatively high spectral overlap, while the spectra are close but clearly distinct for the VI-System matrices. Internal heating of the diode during the measurement can be ruled out as a principal cause, as this effect would red-shift the spectra according to the measurement sequence, *i.e.* in the ascending order of the chips. The influence of the external temperature was nevertheless evaluated by gluing a thermistor and a Peltier element on the backside of the PCB using thermally conductive adhesive. The temperature was regulated using a PID feedback loop, and a stabilisation only down to $\Delta = 0.1^oC$ was achieved during the spectrum measurement due to strong air conditioning, leading to a shift of 0.06 nm/K, consistent with the literature.

For most applications, the spectral tuning of a few nanometres obtained by current tuning is sufficient. A precise control of the intensity is essential in our experiment and other wavelength shifting mechanisms have thus to be exploited. A possible solution consists in integrating a heater in the design of the VCSEL architecture [74], thereby allowing shifts up to 10 nm. Broader calibration ranges up to 85 nm [71] can be obtained using Micro-Electro-Mechanical Systems (MEMS). The principle is to bend the membrane forming the upper DBR in order to change the cavity length in the vertical direction. Combined with an optimised device design, these structures can also achieve single-mode emission and high modulation speeds [75], and are therefore suitable for integration in our QKD sender unit. As MEMS-VCSEL arrays are not commercially available yet, this solution was not implemented in this work but is considered as a viable alternative for future prototypes.

3.3.3. Generation of decoy states

The security of the BB84 protocol can be guaranteed with weak coherent pulses by implementing the decoy protocol. As explained in Section 2.3.1, this method requires the preparation of polarised pulses with different intensities. Unfortunately, the communication speed with the VCSEL driver is not sufficient to modify the intensity at each rising clock edge. To circumvent this issue, we follow the idea first proposed in [76] to turn two diodes on simultaneously to obtain a pulse with different mean photon number. The

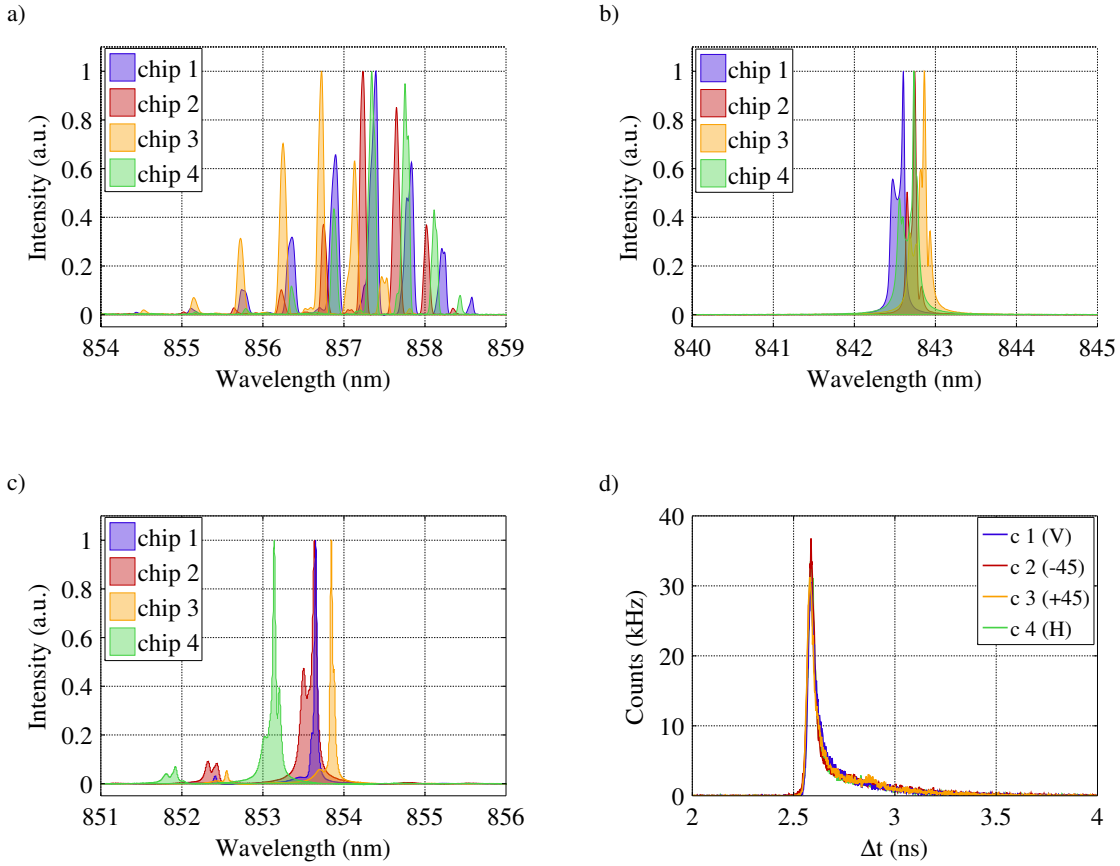


Figure 3.10.: FTIR spectra corresponding to short optical pulses exhibiting low DOP and emitted by (a) the *VM* array, (b) the *RS* array and (c) the *VS* array. (d) Temporal shape of the pulses corresponding to the spectrum pre(c). The amplitude and phase of each signal can be finely tuned to obtain excelsented in lent temporal overlap between the channels.

resulting decoy states have higher mean photon numbers μ_D than the signal states, and undefined polarisation as the phase between both diodes is not known. In this particular case, the decoy states cannot be used to generate the key.

This implementation was tested in an independent optical setup with the *RS* array [77]. The beams of two different VCSELs are overlapped using a $f = 30\,\text{mm}$ lens and an APD without focusing optics is placed at the center of the collimated beam in order to detect both pulses with the same probability. Figure 3.11a confirms that the temporal shape of the decoy and signal states is identical. The mean photon number μ_D calculated using Eq. 3.3 is expected to be the sum of the independent detection rates, but is experimentally found to be higher on account of electrical cross-talk on the driving board (see Fig. 3.11b).

For sake of completeness the supposedly Poissonian statistics of the light was characterised using a Hanbury Brown-Twiss (HBT) setup [78], as depicted in Fig. 3.12a. The temporal coherence of the source is tested by splitting the incoming beam into two components and by recording the arrival time of the photons detected by each APD using a TDC. The time differences between events in different arms are plotted as a histogram

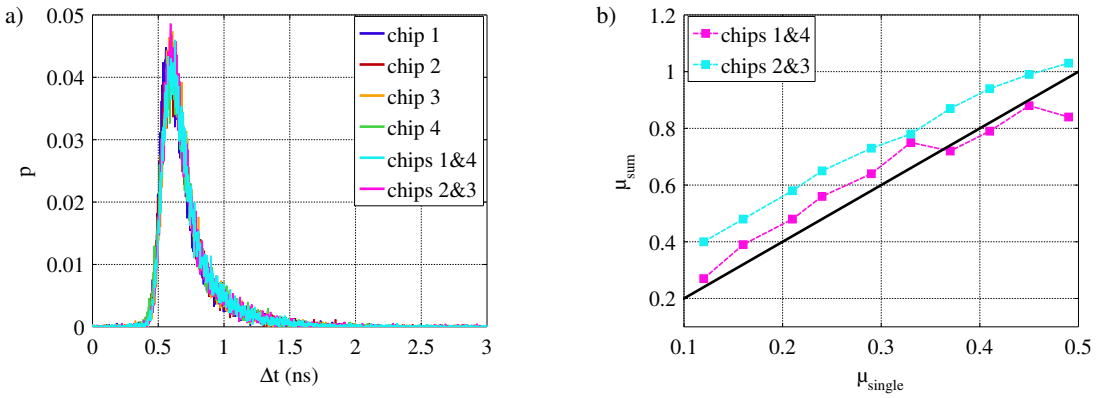


Figure 3.11.: Properties of the generated decoy states obtained by temporal overlap of two signal states. (a) Probability distribution of the arrival times of the photons for signal and decoy states. (b) Mean photon number of the resulting decoy states.

and normalised in order to reconstruct the second-order correlation function

$$g^2(\tau) = \frac{\langle I(t) \cdot I(t+\tau) \rangle}{\langle I(t) \rangle^2} \tag{3.6}$$

which is proportional to the probability to observe a photon at a time τ when a photon has already been detected at a time t. For classical light, it can be demonstrated that $1 \leq g^2(\tau) \leq 2$, where a constant function $g^2(\tau) = 1$ corresponds to coherent light with a Poissonian distribution (see Eq.). Thermal light follows a Bose-Einstein distribution defined as

$$P_\mu(n) = \frac{\mu^n}{(1+\mu)^{n+1}} \tag{3.7}$$

and exhibits a *bunching* behaviour, *i.e.*, higher probability to observe two photons separated by a time interval $\tau = 0$, such that $g^2(0) = 2$ and $g^2(\tau) = 1$ for large τ. Quantum mechanics, on the other hand, allows arbitrary values of $g^2(\tau)$. A number state $|n\rangle$ containing exactly n photons is for instance characterised by a dip in the autocorrelation function corresponding to

$$g^2(0) = \frac{n^2 - n}{n^2} = 1 - \frac{1}{n} \tag{3.8}$$

Single-photon states can therefore be undeniably identified by their *anti-bunching* behaviour corresponding to $g^2(0) = 0$.

The characterisation of $g^2(0)$ thus delivers essential information on the statistics of the light. In this measurement, a polariser fixed along the H axis was used to remove the polarisation dependence of the beamsplitter. The VCSELs were pulsed under strong modulation, such that the emitted light is minimally polarised along V. The time-difference histogram presented in Fig. 3.12b results from a start-stop analysis of 330,000 detection events. The number of events is integrated over each period of 10 ns and normalised such that the autocorrelation function approaches 1 at large τ. The histogram is not centered at $\tau = 0$ due to different cable lengths connecting the APDs with the TDC. Surprisingly, the pulses emitted by all the chips exhibit bunching, with $g^2(\tau_0) \simeq 2$, indicating the a

Bose-Einstein distribution. A strong correlation due to after-pulses of the APDs or other systematic errors was ruled out as a flat g^2 function was obtained for a highly attenuated continuous laser beam. The reconstruction of the statistics from this measurement has been developed in [77]. The Bose-Einstein distribution is confirmed for signal states, while decoy states show a lower degree of bunching.

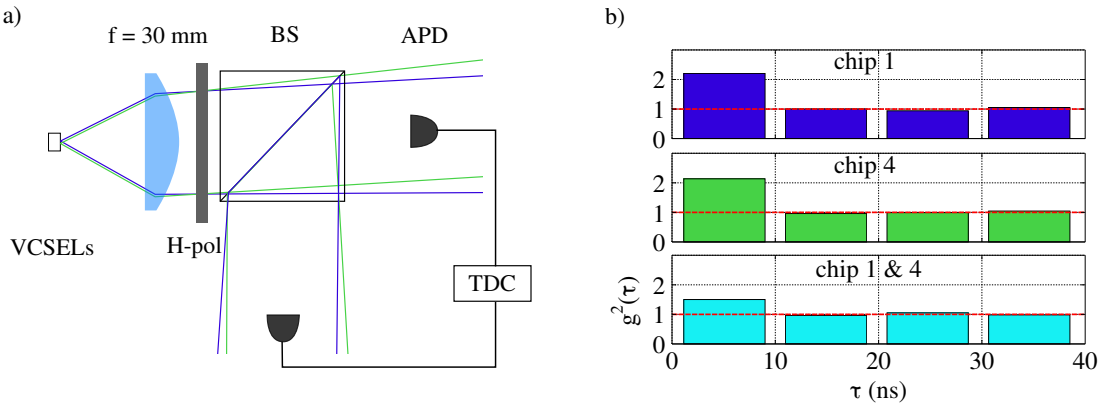


Figure 3.12.: Characterisation of the photon statistics in the strong modulation regime. (a) Schematic representation of a Hanbury Brown-Twiss (HBT) setup. (b) Resulting autocorrelation function for signal states (individual pulses) emitted by the *RS* array and for the corresponding decoy states.

In order to verify the existence of these features in the final module, a deeper study was performed onto a second single-mode array from VI-Systems that will be referred to as *VS2*. The $g^2(\tau)$ function was characterised for different pulse parameters and for different polarisation directions. Figure 3.13a and 3.13b show that only a small bunching with $g^2(0) \leq 1.1$ is observed along the H-axis, corresponding to the dominating mode, for short pulses, and disappears for long pulses. We believe that the deviation from a perfect Poissonian source is due either to a small amount of (amplified) spontaneous emission present at the beginning of the pulse or to small intensity fluctuations (see Fig. 3.8a) that are averaged out for long pulses. The weak mode, however, exhibits a clear thermal behaviour ($g^2(0) = 2$) at low currents and short pulse lengths, with a bunching reaching $g^2(0) = 6$ for stronger and longer pulses. Although more theoretical investigations are necessary to explain this behaviour, we consider the following considerations as a good starting point. In the absence of current, the degeneracy valence band is lifted due to stress birefringence, leading to a higher band gap for the V axis. The population in the conduction band, as well as the transition probability are therefore reduced compared to the H-axis. As the carriers are injected, spontaneous emission fist occurs along both directions, but population inversion is reached earlier for H. Additional electro-optic and elasto-optic effects enhance the unbalance between the reservoirs of both polarisations and yield a quick extinction of the weak mode, as shown in Fig. 3.8a. The value of $g^2(0)$ being also strongly correlated to the noise or the intensity fluctuations of the source, we conjecture that the high values observed arise from the strong damped oscillations experienced by the weak mode.

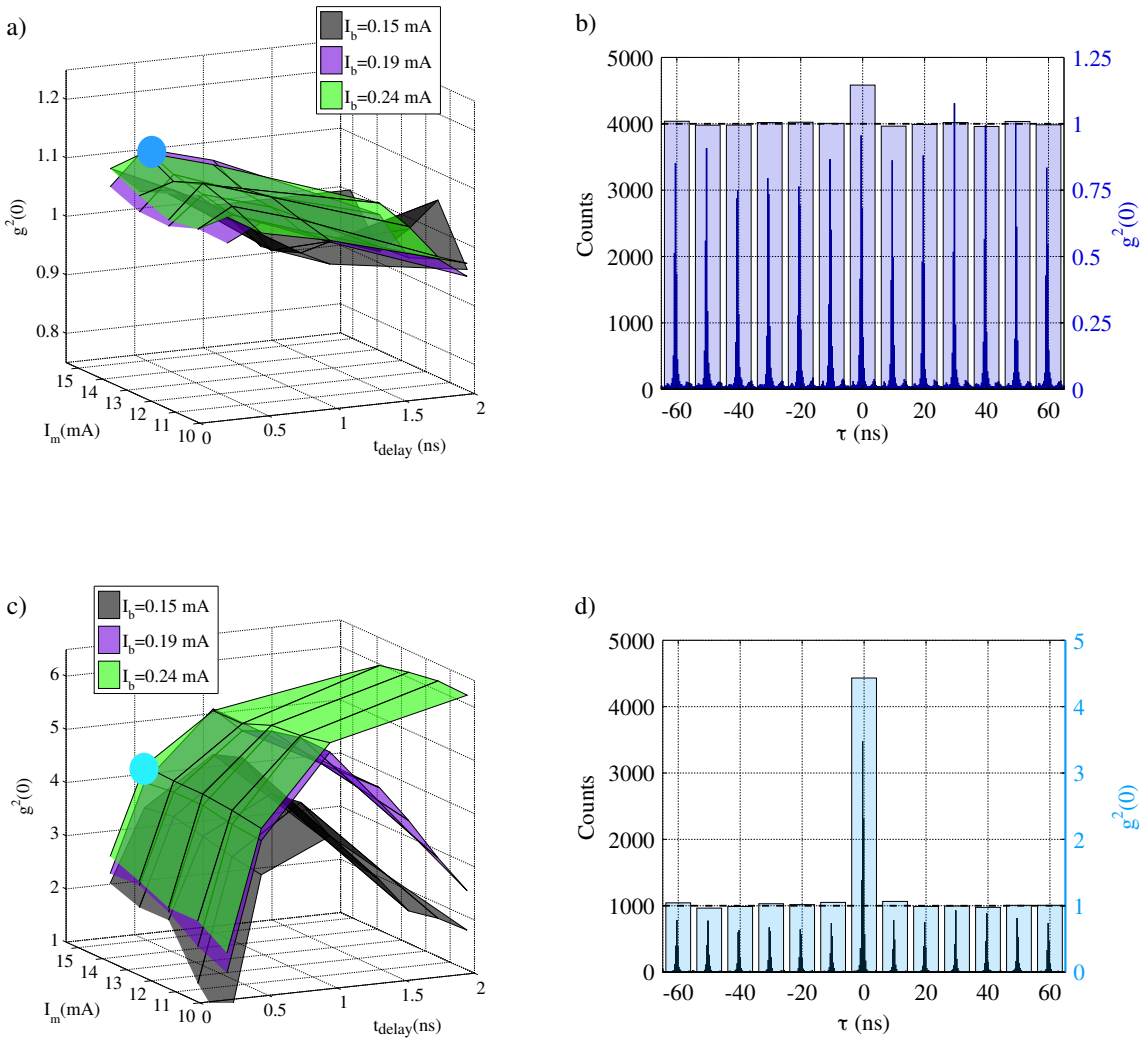


Figure 3.13.: Influence of the electrical pulse parameters onto the photon statistics of the WCP generated by the *VS2* array (t_{delay} denotes the programmed electrical pulse length). The optical pulses are analysed along (a,b) the H-axis (dominating mode) and (c,d) the V-axis (weak mode). Two time-difference histograms (b,d) are shown for a special set of parameters denoted by blue disks in the three-dimensional maps ($I_b = 0.24\,\mathrm{mA}$, $I_m = 15\,\mathrm{mA}$, $t_{delay} = 500\,\mathrm{ps}$).

4. Polarisation control of weak coherent pulses

The short pulses emitted by the VCSELs exhibit a rather low degree of polarisation, thus enabling external control of the polarisation of each channel by a micro-polariser. In order to generate the four states required for the BB84 protocol, an array of four rotated polarisers separated by 250 µm has to be manufactured. Wire-grid polarisers are good candidates for this application, as they feature high extinction ratio and can be fabricated in arbitrary size and orientation using standard clean room processing. This section describes the working principle of such structures, where TE-modes are almost perfectly reflected and TM-modes experience high transmission due to coupling to surface plasmons. The optimisation of the grating parameters using Finite-Difference in Time-Domain (FDTD) simulations is presented, along with the consequent fabrication of the samples. The predicted and observed performances are compared, and the influence of small geometrical variations of the grating are evaluated. Taking into account the fabrication imperfections, a new optimisation model enables us to achieve excellent agreement with the observed response and to re-optimise the grating parameters to ensure experimental extinction ratios well above 1,000 at 850 nm.

4.1. Theory of wire-grid polarisers

A wire-grid polariser consists of a periodic array of subwavelength rectangular apertures within a thin metal film. As depicted in Figure 4.1, the grating is characterised by the period p, the slit width w and the metal thickness h. We consider a monochromatic electromagnetic radiation with wavelength $\lambda = 850\,\text{nm}$ propagating along the z-axis, such that $E(x, y, z, t) = E(x, y) \cdot e^{-i(\omega t + kz)}$. To be consistent with the literature, the wave polarised along the x-axis, *i.e.*, perpendicularly to the metal stripes, is referred to as TM-polarisation (also called "s" or "σ"-polarisation), while the TE-polarisation (also "p" or "π"-polarisation) is considered to be parallel to the stripes.

The following calculations as well as experimental samples focus on gold due to its current availability as deposition material in our clean room. Wire-grid polarisers made of silver [52] or molybdenum [79] have also been demonstrated at infrared wavelengths and the elements of theory we present remain valid for all such materials with comparable optical properties. The complex refractive index is calculated using the Lorentz-Drude dispersion model to take into account the contribution of both bound and delocalised electrons. This relation is given by

$$\varepsilon(\omega) = \varepsilon_D(\omega) + \varepsilon_L(\omega) = 1 + \sum_{n=1}^{N} \frac{\sigma_n {\omega_n}^2}{{\omega_n}^2 - \omega^2 - i\omega\gamma_n} \tag{4.1}$$

where ω_n is the n^{th} Lorentz resonance frequency. The optical constants σ_n, ω_n and γ_n used in the following have been obtained from thin films measurements [80]. For 850 nm

the values of the permittivity and of the refractive index are $\varepsilon_m = -23.8395 + 2.2359\,i$ and $n_m = 0.2287 + 4.8879\,i$, respectively.

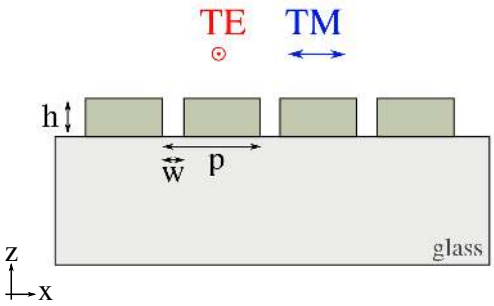


Figure 4.1.: Geometry of a gold wire-grid polariser on a glass substrate. The grating is characterised by the metal height h, the slit width w and the period p.

If $p \ll \lambda$, the behaviour of the polariser can be described using the Effective Medium Theory (EMT)[81]. The metal film with subwavelength discontinuities is equivalent to a birefringent, nevertheless homogeneous medium with a polarisation dependent effective refractive index such that

$$n_{TE} = \sqrt{n_m^2\,(1 - \frac{w}{p}) + \frac{w}{p}} \tag{4.2}$$

$$n_{TM} = \frac{n_m}{\sqrt{(1 - \frac{w}{p}) + n_m^2 \frac{w}{p}}} \tag{4.3}$$

Ref. [82] describes a powerful design protocol based on this method. However, this approximation is no longer valid for $p \lesssim \lambda$ and a deeper understanding of the underlying physical principles becomes necessary to design high performance devices. We start by analysing the evolution of the TE-polarised waves through the structure.

4.1.1. TE-Polarisation

To understand the behaviour of the light in the absence of plasmon excitation, it is sufficient to first consider a metal film with a single slit of width w. We adopt the standard microwave approach [83], where the wave can be guided in air through a rectangular aperture delimited by perfectly conducting walls, *i.e.*, with infinite conductivity σ. According to waveguide theory, the incident wave can only propagate through the slit if its wavelength λ is above the cut-off wavelength λ_c of the fundamental mode, where $\lambda_c = 2\,w$. The propagation constant β in the aperture is defined as

$$\beta^2 = \frac{\omega^2 - m^2\omega_c^2}{c^2} \qquad \forall\ \omega \leqslant \omega_c \tag{4.4}$$

with ω_c the cut-off angular frequency, m the mode number (in the following assumed to be 1) and c the speed of light. The guided wave can be expressed as $E(x, y, z, t) = E(x, y) \cdot e^{-i(\omega t + \beta z)}$ with $z \in [0, h]$. For $\lambda > \lambda_c$, β becomes purely imaginary and the field decays exponentially in the slit with a constant

$$\beta = \sqrt{\frac{\omega_c^2 - \omega^2}{c^2}} = \frac{2\pi}{\lambda}\sqrt{\frac{\lambda^2}{4w^2} - 1} \tag{4.5}$$

resulting in a penetration depth of $\delta_{air} = 1/\beta$. However, real metals exhibit a finite conductivity, which leads to a small penetration of the field within the metal, as depicted in Fig. 4.2a. The optical field decays exponentially in the walls with a constant δ_{skin} called *skin depth*. A more accurate description of the propagation of the TE-waves can be obtained by solving numerically the eigenvalue problem of a metallic waveguide with a complex refractive index [84].

Figure 4.2b compares the propagation constants delivered by both models. The finite conductivity extends the slit width to an effective value $w + 2\delta_{skin}$, and forces the whole curve to shift towards shorter w by $2\delta_{skin}$. Moreover, the skin depth yields a finite penetration of the field $\delta_{air} = \delta_{skin} = 1/\beta(0) = 27.8\,\text{nm}$ even for vanishing w, while perfect conductivity predicts $\delta_{air} = 0$ and therefore $\beta(0) \to \infty$.

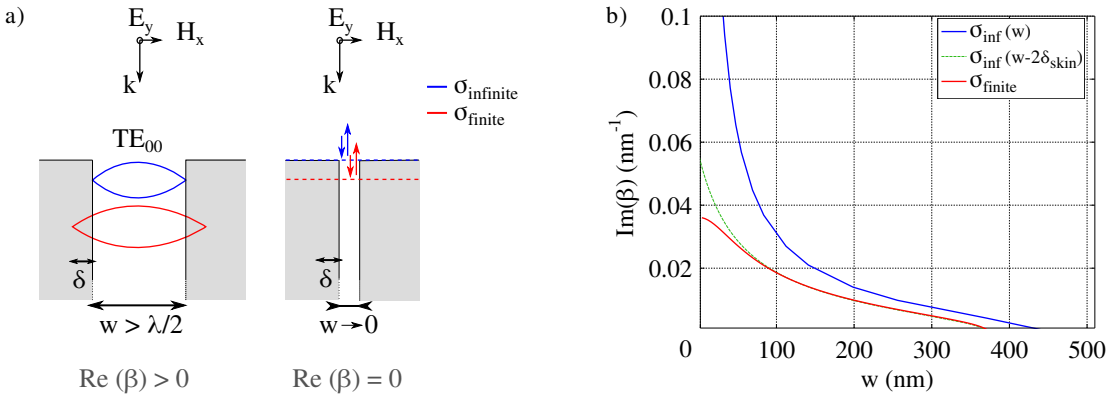


Figure 4.2.: Influence of the slit width w onto the propagation of the TE-polarised waves. The propagation constant β is real for $w > w_c$ and becomes purely imaginary for $w < w_c$, leading to an exponential decay of the field. (a) Illustration of the effect of the finite conductivity onto the propagation constant. The left-hand side corresponds to $w > w_c$, allowing for propagation through the slit, while the right-hand side shows the limiting case for $w \to 0$. Here δ denotes the skin depth. (b) Theoretical calculation of the imaginary part of β using a model based on perfect conductivity (blue curve) or on the real refractive index of gold (red curve).

4.1.2. TM-polarisation

Anomalous transmission of TM-polarisation through a metallic grating was first pointed out by Wood in 1902 [85]. The transmission spectrum of the incandescent light through such grating ($p = 1.8$ µm) exhibited maxima and minima with asymmetrical shapes and unequal broadening, depending on the incidence angle. Using the recently developed grating theory, Rayleigh [86] could explain that a dip in transmission appeared for a particular wavelength when a higher order was diffracted parallel to the surface. The position of the minima derived from this theory reasonably matched the experimental data, but the peaks in transmission observed for specific wavelengths remained unexplained. Fano [87] conjectured a few decades later that these resonance phenomena resulted from the interaction between different scattering processes, involving a coupling between the incident field and a surface wave called *plasmons* or *Surface Plasmon Polariton* (SPP).

The existence of these surface waves was already known for flat metal-dielectric interfaces as a possible solution of Maxwell's equation since 1909 [88].

The interest of plasmons excitations in gratings rose again with the development of nanofabrication techniques allowing high quality, two-dimensional arrays of subwavelength apertures or surface corrugations also for the optical regime. TM-polarised waves have been demonstrated to experience Extraordinary Optical Transmission (EOT) in these structures [89], recently reaching 95 % at infrared wavelengths [90]. It was proven that an artificial, periodic modulation of the metal surface would result in periodic variations of the electron density, therefore mimicking the plasmons properties, and often referred to as *spoof plasmons* [91].

Before moving on to complicated nanostructures, let us recall the general properties of SPP at a plane interface between a metal (1) and a dielectric (2). A wave propagating at such an interface must satisfy Maxwell's equations

$$\nabla \times \overrightarrow{E} = -\frac{\partial \overrightarrow{B}}{\partial t} \tag{4.6}$$

$$\nabla \times \overrightarrow{H} = \frac{\partial \overrightarrow{D}}{\partial t} \tag{4.7}$$

with $\overrightarrow{D} = \varepsilon_0 \varepsilon_r \overrightarrow{E}$ the electric displacement and $\overrightarrow{H} = \overrightarrow{H}/\mu_0$ the magnetising field. Using the monochromatic, plane wave assumption, $E_y = 0$ and $\dfrac{\partial \overrightarrow{E}}{\partial y} = 0$, we can rewrite Eq. 4.7 as

$$\begin{cases} E_{x,i} &= \dfrac{k_{z,i}}{\omega \varepsilon_0 \varepsilon_{r,i}} H_{y,i} \\ E_{z,i} &= \dfrac{k_{x,i}}{\omega \varepsilon_0 \varepsilon_{r,i}} H_{y,i} \end{cases} \tag{4.8}$$

where the subscript i refers to the considered material. The continuity of the field in the (x,y) plane requires $E_{x,1} = E_{x,2}$, $H_{y,1} = H_{y,2}$ and for the z-components $D_{z,1} = D_{z,2}$, and consequently leads to

$$\begin{cases} \dfrac{k_{z,1}}{\varepsilon_{r,1}} &= \dfrac{k_{z,2}}{\varepsilon_{r,2}} \\ k_{x,1} &= k_{x,2} = k_{sp} \end{cases} \tag{4.9}$$

Using $k_x^2 = |k_i|^2 - k_{z,i}^2$ with $|k_i|^2 = \varepsilon_{r,i} \dfrac{\omega^2}{c^2}$

$$\begin{cases} k_{sp} &= k'_{sp} + i k''_{sp} = \dfrac{\omega}{c} \sqrt{\dfrac{\varepsilon_{r,1} \varepsilon_{r,2}}{\varepsilon_{r,1} + \varepsilon_{r,2}}} \\ k_{z,1}^2 &= \dfrac{\varepsilon_{r,1}}{\varepsilon_{r,2}} k_{sp}^2 \end{cases} \tag{4.10}$$

The plasmons exist for non-vanishing k'_{sp} and are bound to the surface if $k'_{sp} > k_{vac}$ (non-radiative region). It is easy to show, following the same process, that no solution exists for TE-polarised waves. Due to either absorption or scattering, the propagation of these surface waves is usually strongly attenuated along the way, with a characteristic length of $L = 1/k''_{sp}$. Since the permittivity of metal is a complex quantity, the dispersion

relation $k'_{sp} = f(\omega)$ is often simplified by approximating ϵ with the Drude model in the literature. This estimation leads to the well-known blue curve depicted in Fig. 4.3b. Nevertheless, the existence of other resonances related to bound electrons and therefore not taken into account by the Drude model, considerably changes the dispersion relation at high frequencies. As can be seen from the red curve in the same figure, both models are reasonably equivalent in our region of interest, for visible and near-infrared light ($1.5 < \omega < 5\,\mathrm{PHz}$), although the calculated values of the permittivity differ significantly (see Fig. 4.3a). For 850 nm radiation we obtain $k_{sp,D} = 7.53 \cdot 10^6 + 5.22 \cdot 10^3\, i$, ($\lambda_{sp,D} = 2\pi/Re(k_{sp}) = 834.8\,\mathrm{nm}$) with the Drude model and $k_{sp,LD} = 7.55 \cdot 10^6 + 1.52 \cdot 10^4\, i$, ($\lambda_{sp,LD} = 832.2\,\mathrm{nm}$) with the Lorentz-Drude model. In order to excite SPPs, the phase

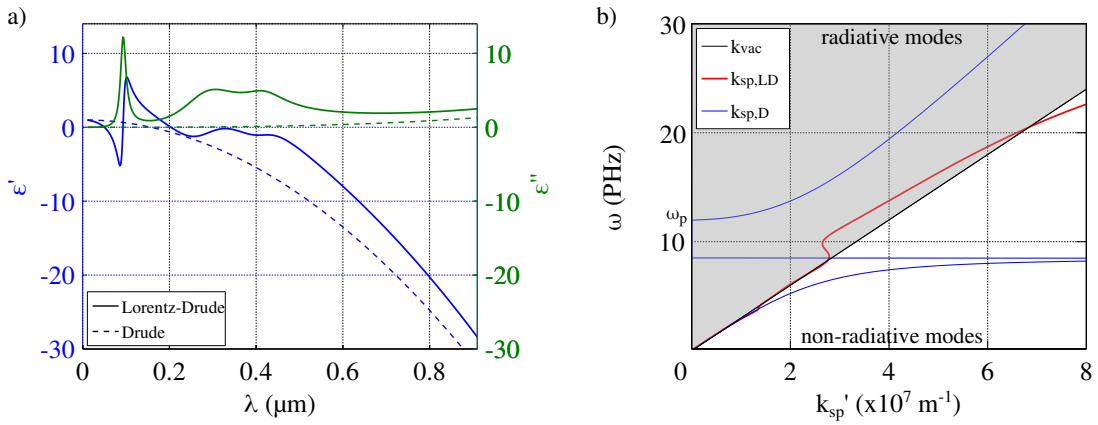


Figure 4.3.: Properties of surface plasmons propagating at a dielectric-metal interface. (a) Permittivity of gold calculated from experimental values obtained in [80] and using a Drude (D) and the Lorentz-Drude (LD) model. (b) Resulting plasmon dispersion relation computed with both models. Surface modes exist below the light cone.

matching condition has to be fulfilled for both z and x components. Because the wave vector of plasmons is always larger than in the dielectric ($k_{sp}/k_{vac} = 1.02$ at 850 nm), direct excitation is not possible. The momentum of the incident wave $k_{x,i}$ can be increased by passing through a high-index material such as a prism, and allows for evanescent coupling into the plasmonic modes. Such configurations are illustrated in Fig. 4.4.

We now consider a periodically corrugated air-metal interface with grating vector $k_g = \frac{\pi}{p}$, as depicted in Fig. 4.5a. A shallow grating supports plasmons with a wave vector k_{sp} equivalent to the flat surface case (see Eq. 4.10), as long as the phase matching condition is fulfilled

$$k_{sp} = \pm k_0 sin(\theta) \pm m k_g \tag{4.11}$$

It is easy to see that for $k_x \sim k_g/2$ a band gap opens up, as two plasmon configurations with different energies can arise. Barnes *et al.* [92] showed that for more complicated shapes such as rectangles comprising at least two harmonics, the dispersion relation acquires a band structure (see Fig. 4.5b). The presence of a higher band within the light cone enables SPP excitation from the air even at normal incidence ($k_x = 0$). At the band edge $k_x = k_g/2$, only stationary waves exist and high field enhancement occurs at the corner of each metallic stripe. The strong field can couple again to plasmons along the slit, allowing

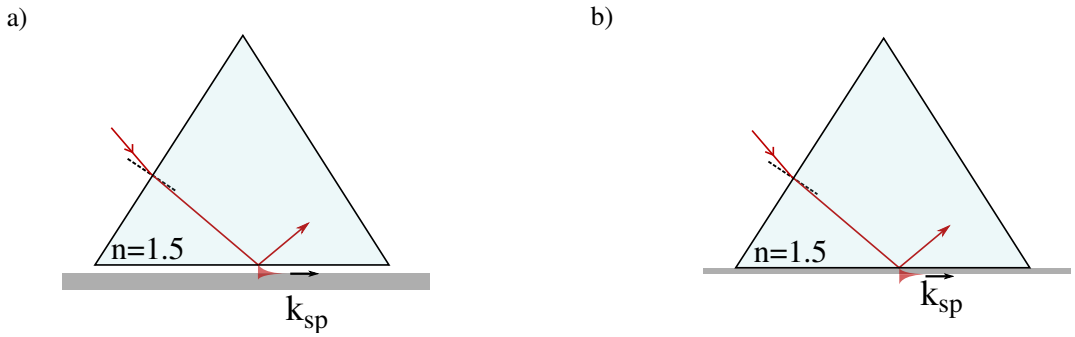


Figure 4.4.: Possible arrangements to achieve plasmon excitation in (a) thick metallic films (Otto configuration) or (b) thin films (Kretschmann configuration).

tunnelling to the other side. Identical conclusions were drawn from alternative approaches based on the study of the electron density at the surface of the grating [93]. Although the SPP model gives a good qualitative explanation of EOT, a quantitative model is obtained by also taking into account the propagation of quasi-cylindrical waves (QCW) [94, 95].

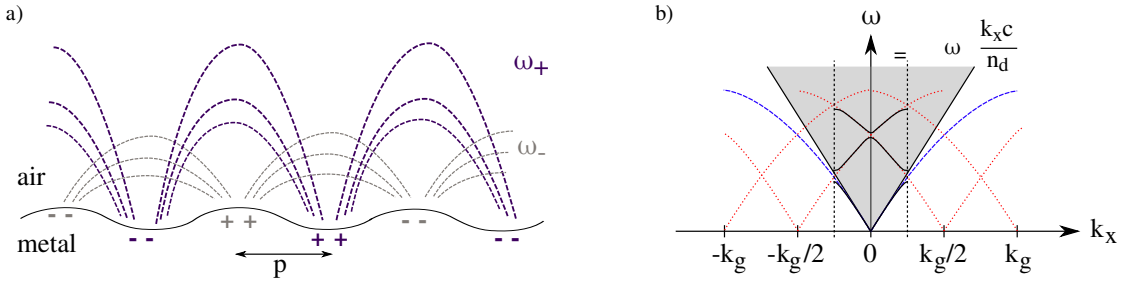


Figure 4.5.: Influence of the periodicity of the surface corrugation onto the surface plasmons. (a) Electric field lines at the edge of the first Brillouin zone for a shallow grating with a sinusoidal profile. A band gap opens up as two solutions arise for the plasmonic wave with $k = \pi/2p$. (b) Schematic band structure arising from the multiple periodicity of the surface corrugations. The blue line shows the dispersion relation at a flat interface for comparison.

4.2. Grating optimisation using Finite Difference Time Domain simulations

The performance of a WGP results from the complex interplay between different physical phenomena. Although the elements of the theory presented in Section 4.1 help understanding some of these effects qualitatively, there is no single analytical solution that would provide quantitative response parameters. In addition, particular effects of realistic components such as the finite size of the grating or the influence of a substrate are hard to take into account. Fortunately, the behaviour of the subwavelength structures can be numerically simulated using either Finite Difference in Time Domain (FDTD), Finite Element Method (FEM) or Rigorous Coupled Wave Analysis (RCWA). This work relies

on FDTD simulations performed with the open-source software MEEP [96] developed at MIT.

FDTD is a powerful time-domain method based on discretisation of both space and time in steps Δx and Δt, respectively, as proposed by Yee. In order to simulate the behaviour of subwavelength gratings, a large computational cell is required to consider coherent effects between periodic elements, albeit with a high resolution to study the field propagation through the narrow slits. We reduce the required computational power by considering a 2D system, where the length of the metal stripes is infinite. The simulation cell has a size of $12 \times 8\,\mu m^2$ with a resolution of 7 nm, and is delimited by Perfectly Matched Layers (PML) to simulate open boundaries. The grating is excited by a single pulse emitting a plane wave with a central wavelength of $\lambda = 850\,nm$. The spectral bandwidth is maintained relatively low ($\Delta\lambda = 10\,nm$) for accurate field distribution analysis, nevertheless it still leads to large pulse lengths in the temporal domain and therefore to long simulation times. In the cases where only the transmission and reflection of the polariser are of interest, a broadband source can be used, as these parameters are computed via Fourier transform of the energy flux above and below the structure.

The resolution and size of the cell are chosen in order to achieve satisfactory simulation times while ensuring numerical stability of the program. The FDTD algorithm converges only if the spatial steps are smaller than the propagation length of the wave within one time increment, *i.e.*, for $c\Delta t > \Delta x$. In practice, the Courant factor defined as $S = \frac{c\Delta t}{\Delta x}$, should be much smaller than $\frac{n_{min}}{D} = \frac{0.23}{2} = 0.115$ for gold at 850 nm, where D represents the dimensionality of the simulated system. Due to the low refractive index associated with the resonant response of the polariser for TM-polarisation, the time increment has to be small. This intrinsic property leads to long computational times, which have been scaled down by taking advantage of the Leibniz Supercomputing center based in Garching, Germany.

Previous studies [51] indicate typical grating parameters, and a period of $p = 500\,nm$ seems to deliver good performances around $\lambda = 850\,nm$. The optimisation of the slit width as well as the gold thickness was thus precisely studied and is presented in Fig. 4.6. Figure 4.6a shows that the transmission of the TE polarisation is exponentially damped with increasing film thickness, as expected from the waveguide analogy presented in Section 4.1.1. This behaviour mainly governs the evolution of the extinction ratio, as the transmission of the TM mode remains almost constant. The latter tends to decrease with h due to the interaction with the surrounding metal, although small maxima related to Fabry-Pérot cavity effects within the slit are visible. The best compromise between high extinction ratio and transmission of the TM-polarisation is obtained for $h = 270\,nm$, as the manufacturing of narrow slits with large metal thickness is usually challenging. Figure 4.6d shows the impact of the slit width onto the ER around the chosen metal height. Here we aim for an ER of 1:1,000, yielding a QBER of 0.1 %, which would be sufficient for our QKD application (the transmission T_{TM} is not critical, as the bright laser pulses have to be strongly attenuated at some point). This condition is fulfilled for $w \leq 120\,nm$. The ER tends to increase with decreasing w, although a resonance is also observed for the TM-waves at $w = 90\,nm$.

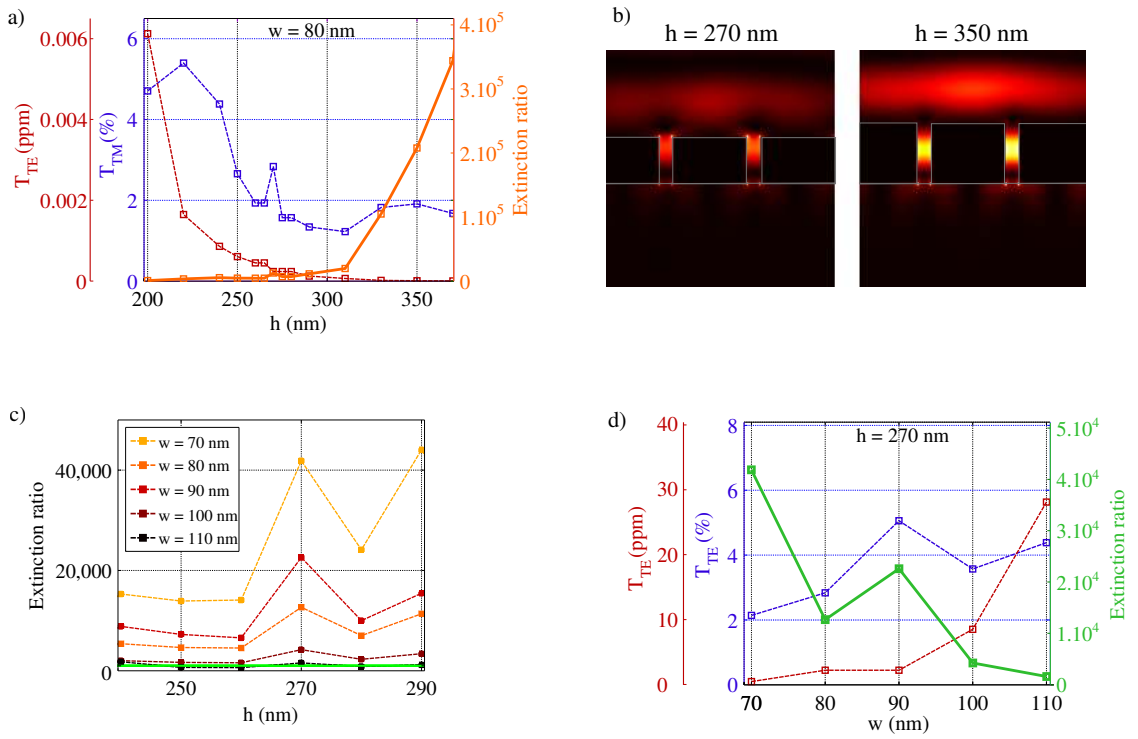


Figure 4.6.: Influence of the design parameters on the performances of the polariser for a fixed period of $p = 500\,\text{nm}$. (a) Dependency of the transmission of TE and TM waves with the metal thickness h for a fixed width of $w = 80\,\text{nm}$. (b) Field distribution of the TE-modes for resonance heights $h = 270\,\text{nm}$ and $h = 350\,\text{nm}$ obtained at the same simulation time. (c) Evolution of the extinction ratio around the vertical resonance occurring at $h = 270\,\text{nm}$. The green line represents our design rule of $ER = 1000$. (d) Transmission of both polarisations as a function of the slit width at $h = 270\,\text{nm}$.

4.3. Experimental results

4.3.1. Wire-grid polariser fabrication

According to the simulations, a sufficient extinction ratio above 1:1,000 should be obtained for $h = 270\,\text{nm}$, $p = 500\,\text{nm}$ and $w \leq 120\,\text{nm}$. Due to the availability of an Electron Beam Lithography (EBL) workstation in the clean room of the university, the first samples were prepared with this method. As the obtained results were not satisfying, we moved on to Focused Ion Beam (FIB) milling.

Electron beam lithography

The goal of Electron Beam Lithography (EBL) is to create a polymer (resist) mask for the deposition or etching of a thin layer. The electron-sensitive resist is irradiated according to a predefined pattern, locally changing its chemical properties. The modified (intact)

region becomes solvable in a developer for a positive (negative) resist.

Here the mask has to be fabricated before the evaporation of the gold layer. Compared to standard nanostructures, both the thickness and the aspect ratio of the trenches ($\gtrsim 1:3$) are relatively high. This sets constraints onto the choice of the photoresist, which should offer good lateral resolution while featuring a large thickness $t \geq 2h$ to allow for successful lift-off. The first negative photoresist (AZnLof 2000), with $t = 0.5\,\mu m$ exhibited inadequate lateral resolution, and was later on replaced by a combination of two thinner PMMA layers with different molecular weights (500k and 950k), and thicknesses of 160 nm and 190 nm, respectively. As the PMMA 500k is more sensitive to electrons, the developed photoresist slabs will exhibit an undercut (see Fig. 4.7). This configuration prevents continuous coating of the flanks during the metal evaporation step, and therefore allows for a successful removal of the resist in the final lift-off step.

The fabrication protocol starts with the cleaning of the glass substrate, a $18 \times 18 \times 0.17$ mm microscope cover plate. The sample is first immersed in an acetone solution and sonicated for 10 minutes, then cleaned by oxygen plasma etching for 3 minutes. A 3 nm thick Chromium discharge layer is deposited onto the sample by thermal evaporation. This conductive film will later allow for the evacuation of the charges implanted in the isolating photoresist during the electron beam lithography process. An adhesion promoter (HDMS:IPA) is spin-coated for 3 seconds at 800 rpm and for 30 seconds at 4000 rpm. The sample is then baked on a hot plate at 115^o for 90 seconds. Finally, two identical steps of spin coating and soft-bake at 180^o for 120 seconds are performed first with PMMA 500k and then with PMMA 950k.

The resist is patterned by electron-beam lithography using an acceleration voltage of 10 kV, an aperture of 20 µm and a dose of $95\,\mu C/cm^2$. The samples are then developed in an IPA:MIBK solution for slightly more than 30 seconds and rinsed with isopropanol for 10 seconds. This duration was found to be the best compromise between partial development and excessive undercuts causing the narrow photoresist slabs to fall aside.

A 3 nm thick titanium adhesion layer is coated via electron beam Physical Vapour Deposition (PVD), followed by 265 nm of gold. Deposition rates are kept below $1.5\,\mathring{A}/s$ in order to minimise the roughness of the resulting film. Due to the long coating time, the temperature of the substrate causes the PMMA structure to creep and crack. Several breaks of one minute every four minutes have been introduced to attenuate this effect.

The last step consists in removing the photoresist below the metal. The samples are immersed in Dimethyl Sulfoxide (DMSO) at 85^o for several hours. To help with the lifting of the resist, air can be gently blown with a pipette onto the surface. Ultrasound baths should be avoided even at low power, as they usually also separate the gold layer from the substrate. Finally, the samples are flushed with isopropanol and dried with nitrogen.

Several issues were encountered during the fabrication process. The total thickness of the PMMA layer ensures successful lift-off for small metal heights only, as shown in Fig. 4.8a. At $h = 250$ nm, the smallest achievable slit width is $w = 200$ nm, while narrower structures lead to a continuous metal layer completely covering the photoresist (see Fig. 4.8b, inset). Moreover, small slits are difficult to obtain due to the proximity effect that widens the structure. The periodicity of the grating causes the theoretically unexposed photoresist regions to collect a certain number of electrons scattered during the writing of both neighbouring areas. Indeed, the injected electrons experience forward scattering due to electron-electron interactions in the resist and back-scattering from the substrate. The accumulated dose leads to a partial dissolution of the narrow photoresist structures during the development and to mechanical instability during the metal deposition process.

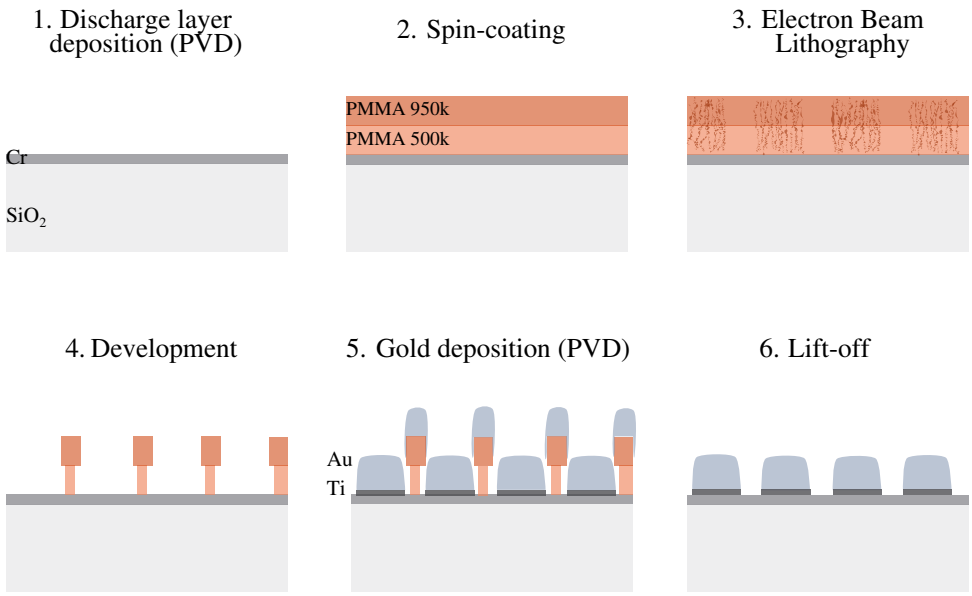


Figure 4.7.: Fabrication procedure of wire-grid polariser based on electron beam lithography with a positive photoresist.

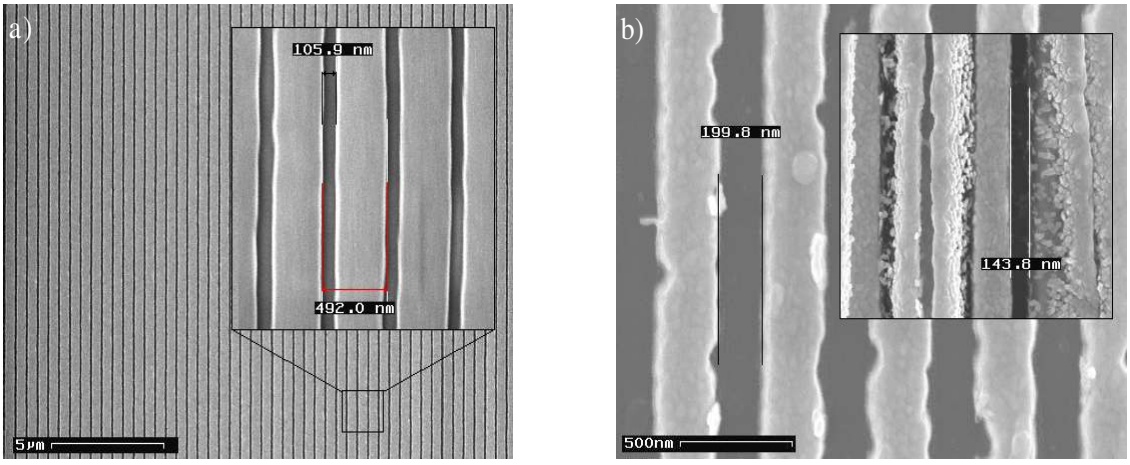


Figure 4.8.: Scanning Electron Microscope pictures of the gratings manufactured by Electron Beam Lithography. The images show the smallest slit width achieved for gold thicknesses of (a) $h = 50\,\mathrm{nm}$ and (b) $h = 250\,\mathrm{nm}$.

Focused Ion Beam milling

The suitability of the Focused Ion Beam (FIB) milling to fabricate high-performance wire-grid polariser was investigated. Here a tightly focused and highly accelerated Gallium Arsenide (GaAs) ion beam allows for precise material removal from the surface of the sample, and can be used to etch narrow slits in the gold layer. The geometry of the ablated region is directly defined by the path of the beam, removing the need for hard masks and photoresists. As ions are heavier than electrons, the writing beam has a smaller focus of a few nanometres, depending on the settings. The focusing of the beam either for milling or for imaging should be done properly and close to the area of interest to obtain an optimal result. Unfortunately, this procedure is critical as it simultaneously leads to irreversible damages.

The samples presented in the following have been fabricated with a workstation combining both an SEM and a FIB column forming an angle of 54^o (*CrossBeam Series*, Zeiss). The apparatus is located at the Center for Nanotechnology and Nanomaterials (ZNN) in Garching, Germany. The FIB can operate in two different modes, the first one being similar to that of an SEM, where one specifies the dose (charge per area) and the dwell time (time spent on one pixel) of the beam. This approach allows the definition of complex geometries using a dedicated lithography software (Raith), but authorises only a single pass of the ion beam. For deep penetration of the beam, the ablated material cannot be sputtered away and is redeposited on the flanks of the trench, which yields V-shaped slits. The profile of the resulting structure can be easily visualised by cutting off a small volume of material, as shown in Fig. 5.2. In the second mode, the beam scans the desired region several times and enables the fabrication of slightly wider trenches but with steeper flanks. Unfortunately, this configuration cannot be considered in the following, as it can be used only to carve single objects and is incompatible with the CAD software required to design a periodical structure. The optimal parameters for the milling were found to be a working distance of 4.9 mm, an acceleration voltage of 30 keV, an aperture of 30 µm and a dose of 82,500 µC/cm^2. These conditions lead to a writing time of about 1,5 hours for a field of $120 \times 120\,\mu m^2$.

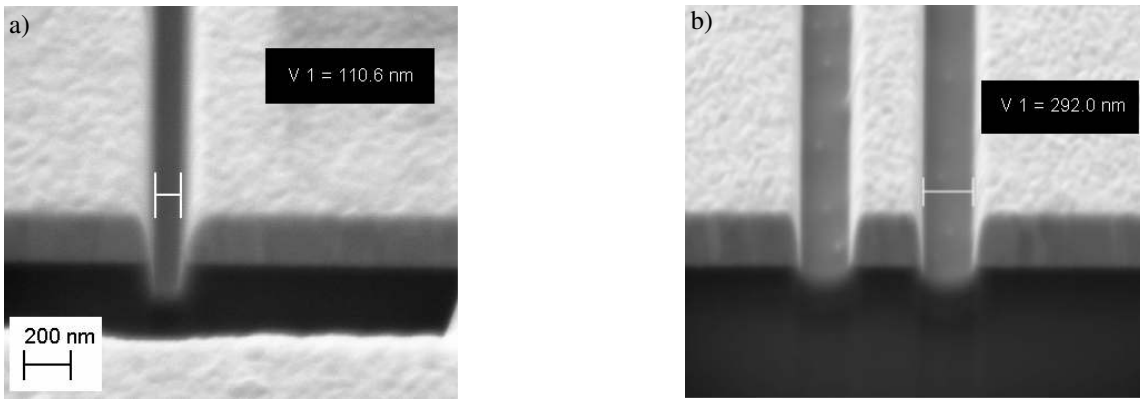


Figure 4.9.: Influence of the operation mode of the FIB onto the shape of the grooves. (a) Single-pass and (b) Multi-pass configuration.

4.3.2. Optical characterisation

The glass substrate was mounted onto a (x,y)-translation stage in order to test different polarisers fabricated in a single run. A polarised laser beam was focused onto the sample, therefore acting as an analyser, using an aspheric lens ($f = 11\,\mathrm{mm}$) and collected using a microscope objective ($NA = 0.6$). The gold surface was imaged using a 12-bit CCD camera equipped with an objective, and the pinpointing of the polarisers was eased by the presence of surrounding position markers etched in the metallic layer. The transmission was measured for well-defined input polarisations using a power-meter, featuring a higher dynamic range than the camera. As the gold gratings exhibit high reflectivity, the backwards propagating light was partially mirrored by the focusing lens and transmitted either through the marks or through the other polarisers, leading to a poor extinction ratio. A spatial filter was therefore implemented on the collection side using two additional lenses and an iris with a diameter of 150 µm.

The samples fabricated by EBL delivered poor extinction ratios, in the best case about 1:80. The performance was limited by a maximum metal thickness ($h = 250\,\mathrm{nm}$) and slit width ($w = 200\,\mathrm{nm}$) allowing for a successful lift-off. The first samples manufactured by FIB milling already showed some improvement, with extinction ratios exceeding 1:150 even for $h = 250\,\mathrm{nm}$. Narrower trenches were gradually obtained by optimising the dose such that the ion beam removes the gold close to the glass interface without penetrating the isolating substrate, thereby avoiding lateral deflection due to accumulated charges. The metal height could also be increased, and better performances were experimentally obtained with $h = 265\,\mathrm{nm}$. The deviation from the optimal thickness of 270 nm can be explained by the lack of spatial resolution in the original simulation but also to the presence of a Titanium adhesion layer of 3 nm, not taken into account in the simple geometrical model. As confirmed later by high-resolution simulations with $\Delta x = 1\,\mathrm{nm}$, the titanium contributes to the total height of the structure, as its thickness is smaller than the penetration depth of the plasmons. Another possible source of error is an uncertainty in the thickness of the gold film, measured by a piezoelectric sensor during the evaporation process.

According to the simulations, an extinction ratio above 2,000 should be obtained for slit widths below 120 nm. The samples A presented in Table 4.1 were fabricated with this largest possible width and exhibited ERs up to 1:650. In order to achieve the desired performances of 1:1,000, new samples B with smaller slit widths down to 80 nm were manufactured. A small improvement to 1:850 was measured, although an tenfold increase was expected according to the simulations. Such discrepancies between experimental and theoretical performances have been often reported in the literature [97–99]. Additionally, the measured ER shows a large scatter for different samples although the gratings exhibit a similar geometry and roughness in top view SEM pictures (see Fig. 4.10a).

Further information about the gratings is obtained by looking at the cross-section of the metallic stripes (see Fig. 4.10b). As already observed in Fig. 5.2, the slits can exhibit a V-shape due to side-redeposition of the ablated material. For sake of completeness, we mention that relatively straight flanks were achieved only once, and are shown in Fig. 4.10c

4.4. Refinement of the simulation model

As the experimental metal stripes exhibit a rather trapezoidal shape, we introduce a refined model to account for the observed geometry. The parameter w now denotes the

Sample	w (nm)	ER (experimental)	ER (simulated)
A_1	120	380	2520
A_2	120	650	
B_1	80	720	12700
B_2	80	850	

Table 4.1.: Comparison between simulated and experimental extinction ratios for different slit widths. Here the structure is simulated with a period $p = 500\,\text{nm}$ and a gold thickness of $h = 270\,\text{nm}$, but fabricated with $h = 265\,\text{nm}$ with additional 3 nm Ti.

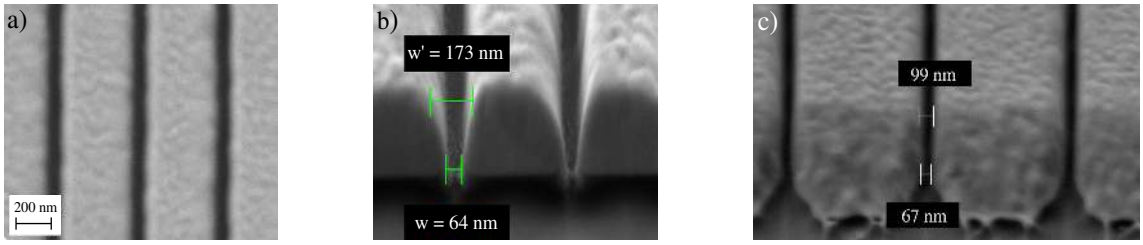


Figure 4.10.: SEM pictures of the polarisers manufactured by FIB milling. (a,b) Typical top and side-view images of the gold stripes, respectively. (c) Exceptional sample exhibiting gold stripes with more rectangular cross-section.

slit width at the bottom of the stripes, close to the substrate, and the angle α corresponds to the deviation from a perfect rectangular structure, as illustrated in Fig. 4.11.

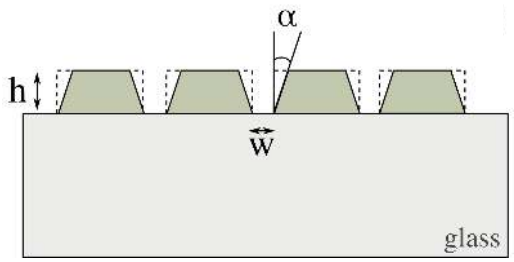


Figure 4.11.: Refined model for the FDTD simulations based on the experimental observation of stripes with trapezoidal cross-section.

The transmission of both *TE* and *TM* modes, as well as the ER are computed varying again the slit width w and additionally the opening angle α. The effect of the opening angle is highlighted by normalising the transmission by the value obtained for $\alpha = 0$. Fig. 4.12a shows an exponential decrease of ER when varying the angle α, caused particularly by the exponential increase of the *TE*-polarisation (see Fig. 4.12c). T_{TM} seems to be rather insensitive to the trapezoidal shape, although larger widths yield a slight increase, as for rectangular shapes. When using the trapezoidal shape in the simulations, the theoretical ER values for $w = 80\,\text{nm}$ are reduced from 12,700 (rectangular stripes) down to 500 for B_1 ($\alpha_{exp} = 25^{\,o}$) and 2,700 for B_2 ($\alpha_{exp} = 16^{\,o}$). This trapezoidal shape indeed explains

the order of magnitude discrepancy observed between simulations of perfectly rectangular stripes and realistic samples.

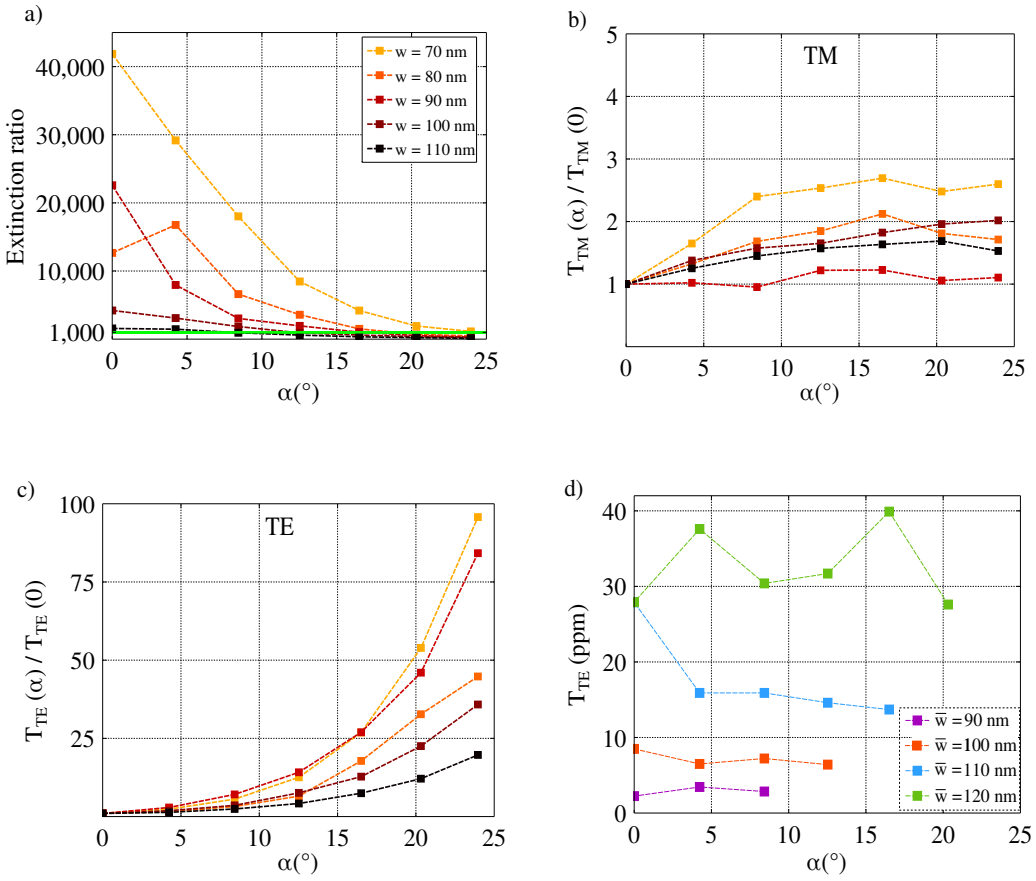


Figure 4.12.: Dependence of the performance on the slit angle α ($h = 270\,\text{nm}$): (a) extinction ratio, (b),(c) transmission of *TM* and *TE* polarisation modes, respectively. The exponential increase of the transmission of *TE*-modes is mainly responsible for the significant reduction of the extinction ratio. (d) Transmission of the *TE* polarisation as a function of the effective slit width $\bar{w}$.

Figure 4.12d shows that the transmission of the *TE*-polarisation, and therefore the ER, is only sensitive to the average slit width $\bar{w} = (w_{max} - w_{min})/2$. This means that the field experiences an average attenuation due to the equally distributed contribution of the different widths existing in the slit. As presented in Section 4.1, a rectangular slit with a width w narrower than the cut-off width w_c can be seen as a metallic waveguide, in which the wave is exponentially damped. After a height h, the intensity has dropped by a factor $e^{-|\beta|h}$ with $\beta \in \mathbb{C}$. The constant β is extracted from the field amplitude decay within the slit (see Fig. 4.13a), and plotted against w in Fig. 4.13b. In the considered range of w, between 70 nm and 180 nm, the imaginary part of the propagation constant exhibits a reasonably linear dependency. As the width varies linearly across the thickness, the attenuation evolves also linearly, allowing to average both values over the metal height.

Using these findings for the next optimisation step, we note that the targeted extinction ratio of 1,000 can be achieved for rectangular stripes with $w \leq 110\,\text{nm}$, but not for

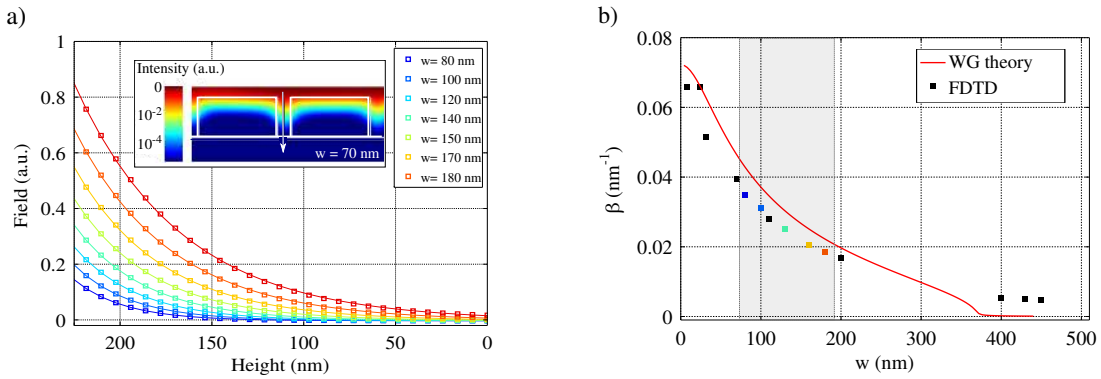


Figure 4.13.: Intensity decay within rectangular slits. (a) Simulated field intensity profile within the slit as a function of the slit width. (b) Damping constant γ extracted from the intensity profile assuming $I(z) \propto e^{-i\beta z}$ for different slit widths. The red line corresponds to the theory of metallic waveguides detailed in Section 4.1.1. The grey area indicates the range where β shows an approximately linear dependency on w.

achievable angles $\alpha \geq 18^o$. Yet reducing the slit width down to 70 nm (corresponding to $\bar{w} = 110$ nm) brings a clear improvement. This simulation was verified experimentally by the fabrication of a new polariser array, presented in Fig. 4.14. Table 4.2 presents the characterisation of these four samples and compares them to the theoretical performances simulated with the refined model. As expected, the ER exceeds 1,000 and even reaches 1,800, yielding the best published ER values observed so far for 850 nm. The transmission is similar for all samples and reaches 9 %.

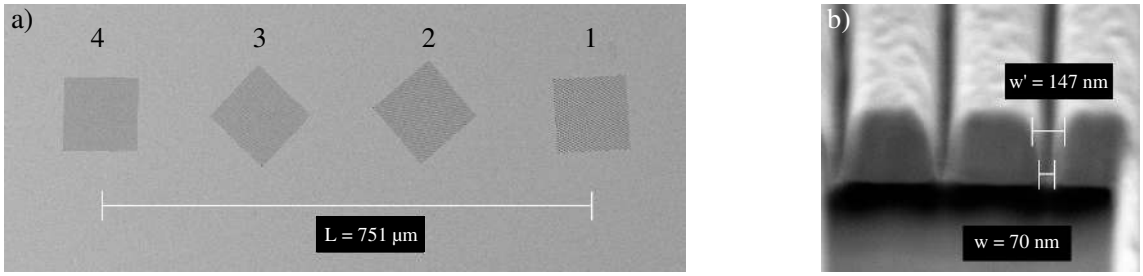


Figure 4.14.: SEM pictures of a four-polariser array exhibiting extinction ratios up to 1,800. (a) Top view of the matrix. (b) Cross-section of the fourth grating. The decrease in performances associated with a large tilting angle $\alpha > 16^o$ are compensated by reducing the slit width.

As will be presented in Section 5.3.3, the prepared states that will be injected into the waveguide chip have to be slightly modified in order to compensate for small polarisation effects within the chip. The optimal orientation of polarisers was calculated to optimise the quality of the states at the output of the Alice module (see Table 4.3). As the FIB can only write along two directions, the whole stage has to be rotated in small steps in order to write all the samples along the same axis. The limited accuracy of the reference frame

Sample	w (nm)	w_{max} (nm)	α (^{o})	ER (experimental)	ER (simulated)
1	70	150	16	1800	4200
2	70	160	19	1620	2870
3	80	160	16	1200	1510
4	70	175	21	1150	1544

Table 4.2.: Experimental results obtained after optimisation of the geometry using a trapezoidal model. The data exhibit clearly improved agreement with the simulations.

and rotation axis definition as well as the mechanical resolution of the stage lead to an estimated overall resolution of about 2^o. The imperfections of the prepared polarisations result from missing steps in the rotation of the reference frame.

Input port	4 (V')	3 (-45')	2 ($+45$')	1 (H')
Optimal input states (simulated)	86.8^o	39.9^o	-43.9^o	-1.0^o
Optimal input states (prepared)	89^o	44.6^o	-50.1^o	-1.0^o

Table 4.3.: State preparation of the polariser array. The linear input states should be slightly rotated to pre-compensated polarisation-dependent effects in the waveguide chip (see Section 5.3.3).

5. Ensuring the spatial overlap of the qubits with photonic integrated circuits

One fundamental requirement on the quantum states of light imposed by the quantum key distribution protocol is their spatial indistinguishability. In our scheme, the polarisation states are generated by different laser diodes, and therefore into different spatial modes. This chapter focuses on the development and characterisation of a waveguide chip combining the four beams into one guided mode. The device is designed and manufactured via femtosecond laser micromachining in Dr. Osellame's group at the Politecnico di Milano (Italy). The basic properties of straight waveguides and directional couplers was first evaluated before expanding the layout into a four mode mixer. A 3D architecture was adopted to guarantee vanishing polarisation dependent effects, thereby fully exploiting the unique capabilities of this fabrication technique. A tomographic measurement allowed to retrieve the polarisation behaviour of each waveguide, and to optimise the input states in order to pre-compensate for the remaining imperfections and to obtain a set of output states producing an average QBER below 0.1 %. Unfortunately, a large discrepancy between the calculated and the experimental states measured at the output of the assembled Alice module was observed (see Section 6.3.2). A deeper study revealed suspicious tomographic data as well as several errors in the first version of the analysis program, both provided by an external source. The corresponding results are therefore presented for sake of coherence only.

5.1. Femtosecond laser micromachining

Most waveguiding systems are based on Total Internal Reflection (TIR) of the light at the interface of a high-index (core) with a low-index material (cladding). Such arrangements include optical glass fibres and planar dielectric waveguides. As discussed in 2.4, fibres are very sensitive to both temperature and mechanical stress, resulting in an unstable birefringence strength and optical axis orientation. Monolithically integrated structures are much more compact and stable, but usually sustain TE and TM modes with different mode sizes. The polarisation qubits are therefore spatially distinguishable and not suitable for QKD schemes or for most quantum optics experiments.

This problem is solved in femtosecond laser written waveguides, as they support both TE and TM modes, which both exhibit a Gaussian mode profile with excellent overlap. This relatively new technique developed in the 1990's by Hirao and coworkers [55] consists in increasing locally and permanently the refractive index of a transparent material using a tightly focused ultrafast laser beam moving along a desired path. The high optical density in the beam focus, on the order of a few TW/cm^2, can lead to nonlinear absorption, avalanche photoionisation, and possible void formation. The laser parameters such as wavelength, polarisation, pulse duration, repetition rate and scan speed, as well as the focussing optics, have to be optimised for each substrate material to engineer the resulting refractive index profiles. The formation of the microstructure and their usage in photonics

are widely discussed in the literature [56, 100]. Further processing of the irradiated regions extends the range of applications to microfluidic devices [101] or invisibility cloaks [102].

Femtosecond laser micromachining has further practical advantages over planar lithography. Indeed, the fabrication does not require a clean room environment, and removes the need for a hard mask created for each design, the layout being directly determined by the programmed path of the laser only. The layout of the photonic devices can easily be extended to three dimensions, thereby opening new possibilities towards complex all-optical networks. Moreover, this single-step prototyping method is really fast and can reach 30 cm/s writing speed [103]. The slight downside of this type of waveguide compared to conventional Photonic Integrated Circuits (PIC) is the relatively high propagation loss of about $\sim 0.5\,\mathrm{dB/cm}$. This is one order of magnitude higher than for other PICs, and five orders of magnitude higher than for standard glass fibres. Accordingly, the bending losses associated to curved waveguides are higher in femtosecond laser written waveguides, and bending radii are much larger than in their lithographically fabricated counterparts to achieve reasonable losses.

Several important parameters have to be optimised to obtain good waveguide quality. First, the birefringence should be as low as possible to avoid possible depolarisation of the qubits and spatial distinguishability of the states. Indeed, the resulting waveguide cross-section is usually elliptical, due to the geometry of the Gaussian laser beam, with a length along the propagation axis of $b = 2\pi w_0/\lambda$ (confocal parameter) and a width of $2\,w_0$, where w_0 corresponds to the beam waist. This so-called *form birefringence* can be corrected by spatial and temporal beam-shaping techniques [104, 105], enabling better coupling to fibres and free-space Gaussian beams. Another problem arises from the difference in optical density along the longitudinal and transverse direction of the femtosecond laser beam, which leads to stress birefringence and therefore to different refractive indices for TE and TM polarised waves. For a top irradiation, both aforementioned anisotropies pin the optical axes of the waveguide to the laser axis and its transverse direction, i.e. to the horizontal and vertical axes. The axis can nevertheless be rotated either by tilting the incoming beam [106] or by adding additional stress fields around the waveguide [107]. The latter can also be useful to increase the birefringence strength and therefore tune the phase matching condition in non-linear applications [108].

5.2. Characterisation of planar waveguide architectures

The samples characterised in this chapter are fabricated in Dr. Osellame's group in Milan, Italy. Here a train of ultrashort ($\approx 400\,\mathrm{fs}$) laser pulses at $\lambda = 1040\,\mathrm{nm}$, produced by a regeneratively amplified Yb-based laser (High-Qlaser FEMTORegen), at the repetition rate of 960 kHz and with an energy of 280 nJ/pulse was focused into an alumino-borosilicate glass substrate (*EAGLE2000*®, Corning Inc.) by means of a microscope objective ($NA = 0.6$, $50\times$ magnification). Single mode optical waveguides for light at 850 nm, with relatively small propagation loss ($\approx 0.5\,\mathrm{dB/cm}$) could be fabricated by translating the substrate at the constant speed of 43 mm/s.

The refractive index contrast between the core and the bulk being small ($\sim 10^{-3}$), the waveguides are not visible to the naked eye. Surface ablation lines placed at regular intervals above defined waveguides allow to locate the different structures. The first test waveguides, thereafter referred to as *I*, are buried 500 µm under the surface of the 1.1 mm

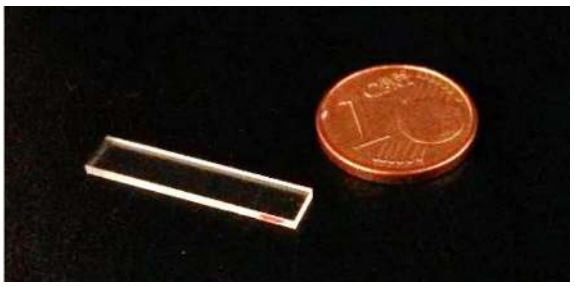


Figure 5.1.: Picture of a femtosecond laser micromachined glass chip containing straight waveguides and directional couplers.

thick glass plate for easier localisation. Their successors (*II*) are written at an optimal depth of 170 µm, determined by the aberration compensation of the objectives used to focus the femtosecond laser beam into the substrate. As will be presented in the next section, better quality in terms of losses and polarisation dependent effects is achieved under these conditions. Most of the experimental results presented in the following are therefore related to these samples.

5.2.1. Straight waveguides

The role of the waveguides is to combine the different polarisation qubits into one spatial mode. It is therefore of major importance to investigate the mode overlap between different states, and to determine the mode size to evaluate the coupling efficiency with the VCSELs in the final module. Both parameters are measured using the near-field imaging set-up shown in Figure 5.2a. The elliptical beam emitted by an edge-emitting laser diode at $\lambda = 851\,\text{nm}$ is first spatially filtered by a single-mode fibre. In order to rotate the polarisation without changing the intensity, an arbitrary linear polarisation is fixed by a polariser, and can be rotated by a half-wave plate. The beam is focused onto the waveguide entrance facet using an aspheric lens ($f_1 = 11\,\text{mm}$) mounted onto a z-translation stage, while the waveguide is clamped onto an arm on top of a 3-axis-stage to facilitate the alignment. In the absence of collimating optics, interference patterns appear between the light partially coupled into the waveguide and the light passing through the glass and can be visualised in the far field regime with a camera. Lateral misalignment leads to interference cones which transform into rings (Fig. 5.2b) when the waveguide is perfectly aligned. Fast coupling into the waveguide can therefore be achieved by analysing the change in orientation of the cones with the waveguide position. Collimation optics including a microscope objective (NA= 0.4) and a lens ($f_2 = 200\,\text{mm}$) and yielding a magnification $M = 22.2$ is used to image the output facet onto a CCD camera with a pixel size of 2.2 µm.

Due to the finite numerical aperture of the objective, the measured mode profile w_m is a convolution of the real mode size w_r and the Airy radius $R \simeq 0.61\frac{\lambda}{NA}$ such that ${w_m}^2 = \sqrt{{w_r}^2 + R^2}$. The real mode size for the samples *II* was evaluated for H and V polarisation:

$$w_{H,x} = 3.38 \pm 0.05\,\mu m \qquad w_{V,x} = 3.34 \pm 0.05\,\mu m \tag{5.1}$$

$$w_{H,y} = 3.74 \pm 0.05 \mu m \qquad w_{V,y} = 3.79 \pm 0.05 \mu m \tag{5.2}$$

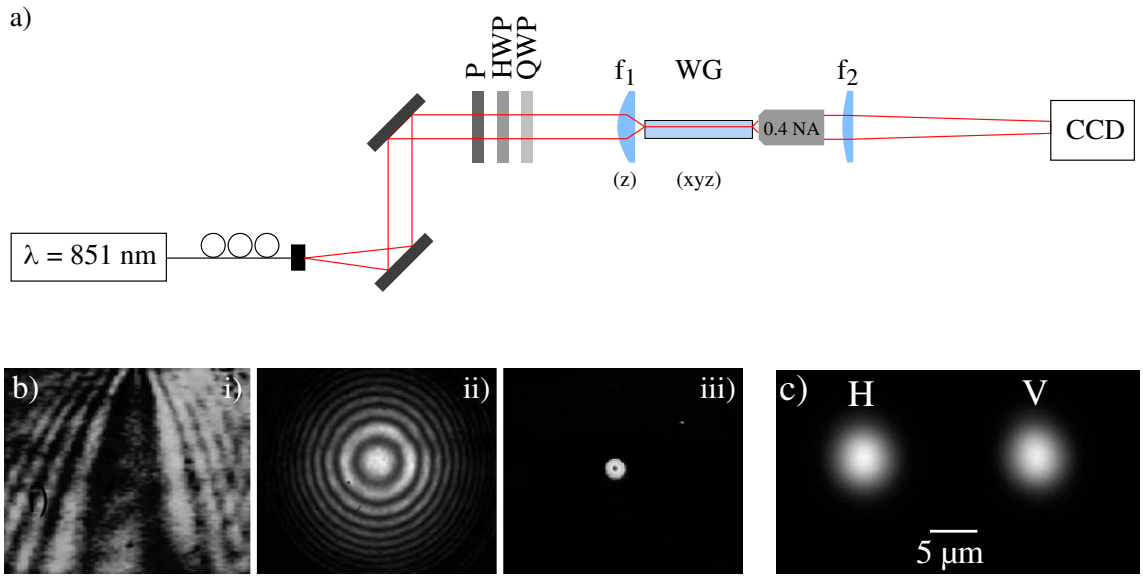


Figure 5.2.: Characterisation of the waveguide modes. (a) Optical setup. P: polariser, HWP: half-wave plate, QWP: quarter-wave plate, WG: waveguide, $f_1 = 11\,\text{mm}$, $f_2 = 200\,\text{mm}$ (b) Coupling procedure without collection optics: (i) the orientation of the cones resulting from the interference between the guided light and the uncoupled light travelling through the glass indicates the direction of the lateral misalignment of the waveguide. (ii) A ring pattern confirms efficient coupling into the waveguide. (iii) Image of the output facet using a microscope objective. (c) Near-field images of output modes for H and V input polarisations.

corresponding to divergence angles of $\theta_{1/e^2,x} = 4.6^o$ and $\theta_{1/e^2,V} = 4.1^o$, respectively. The modes are perfectly overlapping within the measurement errors and therefore suitable for our QKD application.

In a second step, we investigate the birefringence of these straight waveguides. Fast and slow axes are fixed by the manufacturing process and coincide with the vertical and horizontal directions, respectively. A 45^o input state will be decomposed into two orthogonal components travelling with different phase velocities. After a distance L, they are phase shifted by an amount $\Delta\phi$ defined as

$$\Delta\phi = \Delta n\, k_0\, L \tag{5.3}$$

where k_0 denotes the free-space propagation constant and $\Delta n = |n_H - n_V|$ the waveguide birefringence. The phase shift $\Theta_i = \Delta\phi_i\,[2m_i\pi]$ obtained after different propagation lengths ($L_1 = 6.7mm$, $L_2 = 12.5mm$ and $L_1 = 19.3mm$) are measured with a polarimeter (*TXP Series*, Thorlabs). Using a least square fit (see Fig. 5.3) the birefringence was evaluated to $\Delta n_I = \Delta n_{II} = (6.9 \pm 0.2) \cdot 10^{-5}$, consistent with the values supplied by the manufacturing group.

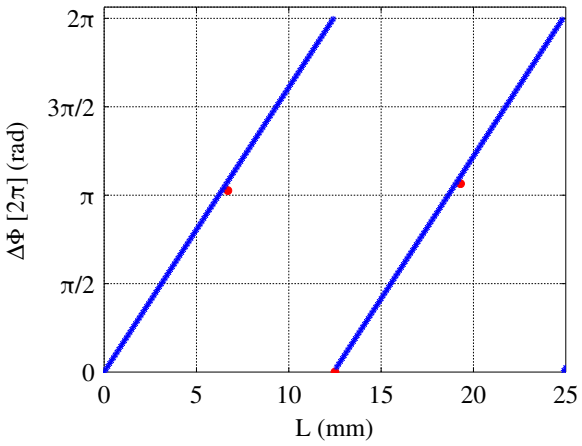


Figure 5.3.: Phase shift acquired by a 45^o input state after propagation through waveguides of different lengths (red dots). The birefringence can be retrieved by a least-square fitting through the experimental points.

5.2.2. Directional couplers

In bulk optics, two beams can be overlapped into one spatial mode using a beamsplitter. In integrated optics, this task is fulfilled by a directional coupler, which architecture is depicted in Fig. 6.1. Provided that both waveguides are separated by a small distance D within an interaction region of length L, the field of one guided beam can be adiabatically transferred to another via evanescent coupling, thereby allowing to overlap two beams launched in different waveguides into one output port. The splitting ratio depends directly on D and L, and the total length of the device is determined by the spatial separation of the ports and the achievable radii of curvature R.

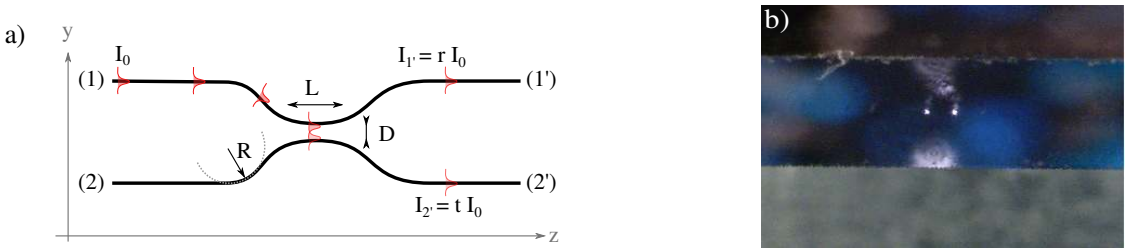


Figure 5.4.: (a) Geometry of a directional coupler. The relevant parameters are the interaction length L, the bending radius R, the distance between the waveguides in the coupling region D and the separation of two input ports. (b) Imaging of the output facet of a directional coupler I buried 500 µm under the surface.

In the weak coupling regime, the evolution of the field in each waveguide can be well approximated by the coupled-mode theory [109]. The main assumption stipulates that the intensities of the propagating modes are modified by the presence of a neighbouring

field. If the amplitude of each mode is defined as

$$A_i = A_i(z)\, e^{-j\,\beta_i\, z} \tag{5.4}$$

where β_i denotes the propagation constant, the transfer in the interaction region $z \in [0, L]$ is governed by the following equations

$$\begin{cases} \dfrac{dA_1}{dz} = -j\, C_{21}\, A_2(z)\, e^{j\,\Delta\beta\, z} \\ \dfrac{dA_2}{dz} = -j\, C_{12}\, A_1(z)\, e^{j\,\Delta\beta\, z} \end{cases} \tag{5.5}$$

where $\Delta\beta = \beta_1 - \beta_2$ is the phase mismatch and C_{ij} the coupling strength such that

$$C_{ij} = \frac{1}{2}\left(n^2_{core,i} - n^2_{clad}\right)\frac{k_0^2}{\beta_j}\int_{d_j} A_i(y)A_j(y)dy \tag{5.6}$$

with d_j the diameter of the j-th waveguide. In the case of two identical guides, $C_{ij} = C$ and $\Delta\beta = 0$, enabling full power transfer from i to j. For light injection in waveguide 1, the intensity of each mode after propagation through the interaction region L is given by

$$\forall\, z \in [0, L] \begin{cases} I_1(z) = I_1(0)\, cos^2(C\, z) \\ I_2(z) = I_1(0)\, sin^2(C\, z) \end{cases} \tag{5.7}$$

and results in an oscillating power along z with period $P = \pi/C$. In order to achieve a small device footprint with a transfer of 50 %, L will be optimised to observe only a quarter of this oscillation.

According to Eq. 5.6, the coupling strength is dependent on the refractive index of the waveguide, which in turn is polarisation dependent due to the intrinsic birefringence. The splitting ratio is therefore different for H and V polarisations in planar couplers and results in the rotation of the $\pm 45^o$ states. Although this property can be exploited to obtain a partially polarising beamsplitter [59], it represents a major drawback for our application.

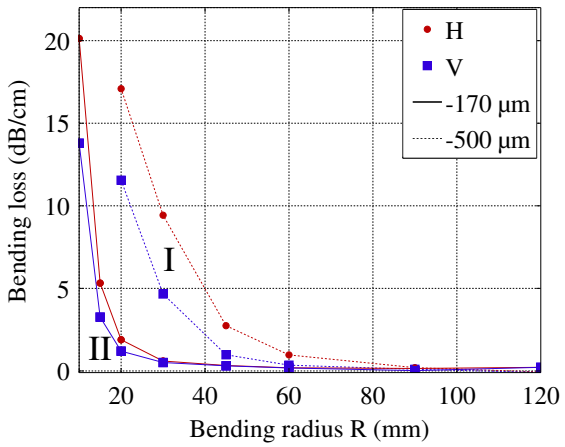


Figure 5.5.: Influence of the radius of curvature on the bending losses α. The dependency is shown for the waveguide depth of 500 µm (I) and 170 µm (II).

In addition, curved waveguides also suffer from bending losses $\alpha_{H,V}$ due to wavefront distortion and coupling to radiative modes. The losses are highly dependent on the field confinement and on the quality of the core-cladding interface. Figure 5.6 illustrates the effect of the radius of curvature and of the writing depth onto the strength and polarisation dependency of the losses. As aforementioned, smoother refractive index profiles are obtained at a depth of 170 µm, resulting in much lower bending losses.

The polarisation dependence of both the splitting ratio and the bending losses contribute to the rotation of the diagonal states in the equatorial plane. If the state

$$|\psi\rangle_{in} = \frac{|H\rangle + |V\rangle}{\sqrt{2}} \tag{5.8}$$

is sent into the input port (1), the state transmitted into (2') will be defined as

$$|\psi\rangle_{out} = \sqrt{\frac{t_H \cdot 10^{-\alpha_H \cdot l/10}}{2}}|H\rangle + \sqrt{\frac{t_V \cdot 10^{-\alpha_V \cdot l/10}}{2}}|V\rangle \tag{5.9}$$

with l the length of the curved path. For a radius of curvature $R = 30\,\text{mm}$, the couplers I exhibit losses of $\alpha_H = 9.4\,\text{dB/cm}$ and $\alpha_V = 4.7\,\text{dB/cm}$, and a transmission from (1) to (2') of 56.2 % for H and 48.2 % for V. A 45^o input polarisation will therefore be reflected into the output port (1') with a linear polarisation of 72.7^o and transmitted into (2') as 69.9^o. In this case the drastic losses α_H mainly dictate the "rotation" towards V. This effect is already strongly attenuated in the higher quality waveguides of the second set (II), where $\alpha_H = 0.33\,\text{dB/cm}$ and $\alpha_V = 0.31\,\text{dB/cm}$ can be achieved with a radius of 45 mm. Although it would be in principle possible to optimise the input states to pre-compensate for these rather strong polarisation dependence of the splitting ratio, a more elegant solution based on a three-dimensional architecture has been adopted.

5.3. Study of three-dimensional waveguide arrays with polarisation insensitive behaviour

5.3.1. Architecture optimisation

The polarisation dependence of the splitting ratio finds its origin in the birefringence of the waveguides, which leads to a different confinement of the modes along both axes. Consequently, the transmission of H and V states through the coupler is different if both waveguides lie in a horizontal plane or are vertically aligned. This idea was used by Dr. Osellame's group to demonstrate that identical coupling can be achieved for both polarisations by writing each arm at a slightly different depth, thereby introducing an elevation angle Θ between them [110]. New samples with an average writing depth of 170 µm have been fabricated in order to find this optimal angle. As shown in Fig. 5.6a, identical transmission can be obtained at $\Theta = 57^o$.

The influence of the interaction length on the splitting ratio was directly investigated in the final layout comprising four inputs and one main output depicted by a red arrow in Fig. 5.7. The three-dimensional architecture includes couplers with a bending radius $R = 45\,\text{mm}$ and an elevation angle between the waveguides of $\Theta = 57\,^o$. As the beams from all inputs are only overlapped in the main output, the other outputs are deviated both vertically and horizontally to limit their collection efficiency in the final module. In addition, a thin absorber will be placed after the chip to block the undesired light.

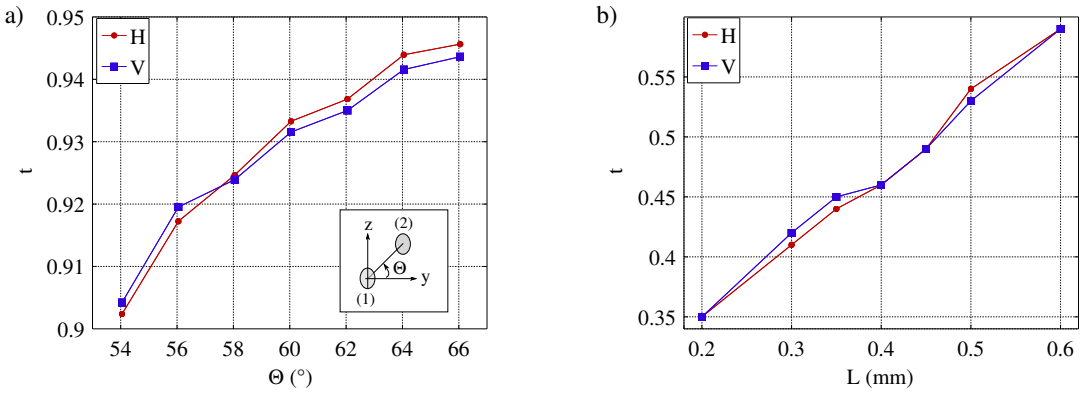


Figure 5.6.: Optimisation of the directional coupler parameters to obtain a 50/50 beam-splitter for both H and V polarisations (courtesy of Dr. Osellame's group). (a) The optimal angle $\Theta = 57^o$ allows identical coupling for both polarisations. (b) The interaction length can then be tuned to achieve 50 % transmission.

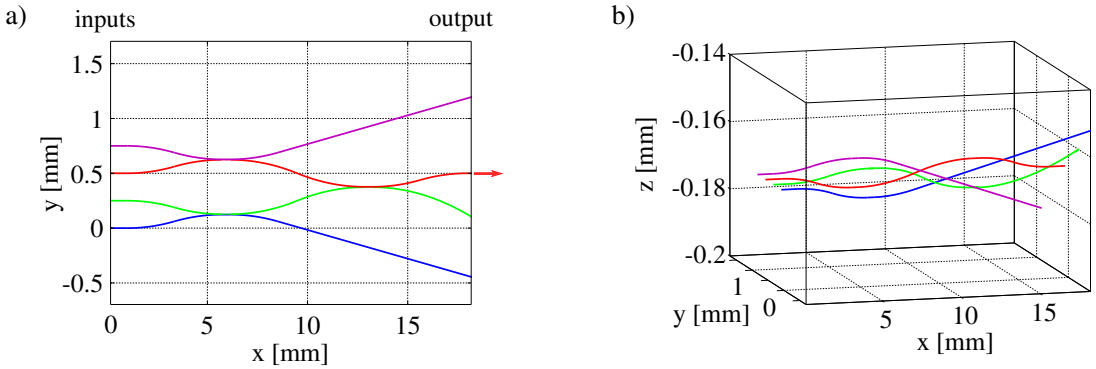


Figure 5.7.: Layout of the polarisation independent mode mixer. (a) Top view and (b) 3d view of the waveguide chip. The four inputs are located on the left, and the red arrow indicates the main output. The other exits are deviated from the central axis to limit the collection efficiency before being blocked by an external absorber.

In order to retrieve the splitting ratio of the three couplers assumed to be identical, polarised light was injected from the back of the chip into the main output, and the relative intensities p_i emerging from each of the four inputs i were analysed using a CCD camera. Depending on the path, the beam experiences a combination of transmission and reflection at the directional couplers. The transmission t of the coupler is determined by

least square fitting of the overdetermined system:

$$\begin{cases} p_1 = t\,(1-t) \\ p_2 = (1-t)^2 \\ p_3 = (1-t)\,t \\ p_4 = t^2 \\ p_1 + p_2 + p_3 + p_4 = 1 \end{cases} \tag{5.10}$$

Directional couplers with interaction lengths between 200 µm and 600 µm have been characterised, and exhibit low polarisation dependence, as shown in Fig. 5.6b. The interaction length of $L = 450$ µm guarantees the closest result to a 50:50 splitting ratio.

5.3.2. Process tomography

The previous measurements indicate that the splitting performed by the coupler is rather polarisation insensitive, but do not provide any information on the conservation of the polarisation state during the propagation. The precise action of the device onto the input states can be determined by a process tomography. In practice, the six states forming the X, Y and Z bases and defined by their Stokes vector $\overrightarrow{S_{in}}$ are prepared using a polariser, a half-wave plate and a quarter-wave plate and injected into the waveguide under test. The corresponding output states $\overrightarrow{S_{out}}$ are reconstructed with the help of a quarter-wave plate and a polariser, as explained in Section 3.2.3. For each input state we obtain an equation of the form:

$$\overrightarrow{S_{out}} = \mathbf{M}\,\overrightarrow{S_{in}} \tag{5.11}$$

where $\mathbf{M}$ is the characteristic 4×4 Müller matrix. The system of six equations associated with each waveguide is overdetermined, and the Müller matrix can therefore be retrieved by a least-square fitting over the complete dataset.

To align the basis measurements of the tomography with the eigen-axes of the chip, the tomography was first performed on a straight waveguide, and then on the mode mixer, where the output state was only characterised for the main output. As an example the action of the different waveguides onto an H input state is shown in Fig. 5.8, while the complete data are shown in Appendix B.

For a perfect alignment, the H-state coincides with one of the optical axes defined during the fabrication and is therefore conserved through the chip. This statement is perfectly verified for the propagation through a straight waveguide (red), as its projection along V is vanishing and amounts to 0.5 along both eigenvectors of the X, Y bases. Yet the curved waveguides all exhibit a slightly different behaviour, where H can be rotated in the equatorial plane and even pick a waveguide-dependent phase. This effect was attributed to the three-dimensional structure of the directional couplers, as recently reported in [107]. The stress field surrounding each waveguide acts like an additional birefringent element onto a neighbouring waveguide, and the orientation of the induced optical axes depends on the relative position of the waveguides. In the considered sample, the elevation angle between both arms is not constant along the path and leads to a complex polarisation rotation. Moreover, each waveguide perceives a different environment and therefore performs a specific transformation.

In principle, these small rotations can be pre-compensated by slightly rotating the input states such that the required BB84-states are obtained at the output of the chip.

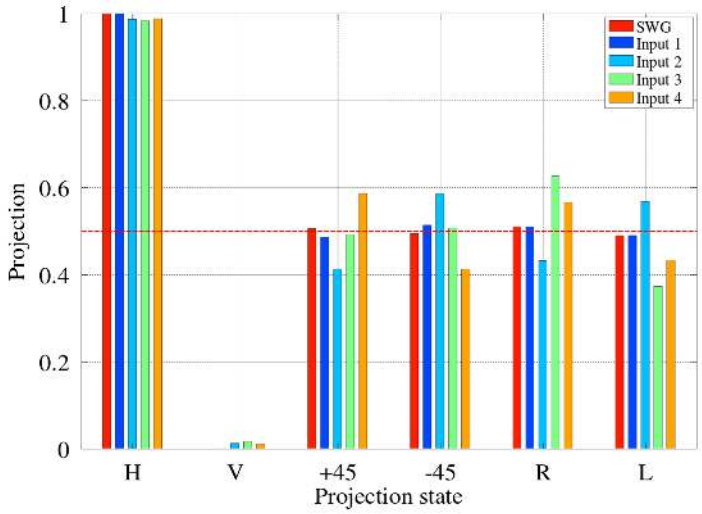


Figure 5.8.: Analysis of the states coming out of the main output when the state H is sent in one of the four inputs. The result obtained for a straight waveguide is shown in red for comparison.

These optimal input states have been implemented in the wire-grid polarisers presented in Fig. 4.14.

5.3.3. Computation of optimal input states

The computation of these optimal input states was based on a Müller matrix (thereafter referred to as $\mathbf{M_{16}}$) retrieved by a least-square fitting procedure where the 16 elements were considered independent. The program then looked for the input states $\overrightarrow{S_{in,opt}}$ such that the projection of $\overrightarrow{S_{out,opt}} = \mathbf{M_{16}}\,\overrightarrow{S_{in,opt}}$ onto a defined BB84 state is maximum (or the QBER minimum). As the output states exhibit an elliptical polarisation due to the birefringence of the waveguides, a global Phase Compensation (PC) step rotating the states back to a set of linear polarised states is necessary for this optimisation criterion to be meaningful. Such unitary operation can be realised by a succession of two quarter-wave plates and a half-wave plate, corresponding to the transformation matrix $T_{PC} = \mathbf{T'}(\alpha,\pi)\,\mathbf{T'}(\beta,\pi/2)\,\mathbf{T'}(\gamma,\pi/2)$ where

$$\mathbf{T'}(\theta,\delta) = \mathbf{T_z}(-\theta)\,\mathbf{T_x}(\delta)\,\mathbf{T_z}(\theta) \tag{5.12}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & cos(\delta)\,sin^2(\theta)+cos^2(\theta) & [1-cos(\delta)]\,cos(\theta)\,sin(\theta) & sin(\delta)\,sin(\theta) \\ 0 & [1-cos(\delta)]\,cos(\theta)\,sin(\theta) & cos(\delta)\,cos^2(\theta)+sin^2(\theta) & -sin(\delta)\,cos(\theta) \\ 0 & -sin(\delta)\,sin(\theta) & sin(\delta)\,cos(\theta) & cos(\delta) \end{bmatrix} \tag{5.13}$$

represents a uni-axial material with its optical axis rotated by an angle θ with respect to H and producing a phase shift δ.

The resulting optimal input states are slightly rotated with respect to the BB84-states, as shown in Table 5.1. QBERs below 0.2 % were predicted, but not verified experimentally. As will be shown in Section 6.3.2, the quality of the output states is not as high

as expected, with an order of magnitude discrepancy between the theoretical and experimentally observed QBERs. The resulting error ratios have been underestimated, and the expected quality device value $q = 0.92$ overestimated.

Input port	1	2	3	4
Optimal input State	-0.95^o	-43.86^o	39.94^o	86.76^o
Output state	H'	$+45$'	-45'	V'
Predicted QBER	**0.07 %**	**0.14 %**	**0.10 %**	**0.13 %**
Experimental QBER	**1.3 %**	**6.4 %**	**2.6 %**	**2.6 %**

Table 5.1.: Optimal linear input states computed by minimising the QBER of the output state ($\overrightarrow{S_{out,th}} = \mathbf{M_{16}}\,\overrightarrow{S_{in}}$). The calculation of the QBER includes a global phase compensation of about $\pi/6$. The experimental error rate measured at the output of the complete Alice module (see Chapters 6 and 7) stronly deviates from the predicted values.

5.3.4. Discussion

A separate study was conducted after the assembly of the complete sender unit to investigate the large discrepancy between the calculated and the observed output states (see Section 6.3.2). While the influence of the input state preparation by the micro-polarisers is discussed in the following chapter, here we report on possible sources of errors in the data analysis or in the tomographic measurement itself.

First, the rotation experienced by the input states is mainly due to birefringent effects, and is therefore expected to correspond to a practically unitary transformation. The polarisation dependence of the bending losses ($\Delta\alpha = 0.04\,\mathrm{dB}$) can be neglected in first approximation, as they lead to a minimal rotation of the $\pm 45^o$ states by less than 0.3^o. The program developed elsewhere used for the analysis retrieved the Müller matrix based on an independent fitting of the 16 matrix elements. The lack of constraints during the fitting procedure led to non-unitary Müller matrices, such that the computed output states exhibit a degree of polarisation up to 1.08. The QBER was thus underestimated due to a calculation on unphysical states (*i.e.*, with a norm larger than 1).

In a second step, the validity of the measurement presented in Fig. 5.8 was verified by trying to fit a unitary Müller matrix $\mathbf{M_{unit}}$ to the experimental data. An arbitrary rotation can be written as $\mathbf{M_{unit}}(\alpha,\beta,\gamma) = \mathbf{T_x}(\alpha)\,\mathbf{T_z}(\beta)\,\mathbf{T_x}(\gamma)$ where α, β and γ are the three Euler angles and

$$\mathbf{T_x}(\theta) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & cos(\theta) & -sin(\theta) \\ 0 & 0 & sin(\theta) & cos(\theta) \end{bmatrix} \tag{5.14}$$

$$\mathbf{T_z}(\theta) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & cos(\theta) & sin(\theta) & 0 \\ 0 & -sin(\theta) & cos(\theta) & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{5.15}$$

correspond to rotations around the X-axis and Z-axis, respectively. In principle the

goodness of a fit can be evaluated using a chi-squared test, where the ratio

$$\frac{\chi^2}{\nu} = \frac{1}{N_D - N_{FP} - 1} \sum_{i=1}^{6} \left(\frac{\overrightarrow{S_{out,i}} - \mathbf{M_{unit}}\, \overrightarrow{S_{in,i}}}{\Delta S_i} \right)^2 \tag{5.16}$$

is equal to 1 for a perfect fit, provided that an accurate statistical model is available for the data. Ratios above 5 or below 1/5 can, as a rule of thumb, be associated either to an inadequate fit or noise model, or to an inappropriate number of parameters (N_D represents the number of experimental data points and N_{FP} the number of free parameters that are fitted). As we do not dispose of any statistics for this measurement, this quantitative criterion cannot be used here.

We then try to estimate the fit goodness by comparing directly the experimental and computed output Stokes vectors ($\overrightarrow{S_{out,th}} = \mathbf{M_{unit}}\, \overrightarrow{S_{in}}$). Table 5.9a shows the angular discrepancy α between both states, as measured in the Poincaré sphere. For linearly polarised states, the angle $\alpha/2$ corresponds directly to the difference in polarisation. The preparation and the analysis of the state involved several wave plates, which between two crossed-polarisers delivered a contrast about 1:5,000. The resolution of these components is thus evaluated around 0.8^o, while the precision of the stepper motors used to rotate them is around 0.5^o. The angular error observed, *e.g.*, for X and Y input states injected into inputs 1 and 3, can thus be explained by the measurement accuracy. Nevertheless, the deviations observed for the inputs 2 and 4 are on average much larger, even reaching 11^o. Moreover, the value of α associated to diagonal states is high, regardless of the input waveguide.

Figure 5.9b illustrates the discrepancy between experimental and reconstructed states on the equatorial plane of the Poincaré sphere. For sake of clarity, only linearly polarised input states are represented. For the first input, and similarly for the third one, the measured output states still form orthogonal bases ($\beta_{H,V}, \beta_{\pm 45^o} > 88^o$), as opposed to input 2 and 4. Here both $|H\rangle$ and $|V\rangle$ states are rotated towards $|-45\rangle$, forming an angle $\beta_{H,V} = 80.6^o$ only and therefore suggesting a non-unitary transformation. As the layout shown in Fig. 5.7a is symmetric, it is reasonable to assume that the waveguides 1 and 4 should not exhibit a fundamentally different behaviour.

By looking again at the tomographic data, we discovered a strong dependence of the total intensity with the input state when the light was injected into the waveguides 2 and 4, (see Table 5.2). Since this variation cannot be explained by the polarisation dependent losses alone ($\Delta\alpha = 0.04\,\mathrm{dB}$), we conjecture that the coupling efficiency might have changed with the polarisation of the input state. Such effect can occur when one of the preparation wave plates is tilted. A misalignment would lead to the preparation of the wrong input states, thus preventing the retrieval of a faithful Müller matrix.

a)

Input state	Input port			
	1	2	3	4
$\|H\rangle$	2.3^o	9.4^o	1.6^o	8.8^o
$\|V\rangle$	2.2^o	8.6^o	3.5^o	10.0^o
$\|A\rangle$	7.8^o	9.3^o	6.3^o	5.8^o
$\|D\rangle$	9.2^o	9.6^o	9.1^o	11.0^o
$\|R\rangle$	1.6^o	7.9^o	1.3^o	8.0^o
$\|L\rangle$	$1.6\ ^o$	7.1^o	2.0^o	8.8^o
$\Delta\alpha$	$(4.1 \pm 3.4)^o$	$(8.6 \pm 1.0)^o$	$(3.9 \pm 3.11)^o$	$(8.7 \pm 1.8)^o$

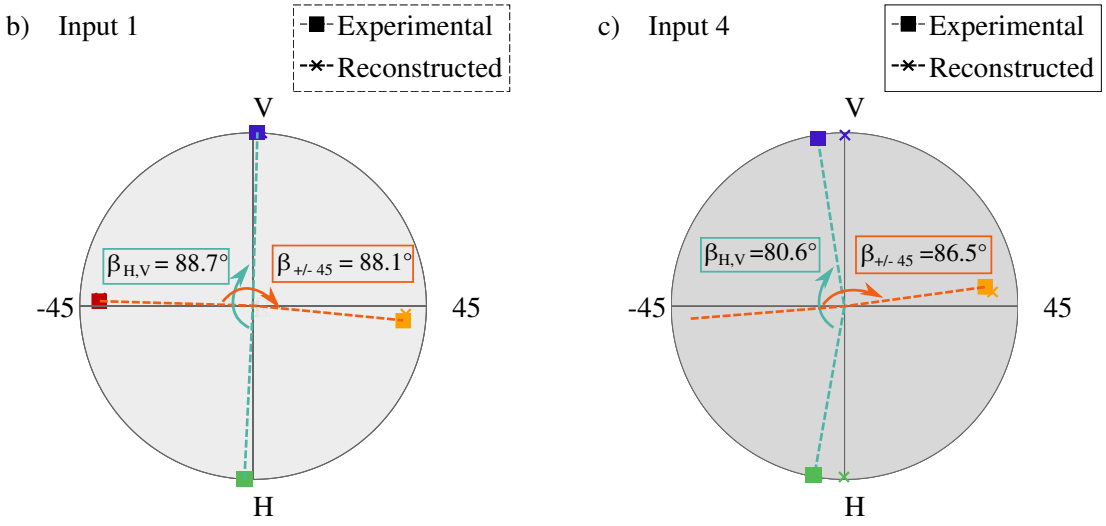


Figure 5.9.: Comparison between the measured output states $\overrightarrow{S_{out,exp}}$ and the predicted output states calculated using a unitary matrix ($\overrightarrow{S_{out,th}} = \mathbf{M}\,\overrightarrow{S_{in}}$). (a) Angular deviation α between both states in the Poincaré sphere ($\alpha/2$ corresponds to the error in the linear polarisation for linearly polarised states). (b,c) Illustration of the discrepancy on the equatorial plane of the Poincaré sphere for linearly polarised input states injected in the first and in the fourth input port, respectively. In the second case, the experimental output states (H,V) do not form an orthogonal basis, suggesting a non-unitary transformation.

Input state	Input port			
	1	2	3	4
$\|H\rangle$	23.15	39.26	47.34	54.55
$\|V\rangle$	21.96	39.73	45.55	53.59
$\|R\rangle$	22.06	42.34	47.70	50.50
$\|L\rangle$	23.04	36.47	45.17	57.57
$\|A\rangle$	22.68	34.29	47.30	62.40
$\|D\rangle$	22.47	44.33	45.71	46.11
I_{mean}	22.56	39.49	46.46	54.14
σ_I	0.49	3.73	1.10	5.62
σ_I/I_{mean}	2.2 %	**9.4 %**	2.4 %	**10.4 %**

Table 5.2.: Variation of the total output intensity with the input state during the tomographic measurement. The intensity was measured with a power-meter and is given in microwatts.

6. Assembly and characterisation of the Alice module

So far we have presented the characterisation of the key optical elements required for a hand-held Alice unit producing four polarised weak coherent pulses. A few additional components such as collimation optics and a visible beacon laser are necessary to ensure efficient short-range communication with a user-friendly aiming procedure. In this section we describe the properties of these supplementary elements, as well as the assembly protocol for their integration onto a miniature micro-optical bench. We also evaluate the quality of the mounting procedure and of the generated set of output states.

6.1. Additional optical elements

6.1.1. Collimation optics

The beam emerging from the waveguide chip with a divergence of 4.6^o has to be collimated in order to reach operation distances of at least 50 cm. As presented in Chapter 2, small aspheric lenses are good candidates as they offer small footprints and sufficient focal lengths. Here a lens (*354130*, Lightpath) with 3 mm outer diameter and 2.6 mm clear aperture, and a back focal length of 4.9 mm was used. An anti-reflection coating optimised for red and infrared wavelengths (600-1050 nm) prevents additional reflection losses.

6.1.2. Visible beacon laser

A multi-mode red beacon VCSEL emitting around 680 nm (*680S-0000-X003*, Vixar) is overlapped with the infrared signal in order to facilitate the aiming into the receiver. Additionally, this laser can be modulated at 100 MHz repetition rate with 50 % duty cycle to synchronise Alice's board with Bob's computer. The bright beacon and the weak signal can be separated on Bob's side using a dichroic mirror (see Chapter 7). For easier handling, the multi-mode beacon VCSEL is packaged in a $3 \times 3\,\mathrm{mm}^2$ chip carrier.

6.1.3. Dichroic beamsplitter

In order to overlap the red and infrared signals, a miniature beamsplitter with almost perfect reflection for the former and perfect transmission for the latter is required. This component can be found in DVD-players, where both 650 nm and 790 nm lasers beams are combined in order to guarantee the reading of DVDs and CDs. The $3.5 \times 3.5 \times 3\,\mathrm{mm}^3$ ($L \times l \times h$) dichroic beamsplitter extracted from a commercial device exhibits low losses at $\lambda = 850\,\mathrm{nm}$ and almost 50:50 splitting ratio in the red (see Table 6.1) and is therefore perfectly suitable for our module. The dimensions of the cube allow its placement between the waveguide chip and the collimating lens. The distance to the output facet of the photonic circuit on one hand and to the chip carrier containing the beacon on the other hand are optimised with Zemax simulations.

λ	R	T
680 nm	48.3 %	51.7 %
850 nm	< 0.2 %	> 99.8 %

Table 6.1.: Characterisation of the miniature beamsplitter at signal ($\lambda = 850$ nm) and beacon ($\lambda = 680$ nm) wavelengths for 45^o input polarisation.

6.2. Assembly onto a micro-optical bench

The planned architecture presented in Fig. 2.3 allows for a two-step assembly of the module. First, the flat optical elements such as the micro-lenses, the polariser array, and the ND filter can be directly stacked onto the PCB where the VCSEL array is bonded. Two consecutive components are separated by glass spacers of optimal thickness in order to ensure a high coupling efficiency into the waveguide. As a clean optical surface is necessary to guarantee a good beam quality, the elements are held from the side by a vacuum gripper equipped with a home-made suction cup, as shown in Fig. 6.1a. The gripper is mounted onto a 6-axis stage with a spatial resolution of 10 nm enabling fine positioning of the components onto the board. A lateral CCD camera monitors the closing of the air gaps between the components, thereby also allowing to adjust the pressure to avoid potential damage. A second camera placed in the beam direction controls the transverse placement and the tilting of the elements. The stack is held together with a high-viscosity, low shrink glue (*OP-67-LS*, Dymax) that can be cured within a few seconds using ultraviolet radiations.

Figure 6.1b illustrates the alignment of the micro-lens array using the top camera, while the critical positioning of the polariser array is presented in Fig. 6.1c. In order to prepare the right input states, the orientation of the VCSEL array and of the polariser array should perfectly overlap. As the area of each polariser ($120 \times 120\,\mu m^2$) is much larger than the beam in order to avoid diffraction effects, it is possible to observe transmission of the four laser beams, even though the polariser array is rotated. In the worst case scenario, the leftmost beam is located in the upper left corner of the corresponding polariser, while the rightmost beam is in the lower right corner of the right polariser, or vice versa, leading to a maximum misalignment of $\alpha = arcsin(120/750) = 9.2^o$. In practice, the VCSEL array is fixed, and its orientation can be finely resolved and marked with a white line when the camera focuses on the focal plane of the beams, which lies above the polariser surface. The VCSELs are then turned off and the polariser array, here marked with a red line, is rotated until it is aligned along this white line. Experimentally, angles well below 1^o are obtained.

In a second step, the waveguide circuit, as well as the beacon laser and the beamsplitter have to be assembled with the PCB. In the final configuration, the output signal has to follow a horizontal path within the device and towards the receiver. The waveguide circuit has therefore to be in a horizontal position, but its length and weight are superior to the previously assembled components and might turn the whole chip into a lever arm. In order to increase the mechanical stability of the module, we designed an aluminium Micro-Optical Bench (MOB) with predefined positions to support the heavy parts. The bench is anodised to avoid strong reflection from the metallic surface, inconvenient for the alignment of glass components. The PCB is placed in a vertical slit such that the emitted beams are parallel to the surface of the bench. The top camera now controls

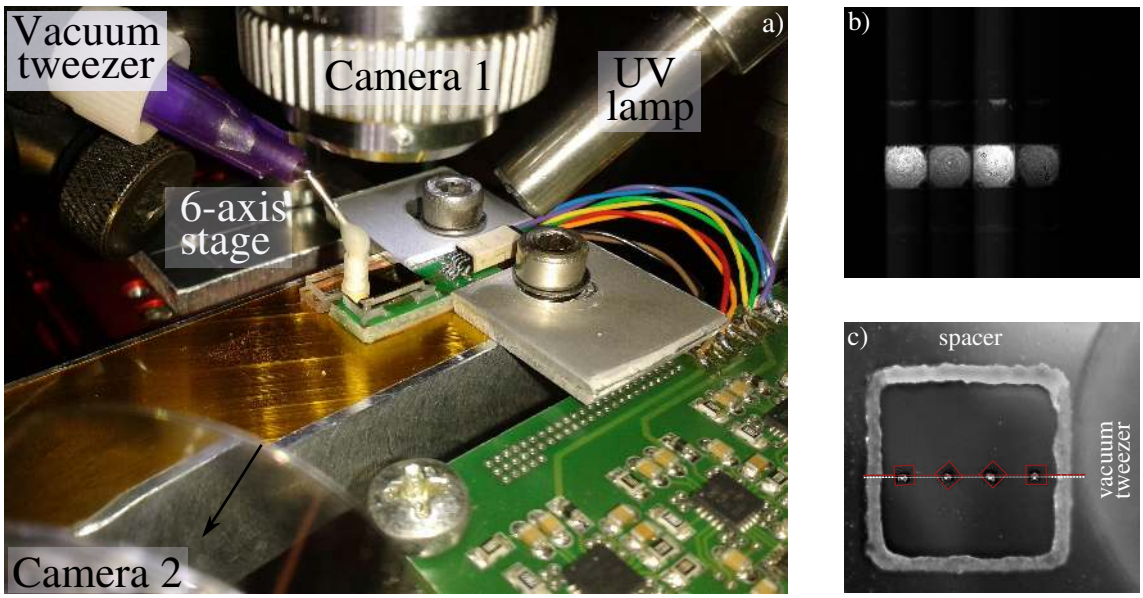


Figure 6.1.: Stacking of the first micro-optical components onto the PCB. The board is clampled while the components are placed using a vacuum gripper mounted onto a 6-axis stage. (a) Picture of the assembly line. (b) Top view of the adjusted micro-lens array. (c) Alignment check between the polarisers array (red line) with the VCSEL array (white line). Picture obtained by subtraction of pictures focused on the polarisers and on the beam foci, respectively.

the air gaps, while the lateral camera is moved to the end of the MOB along the beam direction to monitor the lateral alignment. The waveguide circuit is picked from the top and positioned using the previously described set-up. The coupling in the different waveguides can be verified by only looking at the coupling of the first and last VCSEL from the array. Both beams contribute to the main output mode, only the beam launched in the i-th input port will contribute to the intensity emerging from the i-th output port. If the same intensity is sent into both input ports 1 and 4, the intensity emerging from the first and last output ports is directly proportional to the coupling efficiency of the diodes 1 and 4, respectively. Using the polarisation-dependent LI-curve presented in Fig. 3.7b, the bias current could be chosen to ensure that similar intensities are launched into the circuit, although the prepared polarisation states slightly differ from the $\{H, V, D, A\}$ states used in the tomography. Figure 6.2a shows the output facet of the chip when a good coupling is achieved into all the waveguides.

Once the chip is fixed onto the bench, a spatial filter consisting of an NDF with a slit of about 500 µm is placed after the waveguide to select the right output mode. The optical density was increased from 0.9 to 3.5 by darkening both faces with black ink using a commercial marker. The beamsplitter, separately assembled with the aspheric lens, is then positioned. The collimation of the beam is monitored by a camera placed 60 cm away from the bench. While the theory predicts a radius of $437 \times 475\,\mu m^2$, an experimental value of $451 \times 463\,\mu m^2$ is obtained. Finally, the beacon laser is overlapped with the infrared signal, as shown in Fig. 6.2b. The position and direction of the visible beam are verified simultaneously at two different z-positions using CCD cameras placed at 12.5 cm and

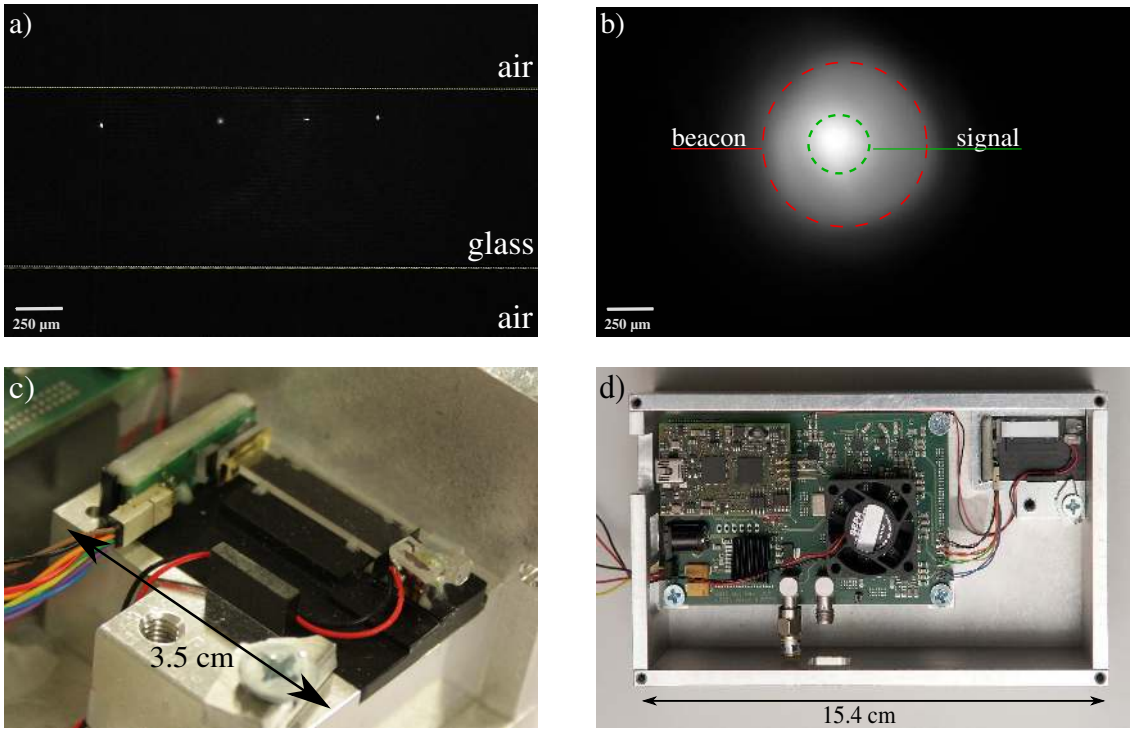


Figure 6.2.: Integration of the PCB and remaining optical components onto the micro-optical bench ($35 \times 20 \times 8\,\mathrm{mm}^3$). (a) Imaging of the output facet of the waveguide after assembly onto the MOB. (b) Output beam profile showing the overlap between the beacon laser and the infrared signal at 60 cm distance. The circles help visualise the contribution of both wavelengths. (c) Picture of the resulting Alice device. (d) Hand-held platform ($154 \times 88 \times 47\,\mathrm{mm}^3$) including the optics and the control electronics.

60 cm, respectively. The resulting micro-optics device (see Fig. 6.2c) is placed with its driving electronics into an aluminium box with dimensions $154 \times 88 \times 47\,\mathrm{mm}^3$ for easier use as hand-held platform.

6.3. Quality of the assembled Alice module

6.3.1. Coupling and collection efficiencies

The intrinsic losses of the different optical elements forming the Alice module have been previously characterised and can be used to calculate the theoretical transmission through the complete device, as shown in Table 6.2. The power emitted by the VCSELs was known before the assembly (see Section 3.3.1), and can be compared to the value obtained at the output of the micro-optical bench. The discrepancy between the expected and measured transmission is largely due to the coupling efficiency into the waveguide. Continuous-wave and pulsed regime measurements have been performed with a power-meter and an APD, respectively. They deliver similar results with a uniform coupling efficiency varying from 19 % to 22 % depending on the waveguide. Given the complexity of the waveguide chip

alignment procedure to achieve simulatenous coupling into the four input ports, and the maximal coupling of 60 % determined by Zemax simulations, the experimental values are considered to be very satisfying.

Element	Transmission	Comment
ND-Filter	8 %	Transmission at 850 nm
Wire-grid polariser	9 %	
Waveguide chip	71 %	Propagation and bending losses
	25 %	Selection of the main output
Air-glass interfaces	64 %	11 interfaces, each accounting for a 4 % loss
Total	0.082 %	

Table 6.2.: Expected transmission of the assembled Alice module based on the intrinsic losses of the different components.

6.3.2. Set of generated output state

The states prepared by the miniature sender unit were reconstructed by a full polarisation analysis using a quarter-wave plate, a polariser and a free-space APD, as explained in Section 3.2.3. The raw data are shown in Appendix B and the output states are presented in Fig. 6.3. Unfortunately, the quality of the set of states is not as high as predicted in the previous chapter. All linear polarisations deviate from the BB84 states by at least a few degrees, even reaching an error of 18 ^{o} for $|D\rangle$.

a)

VCSEL	Azimuth (^{o})	Phase (rad)
1 (V)	90.1^o	-0.07
2 (D)	63.1^o	-0.21
3 (A)	-48.5^o	0.24
4 (H)	3.9^o	0.12

b)

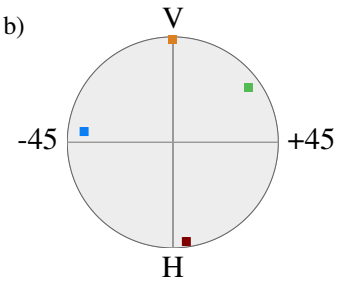


Figure 6.3.: Polarisation states generated by the Alice module reconstructed by tomography. (a) Linear polarisation and phase of the output states and (b) visualisation of the states on the equatorial plane of the Poincaré sphere.

As mentioned in Chapter 4, the input states prepared by wire-grid polarisers are slightly rotated with respect to the calculated optimal states. To evaluate the impact of these imperfections onto the quality of the output states, we computed again the expected states using the retrieved Müller matrix and the input states defined by the polarisers, as presented in Table 4.3. Table 6.3 clearly shows that the linear polarisation component of the output states could not be reproduced by the tomographic measurement performed on the waveguide chip (the phase cannot be compared, as the output states acquire an additional phase after the waveguide due to the slightly birefringent beamsplitter cube).

The discrepancy between calculation and experiment is particularly extreme for the second channel, where the tomographic characterisation was found to be of low quality (see Section 5.3.4). As the errors in the characterisation of the waveguide chip were only discovered at this point, *i.e.*, after the assembly of the complete module, we decided to evaluate the achievable performance of the device in a potential QKD experiment before deciding if the micro-optics setup should be dismantled only to perform the tomography of the waveguide chip again.

		Expected output state			
		$\mathbf{M} = \mathbf{M_{16}}$		$\mathbf{M} = \mathbf{M_{unit}}$	
VCSEL	Input state α_{pol}	Azimuth	Phase (rad)	Azimuth	Phase (rad)
1 (V)	89^o	90.2^o	0	89.6^o	0
2 (D)	44.6^o	-43.1^o	-0.27	-42.9^o	-0.27
3 (A)	-50.1^o	44.7^o	0.24	45.6^o	0.25
4 (H)	-1^o	1.55^o	0.08	-1.1	^{o} 0.07

Table 6.3.: Predicted output states $\overrightarrow{S_{out}} = \mathbf{M}\,\overrightarrow{S_{in}}$ where $\mathbf{M}$ is the Müller matrix retrieved from the tomography presented in Section 5.3.4 using either a least-square fit over 16 independent entries ($\mathbf{M_{16}}$) or over a unitary matrix ($\mathbf{M_{unit}}$). The input vector $\overrightarrow{S_{in}}$ corresponds to the state prepared by the wire-grid polariser.

6.3.3. Phase compensation

While the BB84 protocol requires in principle four states forming two mutually unbiased bases, a key exchange can still take place when the preparation of the states is not perfect. The quality of the set of states can be described by two parameters that are relevant for the extraction of secure bits: the quantum bit error ratio (QBER), which characterises the probability for Bob to detect the wrong state when he performs a measurement in the right basis, and the quality factor q [20] which calculates the maximum overlap between two vectors of different bases.

In our case, the polarisation states emerging from the sender are elliptical due to the birefringence of the waveguide and of the beamsplitter. A phase compensation (PC) scheme is thus necessary to rotate them back to linear states before calculating or performing their projection onto any BB84 state (see Section 5.3.3). The angles of the three wave plates required to perform this operation are optimised by minimising the average QBER over the four states with a least-square fit. A common problem with optimisation procedures is the existence of local minima, which prevent the algorithm to find the absolute minimum of a function. One solution to detect such a case consists in trying different sets of initial conditions, or to test all possible combinations of input parameters, which can be cumbersome. The first solution, then considered as optimum, turned out to be such a local minimum, and as lower experimental QBERs have been observed later on (see Chapter 7). The implementation of the same algorithm on a different software delivered an achievable QBER of 3.2 %, as shown in Table 6.4.

Nevertheless, the phase shift cannot compensate for the deviation of the $|D\rangle$ and $|A\rangle$ from the theoretical $\pm 45^o$ states. Even for the optimal transformation, the overlap of

	V	D	A	H	Total
QBER	2.6 %	2.6 %	6.4 %	1.3 %	3.2 %

Table 6.4.: Predicted QBER resulting from the imperfect polarisation states under assumption of a perfect phase compensation ($\alpha = 41.2^o$, $\beta = 57.8^o$, and $\gamma = 46^o$). The experimental verification of the achievable error ratio is shown in Chapter 7.

both states of the X-basis with $|V\rangle$ is well above the expected value of 0.5:

$$|\langle V|A\rangle|^2 = 0.70 \qquad |\langle V|D\rangle|^2 = 0.65 \tag{6.1}$$

The device quality q is related to the maximum overlap between two vectors of different bases according to the following relation:

$$q = -log_2 \left[\max_{(\psi_x,\psi_z)} \left(|\langle \psi_x \mid \psi_z \rangle|^2 \right) \right] = -log_2 \left[|\langle V|A\rangle|^2 \right] \tag{6.2}$$

The imperfect preparation of the states thus yield a device quality of $q = 0.51$, resulting in a reduction of the number of sifted bits by an additional factor of 2. As the state $|D\rangle$ is mainly responsible for the large value of the total QBER, we considered implementing the *3-state protocol* (TSP) proposed by Fung *et al.* [111], where this state could simply be left out. This protocol was initially developed to ensure the functionality of the sender device when technical problems prevent the preparation of one of the polarisation states. Here a phase compensation optimised for the three other states predicts an average QBER of 1.5 %, as detailed in Table 6.5. Excellent agreement between the calculations and the experimental verification has been observed.

		V	A	H	Total
QBER	simulated	1.8 %	1.3 %	1.50 %	1.5 %
	observed	**2.2 %**	**1.4 %**	**0.9 %**	**1.5 %**

Table 6.5.: Optimal phase compensation minimising the average QBER for the 3-state protocol. The angles of the waveplates are $\alpha = 137.5^o$, $\beta = 117.5^o$ and $\gamma = 74.5^o$.

In this case the Z-basis is used for the key generation while $|A\rangle$ is used only to detect the presence of an eavesdropper. The QBER observed in the Z- and X-basis are noted α and e_b, respectively. Error correction has to be performed in the Z-basis only, while privacy amplification takes into account the phase error rate depending on error rates in both bases. For faint laser pulses the secret key rate is defined as

$$R_{sec} = R_{sift} \cdot \left((1-\Delta) - f(e_b) \cdot H_2(e_b) - (1-\Delta) \cdot H_2 \left(\frac{e_p}{1-\Delta} \right) \right) \tag{6.3}$$

where the phase error rate e_p is upper-bounded by [111]

$$e_p \leq \alpha + 2e_b + 2\sqrt{e_b \alpha} \tag{6.4}$$

This protocol requires stronger privacy amplification than the BB84 protocol, where usually $e_b = \alpha$, compared to $e_p \leq 5\alpha$ for the TSP. This accounts for the fact that Eve introduces less error in the three-state case although she obtains the same amount of information as in BB84. Indeed, Eve knows that she measured in the wrong basis when she detects the fourth unused state (here $|A\rangle$) and does not risk being detected by sending another photon, as the bit will be discarded anyway. Due to this stronger key reduction, the secure key rate of the TSP does not necessarily exceed the one obtained with the standard BB84 protocol, even when lower QBERs are achieved. Also, it is not clear how the imperfections of the generated state preparation influence the final key in this case. The potential performances of both protocols will be compared in the next chapter using the achievable experimental parameters.

7. Quantum Key Distribution experiment

The quality of the resulting Alice module is finally evaluated in a proof-of-principle quantum key distribution experiment. In this section we briefly present the optical setup of the receiver (Bob) developed and characterised by T. Vogl as a separate project [41][42]. This apparatus is capable of discriminating between the incoming polarisation states and is equipped with an efficient beam tracking system to maintain a stable optical link with the sender. A dynamic basis alignment compensates for the variable tilting of the hand-held Alice module and thereby maximises the performance of the BB84 protocol. While the first results are very promising, we discuss the further optimisation of the experimental parameters to achieve higher key generation rates.

7.1. Optical setup of the receiver

The primary role of the receiver is to measure the polarisation qubits sent by Alice in order to retrieve the corresponding bit values. The basic design of this unit has been extensively used in other QKD experiments such as [11][48], but has been extended for this project to enable user-friendly operation via beam steering and live basis alignment, as illustrated in Fig. 7.1. The different functions are exhaustively detailed in [42] and are summarised again below.

7.1.1. Polarisation analysis of the faint laser pulses

As Alice prepares linearly polarised weak coherent pulses, it is necessary that Bob's apparatus is able to detect these states. The qubit measurements will deliver meaningful outcomes only if the quantum channel and the detection optics perfectly preserve the polarisation, and if Alice and Bob share the same reference frame. In practice, several unitary transformations have to be applied to satisfy these conditions.

Reference-frame alignment

In order to minimise the QBER, and therefore maximise the key generation rate, Alice and Bob should share the same definition of a horizontal and vertical polarisation. When the user holds the sender device in his hand, the rotation of the unit around the optical axis is not restricted, such that Alice's reference frame changes for each user but is also likely to be unstable in time if the hand is not perfectly steady. Under real conditions, the micro-optical system should be controlled by a smartphone placed on top of the aluminium box, such that we can take advantage of the accelerometer embedded in the latter to obtain the absolute tilting angle of the whole unit. In the following experiments, the integrated module is connected to a computer, but the phone is used during hand-held operation to test this alignment procedure. A calibration step has to be performed since the emitted laser beam is not exactly parallel to the edges of the device. The resulting angle is a 64-bit word transmitted to Bob over WLAN at about 80 kHz, depending on current traffic. Live

basis alignment is performed by rotating the motorised half-wave plate placed before the Polarisation Analysis Unit (PAU). The communication with the stepper motor limits the update frequency of the wave plate position to 57.5 ms.

Phase compensation

As mentioned in the previous chapters, Alice's states exhibit an elliptical polarisation, which should be rotated back to the equatorial plane of the Poincaré sphere by a phase compensation scheme. The optimal angles of the three wave plates differ from the ones calculated in Table 6.3 since additional polarisation dependence of certain components on Bob's side has to be taken into account. To determine the new optimal values, a partial tomography is performed on Bob's device. The four states generated by Alice are sent and analysed using an additional quarter-wave plate and a polariser placed before the PAU. In this measurement the intensity is recorded by one APD only, and a fixed polariser is positioned before the PAU to remove the effect of the PBS. An optimal phase compensation is obtained for the following orientations of the wave plates:

$$\alpha = 51.6\,^{o} \tag{7.1}$$
$$\beta = 0\,^{o} \tag{7.2}$$
$$\gamma = 160.4\,^{o} \tag{7.3}$$
$$\tag{7.4}$$

Measurement of the polarisation qubits

The PAU discriminates between the qubit states by splitting the incoming pulses into four spatial modes, depending on their polarisation. A first non-polarising beamsplitter (BS) randomly chooses the detection basis. A polarising beamsplitter (PBS) placed in one arm transmits H states and reflects V states, while a $\lambda/2$-wave plate rotated by $22.5\,^{o}$ and followed by a PBS in the transmitted arm allows to discriminate between $\pm 45^{o}$ states. Each path is terminated by an actively quenched fibre-coupled APD (*SPCM-AQ4C*, Perkin Elmer) operated in Geiger mode. The detectors typically feature a detection efficiency at 850 nm of 38 %, a jitter of 400 ps, a dark count rate of 500 Hz and a dead time of 50 ns. The timestamps of the events are recorded by a TDC with 81 ps resolution.

The driving electronics shuts the APDs down when a fast increase of the count rate is observed in order to prevent physical damage. This procedure, although necessary under usual conditions, is dramatic for the hand-held operation, where the detection rate exhibits strong fluctuations due to frequent loss and recovery of the signal. This issue is partially circumvented by placing additional weak neutral density filters reducing the absolute ramp-up of the detection rate. A stronger improvement was brought by a fast tracking system ensuring a better stability of the optical link.

7.1.2. Tracking system

The angular precision required for a stable link was first evaluated in order to develop a beam steering system accordingly.

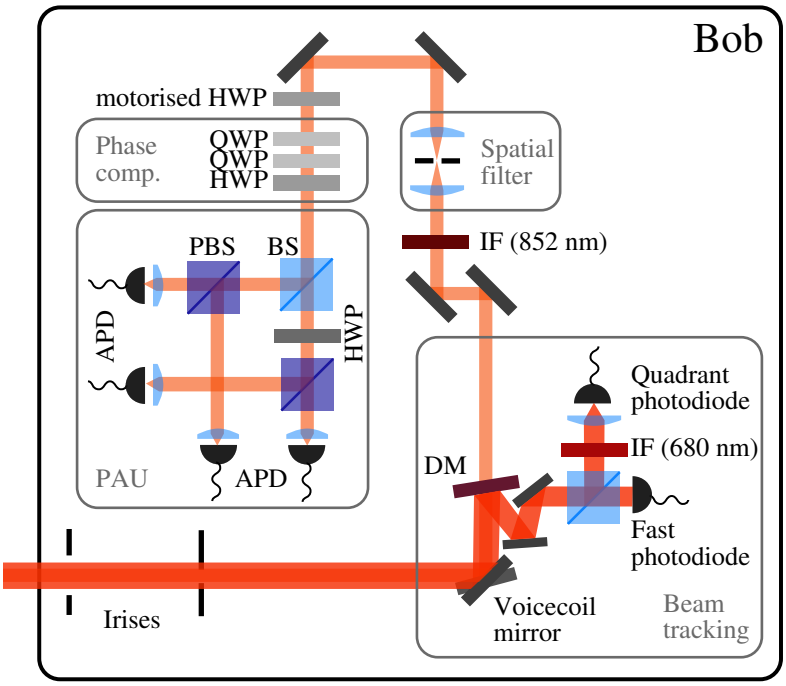


Figure 7.1.: Optical setup of the receiver (Bob) developed in [41, 42]. The polarisation states sent by Alice are analysed as follows. First, a static phase compensation scheme rotates the elliptical polarisation states back to linear states. A motorised half-wave plate controlled over WLAN rotates Bob's reference frame in real time depending on the tilting of the hand-held unit. Finally, a first beamsplitter (BS) performs a random basis choice. A polarising beamsplitter (PBS) placed in one arm allows to discriminate between $|H\rangle$ and $|V\rangle$, while a half-wave plate rotated by 22^o combined with a PBS in the second arm project the qubits onto $|D\rangle$ and $|A\rangle$. The red beacon laser, overlapped with the polarised qubits, is used for clock recovery and efficient beam tracking. Technical abbreviations: DM: Dichroic Mirror; IF: Interference Filter; QWP (HWP): Quarter (Half) Wave Plate; PAU: Polarisation Analysis Unit; APD: Avalanche PhotoDiode.

Acceptance angle of the polarisation analysis setup

The discriminated polarisation modes are coupled via aspheric lenses with $f = 11\,\text{mm}$ into multi-mode fibres that guide the light to the APDs. The core diameter d_c of the fibres, in our case of $62.5\,\mu\text{m}$, restricts the incidence angle α_{in} of the incoming beam to a maximum value defined by

$$\alpha_{in,max} = arctan\left(\frac{d_c}{2f}\right) \tag{7.5}$$

$$= 2.8\,mrad = 0.163^o \tag{7.6}$$

Maintaining the angle within this narrow range for each of the four detectors simultaneously is quite challenging, especially with a hand-held sender unit. The position of

the collection optics is fixed onto an aluminium plate, such that only the orientation of each fibre coupler can be adjusted. The possible misalignment of the couplers in the different arms can result in a slight optical path length difference, creating an imbalance in the coupling efficiencies of the different states into the fibre-coupled detectors. Other free-space systems receivers equipped with several detectors may suffer from this issue, as nothing usually prevents Alice from aiming with angles larger than $\alpha_{in,max}$. However, the influence of α_{in} onto the detection efficiencies was first reported in our recent study [112], and independently by another research group at a later stage [113]. Here a dummy hand-held module emitting circular polarisation states was used as input beam in order to remove the polarisation dependency of the coupling efficiencies. Under certain incidence angle values, the probability for the photon to end in one particular detector strongly increases even within the limited acceptance window, as illustrated in Figure 7.2. Eve can therefore control the incidence angle of the beam and be able to predict with high probability which state Bob will measure. Although this loophole exploits a spatial side-channel, its principle is similar to other attacks based on intrinsic efficiency mismatch induced by blinding some of the detectors [114]. As a countermeasure, a spatial filter was implemented using two $f = 11\,\text{mm}$ aspheric lenses and a pinhole with a diameter of $30\,\mu\text{m}$ placed in the focus of the beam. Consequently, only input beams under oblique incidence with $\alpha_{in} < 1.36\,mrad < \alpha_{in,max}$ are transmitted to the polarisation analysis unit. The efficiency mismatch is considerably reduced for the transmitted angles, and data points corresponding to larger values indicate that the beam is actually blocked.

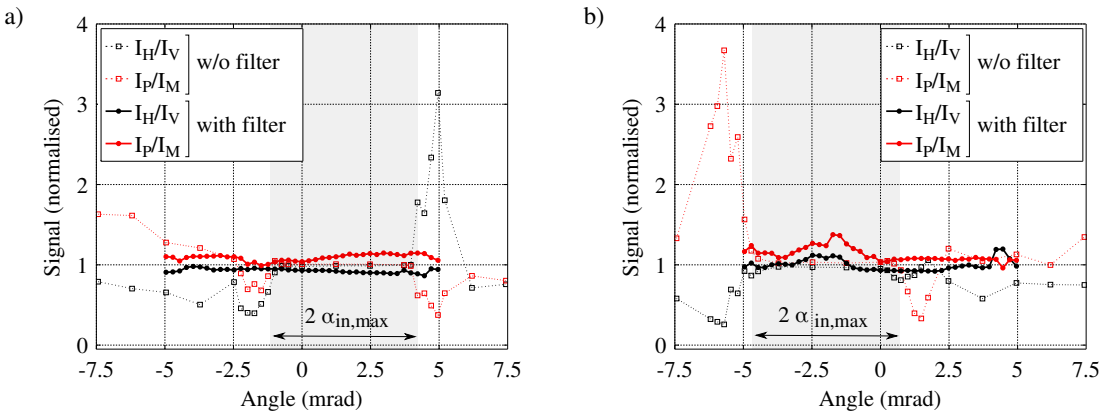


Figure 7.2.: Influence of a (a) vertical and (b) horizontal incidence angle of a circularly polarised laser beam on the coupling into the different fibre-coupled detectors of the receiver. For sake of clarity, only the ratio of intensities is shown for states of the same basis. The implementation of the spatial filter (bold lines) reduces the strong detection mismatch observed in standard polarisation analysis units (dashed lines). Taken from [41].

Beam steering

In order to ensure a stable optical link, the infrared signal emitted by Alice should constantly feature an incidence angle below 0.08^{o} in order to be transmitted through the

spatial filter. As depicted in Fig. 7.1, the adopted solution consists in tracking the incoming beam using a position-dependent detector and a fast moveable mirror. This procedure requires a sufficient beam intensity and therefore applies only to the beacon laser, overlapped with the infrared signal. To restrict the aiming angle, two irises with a diameter of about 1 mm each are placed at the entrance of the Bob module. As the visible beam has a size similar to the pinholes, the user knows that the signal is blocked when he sees the reflection of the red beam around one of the irises and can adapt the direction of the Alice unit accordingly. After these irises the beam impinges onto a moveable mirror at a constant position, and is then directed to a dichroic mirror that transmits the infrared signal and reflects the visible laser [1]. The latter is sent onto a quadrant-photodiode, which retrieves the aiming angle and feeds it back to the electrically driven mirror. The beam direction of the faint laser pulses is therefore constantly adjusted to maintain high coupling efficiencies to the APDs. The mirror operation frequency of 850 Hz is assumed to be faster than the possible shaking of the user's hand holding the sender unit. This tracking mirror can compensate for incoming angles up to 52.4 mrad (3^o) with an angular precision of 1.7 µrad and 1.5 µrad along the horizontal and vertical direction, respectively.

Figure 7.3 shows a typical trace of the light coupled into the fibres of the PAU when the user aims into the receiver using the Alice module. During the development of the receiver, *i.e.*, before the availability of the sender unit, the APDs were replaced by an array of photodiodes, less sensitive to strong intensity variations. The Alice module was emulated by a dummy unit generating an infrared beam of the same size. We define the link efficiency ξ as the ratio of the average detection rates observed for dynamic and static alignments:

$$\xi = \frac{R_{det,\,dynamic}}{R_{det,\,static}} \tag{7.7}$$

The fraction of time during which the beam is successfully tracked can be written as

$$\Gamma_{R_{min}} = \frac{t\,(R > R_{min})}{t_{total}} \tag{7.8}$$

where R_{min} is an appropriate threshold. Experimentally, an average link efficiency up to $\xi = 33\,\%$ could be achieved over almost 30 seconds, with a beam tracked more than 85 % of the time ($R_{min} = R_{max}/10$).

7.1.3. Synchronisation with the sender

The beacon laser provides not only a good visual indicator during the aiming procedure but also allows for efficient beam tracking and perfect synchronisation between Alice and Bob. In order to associate each measurement outcome with the right input qubit, both apparatus need to run at the exact same frequency. Two physically separated clocks would, with high probability, exhibit a small frequency offset and a different drift with time, quickly limiting the amount of exploitable data. Thus Alice's clock is directly transmitted to Bob via the beacon laser, which is modulated at 100 MHz repetition rate and with a duty cycle of 50 %. This signal is detected on the receiver side by an additional fast photodiode (*DET210*, Thorlabs) and transferred to a clock recovery chip based on a Phase-Locked Loop (PLL). The clock can be retrieved with a frequency of 100 kHz.

[1] The angle between the dichroic mirror and the beam was first fixed at 45^o, but was later reduced to a few degrees to limit the impact of the experimentally observed polarisation-dependent transmission at infrared wavelengths, leading to high QBERs.

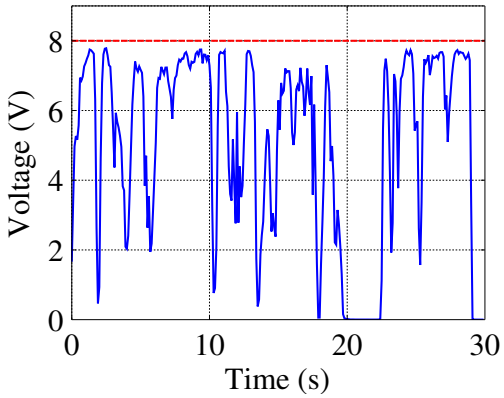


Figure 7.3.: Evolution of the signal detected by the fibre-coupled detectors (here standard photodiodes) when the Alice module is hand-held and the beam tracking system is turned on. The red bar indicates the intensity detected with a static alignment.

Nevertheless, the synchronisation also entails Bob's ability to assign each sent bit to the right detection event. The delay τ between the detection of a start signal (here the sequence *01010111*) sent over the beacon, and the detection of the polarisation state sent simultaneously, should thus be known. This time is constant and only dependent on the electronic and optical path length difference between the signal and beacon pulses. The delay can be determined by sending a constant pattern at red and infrared frequencies, and by shifting the detection times until a minimum QBER is reached.

7.2. Preliminary tests

As the sender and the receiver have been developed separately, a few tests have been performed to optimise the experimental parameters and to check the communication between both parties.

7.2.1. Characterisation of the optical pulses

The temporal overlap of the optical pulses was verified using Bob's module. The electrical pulse parameters determined in Chapter 3 had to be slightly modified to take into account the presence of the closed aluminium box in which the optics and electronics of the Alice module are embedded. Due to the reduced convection effects at the PCB's surface, the delay lines reach a higher temperature, causing a quick shift of the pulses until thermal stabilisation. With two fans placed above and below the PCB, a stable temperature is achieved after 30 seconds (see Fig. 7.4a).

The time-difference histogram reconstructing the optical pulse trace is presented in Fig. 7.4b. The peak probability distribution of the pulses does not feature the exact same amplitude, as the signal-to-noise ratio of each prepared state is dependent on the intensity lost by polarisation selection and on the brightness of the corresponding VCSEL. The length of the pulses appears to be larger than measured in the previous study due to the larger jitter of the APDs embedded in the receiver.

The count rate was measured for each state separately and equalised. For the maximum

intensity of the VCSELs guaranteeing the temporal overlap of the pulses, a mean photon number $\mu_{Alice} = 0.49$ was calculated. This value is much higher than predicted in previous characterisations, and we assume that an inefficient coupling onto the single APD with an active area of 30 µm led to this underestimation. The computation of μ was based on Eq. 3.3 with an additional correction factor c taking into account the saturation of the detectors at high count rates [115]. Assuming a Poissonian distribution, an observed detection rate R_{det} corresponds to a mean photon number

$$\mu = -\frac{1}{t_{link}} ln\left(1 - \frac{c \cdot R_{det} - R_{dark}}{R_{rep} \cdot \eta}\right) \tag{7.9}$$

with $c = 1/(1 - \tau_d \cdot R_{det})$ and t_{link} the overall transmission through the quantum channel and the receiver. According to the specifications, the dead time τ_d is larger than 50 ns, and the factor c is typically in the order of 1.01 to 1.12 for count rates ranging from 200 kHz to 1.5 MHz per detector.

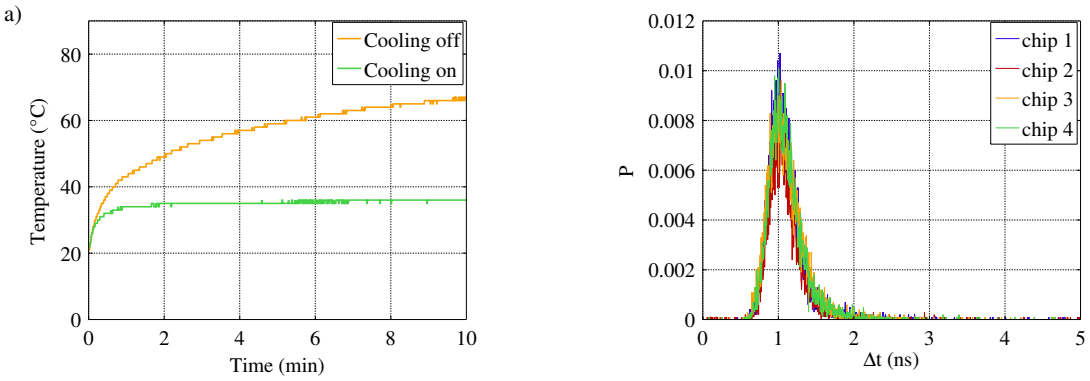


Figure 7.4.: Adjustment of the electrical pulse parameters on Alice's side. a) Evolution of the temperature of the delay lines controlling the phase of the generated pulses when Alice's aluminium box is closed. A thermal instability leads to a temporal shift of the pulses. b) Temporal distribution density of the resulting faint laser pulses as measured on Bob's side and showing a perfect overlap.

7.2.2. Evaluation of the dark count rate

The precise measurement of the dark count rate is necessary to accurately determine the key generation rate. To limit the parasitic rate due to background light, the polarisation analysis unit as well as the spatial filter are hermetically sealed within a black box with the interference filter placed on the beam aperture. In this configuration, a mean overall dark count rate $R_{dark} = 1.42 \pm 0.13$ kHz is observed. The influence of this imperfection will be further reduced in the experiment by processing only events occurring within a certain time window.

The beacon laser alone, even with an injection current just above the threshold, led to an overall rate of 4 MHz (see Fig. 7.5b), despite the embedded interference filter (850 ± 5 nm). This rate indicates either fluorescence from an optical component or, more probably, a side-band from the beacon at infrared wavelengths. Due to its low intensity, this side-band could not be identified with a standard fibre-coupled spectrometer (Ocean Optics), but

could be resolved with a CCD-based (*iDus series 401*, Andor) single-photon spectrometer with 1 nm spectral resolution (Fig. 7.5d). A long-pass filter with cut-off wavelength at 780 nm and $T > 99\,\%$ was used in the measurement to filter out the bright 682 nm peak visible in Fig. 7.5c and avoid saturation of the camera.

The intensity of this side-band could be decreased by several orders of magnitude by placing a customised short-pass filter from BK Interferenzoptik GmbH with transmission of $T = 50\,\%$ at 680 nm on Alice's side, between the chip carrier and the miniature beam-splitter. Even at high intensities around 800 µW, the beacon laser is responsible for an additional count rate of only 2.2 kHz. This contribution can be further reduced by adjusting the bias current such that the red light is only sufficiently visible for the aiming procedure (typically below 500 µW)

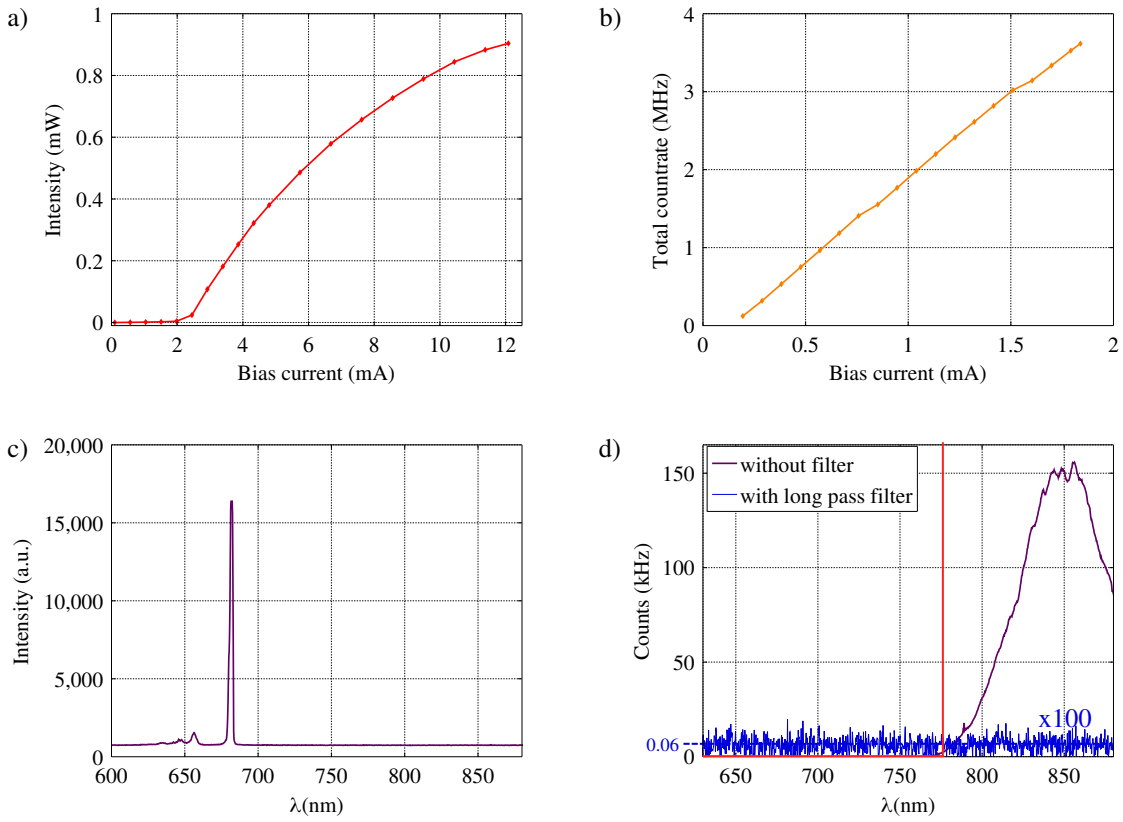


Figure 7.5.: Emission properties of the red beacon laser. (a) Intensity of the visible beam at the output of the Alice module as a function of the bias current. (b) Total detection rate measured by the receiver despite a dichroic mirror and an interference filter at $\lambda = 850 \pm 5$ nm. (c) Spectrum measured with a classical spectrometer and (d) with single-photon detector and a long-pass filter with $\lambda_c = 780$ nm indicated by a red line. The beacon VCSEL exhibits a side band around 850 nm (purple curve), responsible for the high background rates detected on the receiver's side. The intensity can be reduced by more than 3 orders of magnitudes by placing an additional long-pass filter in front of the chip carrier (blue curve).

7.2.3. Test of the dynamic alignment systems

The receiver includes two separately developed alignment systems, the first one adjusting the direction of the beam, and the other compensating the rotation of the beam around its own axis. A first test measurement was therefore performed to verify the simultaneous operation of both functions. The Alice unit was held manually at roughly 30 cm of the entrance pinholes of the receiver. The three-state protocol introduced at the end of Chapter 6 was implemented, as the existence of a better phase compensation for the 4-state protocol had not been discovered yet.

Figure 7.6 shows the excellent stability of the optical link and of the resulting QBER over several seconds. The peak detection rate reaches 2.5 MHz, *i.e.*, more than 60 % of the rate achieved with a static alignment, with an average link efficiency of $\xi = 38\,\%$. The beam is successfully tracked $\Gamma_{R_{det,max}/10} = 74\,\%$ of the time. The large average value of the QBER, not taking into account the peak values obtained when the signal is lost, is related to several issues. First, a large detection window of 1.3 ns was used in the post-processing step, thereby reducing the signal-to-noise ratio. In our scheme, the noise is mainly related to the background emission of the three VCSELs that are not currently emitting a pulse. Second, a careful analysis of Bob's setup showed that several mirrors as well as the dichroic mirror separating the red and infrared signal exhibited a strong polarisation dependence of the reflection. The replacement of the mirrors and the rotation of the dichroic filter such that it forms an angle of a few degrees with the infrared beam led to a reduction of the overall QBER down to 2.9 %.

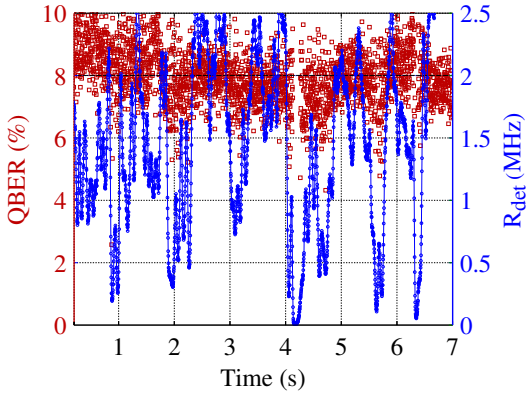


Figure 7.6.: First QKD test based on the three-state protocol showing an excellent simultaneous operation of the beam tracking system and of the live-basis alignment procedure. The large values of the QBER were reduced down to 2.9 % after the replacement of the mirrors on Bob's side.

7.3. Experimental quantum key distribution

Finally, quantum key distribution experiments based on the BB84 protocol have been performed under laboratory conditions. Calculations predict similar secure key rates for the BB84 and three-state protocols, but we opted for the former solution as the corresponding theory is more complete and includes for instance the effects of finite sampling and state preparation imperfections. In the following measurements, the sender and the

receiver were both connected to a computer, and a fixed pattern $\{H, D, A, V\}$ was used for the sequence of the faint laser pulses. The recorded data were analysed *a posteriori* and the asymptotic secret key rate was evaluated using Eq. 2.12, assuming a imperfect error correction characterised by $f = 1.22$. In view of a more realistic implementation, an experiment was also performed using random numbers loaded from an external generator [116] into the FPGA of the sender unit. As the size of the embedded memory is limited, 131,056 different numbers were stored and repeated periodically. The corresponding results are detailed in [42] and are therefore not repeated here, as the obtained performances equal those measured for a fixed pattern.

7.3.1. Static alignment of the sender unit

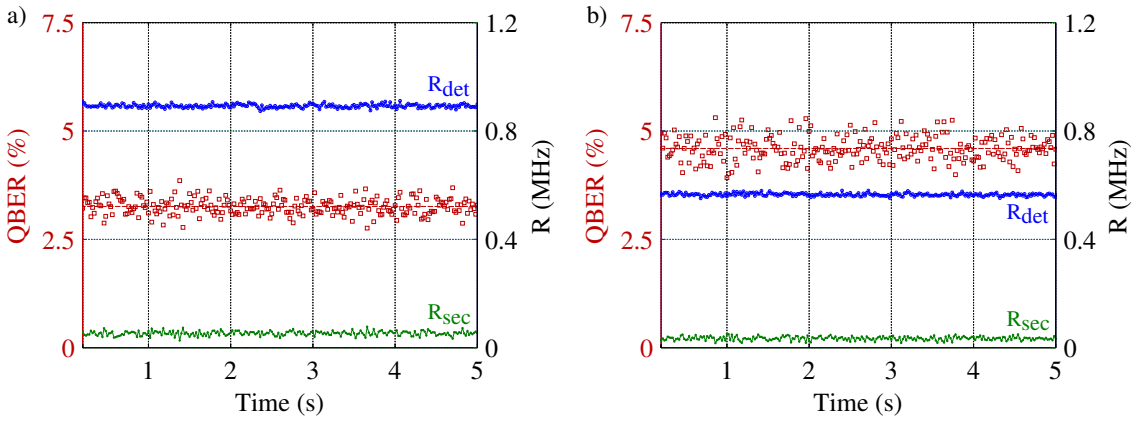
Initially, the Alice unit is fixed in front of the receiver. The QKD experiment allows to evaluate the intrinsic quality of the sender, while the efficiency of the module in a hand-held scenario will be described in the following section. The experiment was repeated for different mean photon numbers, which due to time constraints were controlled by additional ND filters on Alice's side. As shown in Fig. 7.7, the imperfections of some filters led to an increase of the QBER, however this effect should not occur when monitoring μ with the injection current of the VCSELs. A minimum QBER of 3.3 % was observed, in perfect agreement with the simulations obtained for an optimal phase compensation (see Table 6.3). These results show that both the quantum channel and the receiver perform only unitary transformations. The overall transmission is estimated at $t_{link} = 24\,\%$, mostly limited by the entrance irises and the spectral filters.

A secure key rate of 54 kHz is achieved for an optimal mean photon number $\mu = 0.09$, corresponding to a tenfold improvement compared to two other miniaturised sender units with much larger footprints [43, 44]. In this proof-of-concept experiment, the decoy protocol required to ensure the security of a generation process involving fake laser pulses was not implemented, although we demonstrated in Section 3.3.3 that Alice's hardware could support this additional function in the future. To take into account possible PNS attacks, the number of multi-photon pulses has therefore to be minimised. Here a low mean photon number was used, resulting in a low detection rate. An upgrade to the decoy protocol would allow values of μ close to 0.5, and is expected to improve the secure key rate by a factor 5.

For sake of completeness, we also performed long-test measurements. These results might not be relevant for a real hand-held scenario, but are of interests in long-distance experiments where the miniature Alice unit is plugged into a telescope. The QBER is very stable over 45 minutes with a standard deviation $\sigma_{QBER} < 0.1\,\%$. The continuous raw key rate's increase of 8 % might be explained by the slow increase of the coupling efficiency related to the movement of the micro-optical bench within the aluminium box.

7.3.2. Dynamic alignment of a hand-held Alice module

In this section, realistic operations conditions were simulated. The sender unit is held manually at an operating distance of about 30 cm, and aimed at the two entrance pinholes of the receiver. The smartphone placed on top of the device records its orientation and communicates with Bob's computer over WLAN. Both dynamic alignment systems should compensate simultaneously for the small lateral displacements and rotations of the sender



c)

Test	(not shown)	a)	b)
Mean photon number μ	0.19	**0.09**	0.06
QBER δ	5.1 %	**3.3 %**	4.6 %
Detection rate R_{det}	1,740 kHz	**893 kHz**	565 kHz
Sifted key rate R_{sift}	731 kHz	**445 kHz**	278 kHz
Secret key rate R_{sec}	0	**54 kHz**	35 kHz

Figure 7.7.: Quantum key distribution experiment based on the BB84 protocol and performed with the sender unit fixed in front of the receiver. The different mean photon numbers were simulated by additional ND filters. The calculation of the asymptotic secret key rate used a detection window of 740 ps, and correction factors for the raw key rate and the error correction by a factor $c = 1.02$ and $f = 1.22$, respectively.

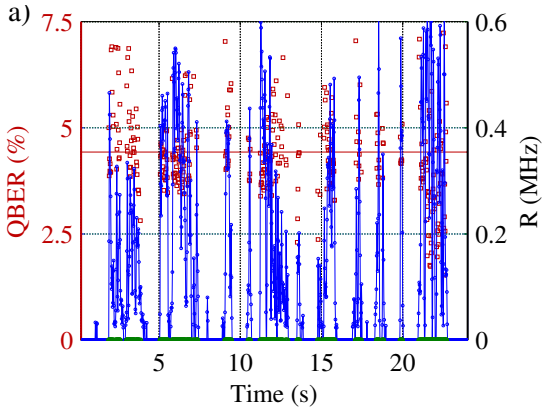
due to a wobbly hand. As the transmission loss is expected to be higher than in the static case, a lower mean photon number $\mu = 0.06$ was used.

The achieved key rate and the corresponding QBER is presented in Fig. 7.8 for the best trial. The average detection rate is quite low, and the fraction of the time where successful tracking is observed is reduced by an order of magnitude compared to the first tests (see Fig. 7.6). It seems that a problem occurred with the beam tracking, and new experiments would have to be performed to verify this hypothesis. The reference frame was updated only each second due to a slow WLAN connection, thereby leading to higher QBERs. In this scenario, the average QBER was evaluated slightly differently than for static alignment, to take into account the problems arising from the loss of the signal. When the infrared beam is not detected, the QBER is defined by the dark count rates, which is a random process for all detectors, and therefore reaches 50 %. Thus only the time intervals where the signal-to-noise ratio exceeds an arbitrary amount, typically 1:100, were taken into account. Additionally, the bursts featuring a QBER exceeding 11 % were discarded as no secure bit can be extracted.

Among the different trials, the highest asymptotic secret key rate was evaluated at 31 Hz with an average QBER of 4.1 %. This value could be further improved by optimising the

mean photon number, and by solving the aforementioned technical issues [42]. For real-life implementations, finite-key effects should also be considered.

a)



b)

Average transmission t_{link}	**4.7 %**
Link efficiency ξ	**19 %**
Tracking time $\Gamma_{R_{max}/5}$	**8.3 %**
QBER δ	**4.1 %**
Average detection rate R_{det}	**79.7 kHz**
Average secret key rate R_{sec}	**31 Hz**

Figure 7.8.: First quantum Key distribution experiments performed with a hand-held sender unit. The calculation of R_{sec} is based on the following parameters: $\mu = 0.06$, $c = 1.01$ and $f = 1.22$.

In this proof-of-principle experiment, Alice's and Bob's data were stored on a computer and processed at a later stage. The communication speed between the sender and the receiver, as well as the performance of the smartphone for error correction and privacy amplification, were not taken into account into the calculation of the key generation rate. As a first step, we conducted a separated study to evaluate the time needed by a *Nexus 5* [1] running on Android 4.4.2 ("Kit Kat") to perform these operations [117]. Simulations delivered a WLAN transfer rate of 42.4 Mbs could be achieved with an Android App based on the Kryonet TCP-IP library from EsotericSoftware. For a number of 10^7 sifted bits and a maximum QBER of 11 %, the error correction based on the Winnow protocol is performed within 50 ms. Privacy amplification based on Töplitz matrices requires less than 3 seconds, thereby using 121 MB of RAM. Given the experimental detection rates observed in Fig. 7.8, for which the mean photon number is not optimal, the exchange of 10^7 sifted bits would take 25 seconds, while the post-processing (excluding the authentication process, which was not simulated) would be performed within less 3 seconds for this error rate.

[1] The hardware of the *Nexus 5* includes a quad-core processor running at 4×2.3 GHz; 1×4 kB of L0 Cache, 2×16 kB of L1 Cache, and 2 MB of L2 Cache; 2 GB of RAM, although only 512 MB are available for each program; a WLAN router specified under the norm 802.11n, designed for 600 Mbs data rates.

8. Conclusion and outlook

This work demonstrated the first secure key exchange based on the BB84 protocol between a hand-held platform and a free-space receiver. The user is assisted during the aiming procedure by a beam tracking system placed in the receiver and guaranteeing a stable optical link. A separate live-basis alignment also compensates for the manual tilt of the sender unit. This dynamic alignment configuration leads to an average QBER of 4.1 % and an asymptotic secure key rate of 31 Hz. The user-friendliness of the system is further increased by small dimensions of the transmitter ($35 \times 20 \times 8\,\mathrm{mm}^3$) and its compatibility with current smartphone technology. Additionally, the driving electronics of this QKD add-on, here integrated onto a single printed circuit board, includes only off-the-shelf components and could thus be easily integrated monolithically into the hardware of a multitude of host devices.

The novel architecture of the miniature QKD sender add-on developed in this thesis proved to be suitable for the preparation of the four polarised weak coherent states required by the BB84 protocol. The 40 ps long optical pulses are generated at 100 MHz repetition rate by an array of four VCSELs emitting around 850 nm. Under large signal modulation, the pulses appear *unpolarised* such that the polarisation of each diode can be controlled by an external wire-grid polariser. We introduced a geometrical model taking into account fabrication imperfections in the FDTD simulations performed to optimise the grating parameters of these structures. An excellent agreement between calculations and experiments was achieved for the first time, with measured extinction ratios up to 1,800, establishing a new record for 850 nm. The resulting polarised faint laser pulses are finally combined into one spatial mode using a glass waveguide chip manufactured by femtosecond laser writing. A red beacon laser overlapped with the infrared signal allows for efficient beam tracking and provides a useful visual indicator during the aiming procedure. The complete module emits polarised weak coherent states with a maximum mean photon number $\mu = 0.49$, and an intrinsic QBER of 3.3 %, mainly due to a low quality characterisation of the polarisation effects in the waveguides and due to imperfections in the orientation of the polarisers preparing the input states. Higher quality of the state preparation could be achieved in the next prototype by solving these practical issues. Moreover, the size of the optical module could be further reduced to fit in the restricted volume offered by most host systems. For instance, more suitable assembly techniques would allow to shrink the module by reducing the size of each optical component to the minimum area or by allowing the spatial overlap of the beacon laser with the signal states within the waveguide chip.

In this proof-of-concept experiment, we used a mean photon number of $\mu = 0.09$ as a trade-off between a fast key generation process and a low fraction of multi-photon pulses, yielding a secret key rate of 54 kHz under static alignment. In order to rule out the possible photon-number-splitting attack, the decoy protocol should be implemented. This solution would simultaneously enable to work with higher values of μ, thus allowing a significant increase of the achievable key rates. Here the slow communication with the laser driver prevents changing the intensity of each pulse, but decoy states could in principle

be generated by turning two diodes on at the same time. The downside of this method is that the resulting faint laser pulses do not exhibit a defined polarisation and thus cannot contribute to the final key. Also, a precise characterisation of the photon statistics should be conducted. The theory of the decoy protocol relies on a Poissonian distribution of the photons, while first tests have demonstrated a more complicated statistics of the short pulses, depending on the pulse parameters and on the selected polarisation. The implication of a thermal behaviour onto the security of the protocol should thus be studied carefully.

Further security aspects such as finite-key effects have not be taken into account in this work but definitely need to be considered in the next steps. The impact of short key length onto the key generation rate is not trivial for practical implementations where the intensity exhibits strong fluctuations. A more efficient beam tracking system might improve the key rate by reducing the intensity variations and therefore the associated key shrinkage due to finite-key effects while simultaneously allowing for a higher transmission. Moreover, the side-channel resulting from the small spectral mismatch between the laser sources could in principle be exploited by a third party and should thus be addressed. One convenient solution would consist in replacing the traditional VCSELs with their tunable (MEMS) counterparts.

While this work paves the way towards secure short-distance communication, it also opens new possibilities towards secure long-distance links. The miniature sender unit could be embedded as a QKD add-on in virtually all existing free-space systems involving either statically or dynamically aligned platforms. Such applications would not only include hand-held devices but also metropolitan optical networks and downlinks from satellites or aircrafts.

A. Printed Circuit Board layouts

A.1. Driving Electronics

Figure A.1.: (Not available in the online version)

A.2. VCSEL board

Figure A.2.: (Not available in the online version)

B. Tomographic measurement data

B.0.1. Tomography of the waveguide chip

Input state	Projection state					
	$\|H\rangle$	$\|V\rangle$	$\|R\rangle$	$\|L\rangle$	$\|A\rangle$	$\|D\rangle$
Waveguide 1						
$\|H\rangle$	23.18	0.024	11.81	11.36	10.95	13.13
$\|V\rangle$	0.010	22.09	11.15	10.72	11.27	10.66
$\|R\rangle$	11.59	10.57	1.33	20.72	16.27	5.71
$\|L\rangle$	11.62	11.50	21.63	1.37	5.91	17.08
$\|A\rangle$	11.05	11.71	6.34	16.25	1.26	21.41
$\|D\rangle$	12.23	10.33	16.5	5.98	20.88	1.50
Waveguide 2						
$\|H\rangle$	39.02	0.391	22.56	16.90	22.24	17.02
$\|V\rangle$	0.50	39.53	17.14	22.53	23.3	16.43
$\|R\rangle$	23.83	18.80	4.88	37.64	34.68	7.66
$\|L\rangle$	15.68	20.89	34.72	1.72	10.7	25.77
$\|A\rangle$	17.99	16.41	7.29	26.98	3.35	30.94
$\|D\rangle$	21.54	23.08	31.99	12.45	41.8	2.53
Waveguide 3						
$\|H\rangle$	46.22	1.18	16.34	31.12	23.22	23.95
$\|V\rangle$	0.77	45.01	28.41	16.95	23.08	22.43
$\|R\rangle$	18.60	29.28	3.30	44.48	34.75	12.69
$\|L\rangle$	28.53	16.73	41.36	3.67	11.51	33.73
$\|A\rangle$	20.21	27.24	12.82	34.38	3.06	44.3
$\|D\rangle$	27.05	18.89	31.65	14.07	43.06	2.41

(Continued on next page)

(Continued from previous page)

Input state	Projection state					
	$\|H\rangle$	$\|V\rangle$	$\|R\rangle$	$\|L\rangle$	$\|A\rangle$	$\|D\rangle$
Waveguide 4						
$\|H\rangle$	0.72	53.73	32.27	22.44	23.18	31.31
$\|V\rangle$	53.26	0.61	23.19	30.24	22.21	31.56
$\|R\rangle$	28.81	21.73	48.51	2.28	35.03	15.14
$\|L\rangle$	24.90	32.67	6.90	50.31	10.19	47.74
$\|A\rangle$	33.26	28.97	45.36	16.96	3.63	59.00
$\|D\rangle$	20.61	25.73	10.52	35.60	41.56	4.32

Table B.2.: Raw data obtained from the waveguide chip tomography. The intensity is given in microwatts and was measured with a powermeter.

B.0.2. Tomography of the states prepared by the Alice module

Channel	Input state	Projection state					
		$\|H\rangle$	$\|V\rangle$	$\|R\rangle$	$\|L\rangle$	$\|A\rangle$	$\|D\rangle$
1	$\|V\rangle$	5,181	73,781	25,159	53,410	47,660	30,098
2	$\|P\rangle$	78,372	116,974	15,263	177,184	141,829	52,146
3	$\|M\rangle$	14,396	40,012	46,563	8,611	13,354	41,141
4	$\|H\rangle$	156,990	6,624	98,958	69,460	60,285	106,826

Table B.3.: Tomography of the output states of the assembled Alice module performed with an APD.

List of abbreviations

APD Avalanche PhotoDiode

CCD Charge-Coupled Device

CML Current Mode Logic

DBR Distributed Bragg Grating

DFB Distributed FeedBack (laser)

DOP Degree Of Polarisation

DUT Device Under Test

EBL Electron Beam Lithography

ECL Emitter-Coupled Logic

EEL Edge-Emitting Laser

EOT Extraordinary Optical Transmission

FCA Free Carrier Absorption

FDTD Finite-Difference Time-Domain

FTIR Fourier Transform InfraRed (spectrometer)

FIB Focused Ion Beam

FPGA Field Programmable Gate Array

HCG High-Contrast Grating

HWP Half-Wave Plate

IF Interference Filter

LED Light Emitting Diode

MLA Micro-Lens Array

MM Multi-Mode

MOB Micro-Optical Bench

NDF Neutral Density Filter

NIR Near InfraRed

PC	Phase Compensation
PCB	Printed Circuit Board
PIC	Photonic Integrated Circuit
QBER	Quantum Bit Error Ratio
QKD	Quantum Key Distribution
QW	Quantum Well
QWP	Quarter-Wave Plate
RS	Single-Mode VCSEL array from Raycan
SHB	Spatial Hole Burning
SM	Single-Mode
SPP	Surface Plasmon Polariton
TDC	Time-to-Digital Converter
TDH	Time-Difference Histogram
TE	Transverse Electric
TM	Transverse Magnetic
TSP	Three-State Protocol
TTL	Transistor-Transistor Logic
VCSEL	Vertical-Cavity Surface-Emitting Laser
VM	Multi-Mode VCSEL array from VI-Systems
VS	Single-Mode VCSEL array from VI-Systems
WCP	Weak Coherent Pulse
WGP	Wire-Grid Polariser
WLAN	Wireless Local Area Network

Bibliography

[1] Rivest, R. L., Shamir, A., and Adleman, L., "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM* **21**(2), 120–126 (1978).

[2] Shor, P., "Algorithms for quantum computation: discrete logarithms and factoring," *Proceedings 35th Annual Symposium on Foundations of Computer Science* , 124–134 (1994).

[3] Martín-López, E., Laing, A., Lawson, T., Alvarez, R., Zhou, X.-Q., and O'Brien, J. L., "Experimental realization of Shor's quantum factoring algorithm using qubit recycling," *Nature Photonics* **6**(11), 773–776 (2012).

[4] Bennett, C. H. and Brassard, G., "Quantum cryptography: Public key distribution and coin tossing," *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* , 175–179 (1984).

[5] Lo, H. and Chau, H., "Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances," *Science* **283**(5410), 2050–2056 (1999).

[6] Mayers, D., "Unconditional security in quantum cryptography," *Journal of the ACM* **48**(3), 351–406 (2001).

[7] Stucki, D., Legré, M., Buntschu, F., Clausen, B., Felber, N., Gisin, N., Henzen, L., Junod, P., Litzistorf, G., Monbaron, P., Monat, L., Page, J.-B., Perroud, D., Ribordy, G., Rochas, A., Robyr, S., Tavares, J., Thew, R., Trinkler, P., Ventura, S., Voirol, R., Walenta, N., and Zbinden, H., "Long-term performance of the Swiss Quantum quantum key distribution network in a field environment," *New Journal of Physics* **13**, 123001 (2011).

[8] Wang, S., Chen, W., Yin, Z.-Q., Li, H.-W., He, D.-Y., Li, Y.-H., Zhou, Z., Song, X.-T., Li, F.-Y., Wang, D., Chen, H., Han, Y.-G., Huang, J.-Z., Guo, J.-F., Hao, P.-L., Li, M., Zhang, C.-M., Liu, D., Liang, W.-Y., Miao, C.-H., Wu, P., Guo, G.-C., and Han, Z.-F., "Field and long-term demonstration of a wide area quantum key distribution network," *Optics Express* **22**(18), 21739 (2014).

[9] Sasaki, M., Fujiwara, M., Ishizuka, H., Klaus, W., Wakui, K., Takeoka, M., Miki, S., Yamashita, T., Wang, Z., Tanaka, A., Yoshino, K., Nambu, Y., Takahashi, S., Tajima, A., Tomita, A., Domeki, T., Hasegawa, T., Sakai, Y., Kobayashi, H., Asai, T., Shimizu, K., Tokura, T., Tsurumaru, T., Matsui, M., Honjo, T., Tamaki, K., Takesue, H., Tokura, Y., Dynes, J. F., Dixon, A. R., Sharpe, A. W., Yuan, Z. L., Shields, A. J., Uchikoga, S., Legré, M., Robyr, S., Trinkler, P., Monat, L., Page, J.-B., Ribordy, G., Poppe, A., Allacher, A., Maurhart, O., Länger, T., Peev, M., and Zeilinger, A., "Field test of quantum key distribution in the Tokyo QKD Network.," *Optics express* **19**(11), 10387–10409 (2011).

[10] Fröhlich, B., Dynes, J. F., Lucamarini, M., Sharpe, A. W., Tam, S. W.-b., Yuan, Z., and Shields, A. J., "Quantum secured gigabit optical access networks," *Scientific Reports* **5**, 18121 (2015).

[11] Nauerth, S., Moll, F., Rau, M., Fuchs, C., Horwath, J., Frick, S., and Weinfurter, H., "Air-to-ground quantum communication," *Nature Photonics* **7**(5), 382–386 (2013).

[12] Vallone, G., Bacco, D., Dequal, D., Gaiarin, S., Luceri, V., Bianco, G., and Villoresi, P., "Experimental Satellite Quantum Communications," *Physical Review Letters* **115**, 040502 (2015).

[13] Wiesner, S., "Conjugate coding," *ACM SIGACT News* **15**(1), 78–88 (1983).

[14] Cerf, N. J., Bourennane, M., Karlsson, A., and Gisin, N., "Security of Quantum Key Distribution Using d-Level Systems," *Physical Review Letters* **88**(12), 127902 (2002).

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

[16] Brassard, G. and Salvail, L., "Secret-key reconciliation by public discussion," *Advances in Cryptology EUROCRYPT'93* , 410–423 (1994).

[17] Buttler, W. T., Lamoreaux, S. K., Torgerson, J. R., Nickel, G. H., Donahue, C. H., and Peterson, C. G., "Fast, efficient error reconciliation for quantum cryptography," *Physical Review A* **67**(5), 52303–52308 (2003).

[18] Shannon, C. E., "A mathematical theory of communication," *The Bell System Technical Journal* **27**, 379–423 (1948).

[19] Krawceyk, H., "LFSR-based Hashing and Authentication," *Advances in Cryptology CRYPTO 94* **10598**, 129–139 (1994).

[20] Tomamichel, M., Lim, C. C. W., Gisin, N., and Renner, R., "Tight finite-key analysis for quantum cryptography.," *Nature communications* **3**(may 2011), 634 (2012).

[21] Lucamarini, M., Patel, K. A., Dynes, J. F., Sharpe, A. W., Yuan, Z. L., Penty, R. V., and Shields, A. J., "Efficient decoy-state quantum key distribution with quantified security," *Optics Express* **21**(21), 24550–24565 (2013).

[22] Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H., "Quantum cryptography," *Reviews of Modern Physics* **74**(1), 145–195 (2002).

[23] Lo, H.-K., Chau, H. F., and Ardehali, M., "Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security," *Journal of Cryptology* **18**(2), 133–165 (2004).

[24] Dynes, J. F., Choi, I., Sharpe, A. W., Dixon, A. R., Yuan, Z. L., Fujiwara, M., Sasaki, M., and Shields, A. J., "Stability of high bit rate quantum key distribution on installed fiber," *Optics Express* **20**(15), 16339 (2012).

[25] Lo, H.-K., Curty, M., and Tamaki, K., "Secure quantum key distribution," *Nature Photonics* **8**(8), 595–604 (2014).

[26] Gottesman, D., Lo, H.-K., Lütkenhaus, N., and Preskill, J., "Security of quantum key distribution with imperfect devices," *Quantum Information and Computation* **4**(5), 325–360 (2004).

[27] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., and Peev, M., "The security of practical quantum key distribution," *Reviews of Modern Physics* **81**(3), 1301–1350 (2009).

[28] Dušek, M., Haderka, O., and Hendrych, M., "Generalized beam-splitting attack in quantum cryptography with dim coherent states," *Optics Communications* **169**(1-6), 103–108 (1999).

[29] Brassard, G., Lutkenhaus, N., Mor, T., and Sanders, B., "Limitations on practical quantum cryptography," *Physical review letters* **85**(6), 1330–3 (2000).

[30] Scarani, V., Acín, A., Ribordy, G., and Gisin, N., "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations," *Physical Review Letters* **92**(5), 1–4 (2004).

[31] Hwang, W.-Y., "Quantum Key Distribution with High Loss: Toward Global Secure Communication," *Physical Review Letters* **91**(5), 1–4 (2003).

[32] Lo, H.-K., Ma, X., and Chen, K., "Decoy State Quantum Key Distribution," *Physical Review Letters* **94**(23), 15–18 (2005).

[33] Gisin, N., Fasel, S., Kraus, B., Zbinden, H., and Ribordy, G., "Trojan-horse attacks on quantum-key-distribution systems," *Physical Review A* **73**(2), 1–6 (2006).

[34] Lucamarini, M., Choi, I., Ward, M. B., Dynes, J. F., Yuan, Z. L., and Shields, A. J., "Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution," *Physical Review X* **5**(3), 031030 (2015).

[35] Makarov, V., Anisimov, A., and Skaar, J., "Effects of detector efficiency mismatch on security of quantum cryptosystems," *Physical Review A* **74**(2), 1–11 (2006).

[36] Weier, H., *European Quantum Key Distribution Network*, PhD thesis, Ludwig-Maximilians-Universität (2011).

[37] Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J., and Makarov, V., "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nature Photonics* **4**(10), 686–689 (2010).

[38] Lo, H.-K., Curty, M., and Qi, B., "Measurement-Device-Independent Quantum Key Distribution," *Physical Review Letters* **108**(13), 130503 (2012).

[39] Pirandola, S., Ottaviani, C., Spedalieri, G., Weedbrook, C., Braunstein, S. L., Lloyd, S., Gehring, T., Jacobsen, C. S., and Andersen, U. L., "High-rate measurement-device-independent quantum cryptography," *Nature Photonics* **9**(6), 397–402 (2015).

[40] Bond, M., Choudary, O., Murdoch, S. J., Skorobogatov, S., and Anderson, R., "Chip and Skim: Cloning EMV Cards with the Pre-play Attack," *Security and Privacy (SP), 2014 IEEE Symposium on* , 49–64 (2014).

[41] Vogl, T., *Security of a free space QKD-receiver module with angle-dependent detection efficiency mismatch*, Bachelor's thesis, LMU München (2014).

[42] Vogl, T., *Mobile Free Space Quantum Key Distribution for short distance secure communication*, Master's thesis, LMU München (2016).

[43] Duligall, J. L., Godfrey, M. S., Harrison, K. A., Munro, W. J., and Rarity, J. G., "Low cost and compact quantum key distribution," *New Journal of Physics* **8**(10), 249–249 (2006).

[44] Benton, D., Gorman, P., Tapster, P., and Taylor, D., "A compact free space quantum key distribution system capable of daylight operation," *Optics Communications* **283**(11), 2465–2471 (2010).

[45] Jofre, M., Gardelein, A., Anzolin, G., Amaya, W., Capmany, J., Ursin, R., Peñate, L., Lopez, D., San Juan, J. L., Carrasco, J. A., Garcia, F., Torcal-Milla, F. J., Sanchez-Brea, L. M., Bernabeu, E., Perdigues, J. M., Jennewein, T., Torres, J. P., Mitchell, M. W., and Pruneri, V., "Fast optical source for quantum key distribution based on semiconductor optical amplifiers," *Optics express* **19**(5), 3825–3834 (2011).

[46] Hughes, R. J., Nordholt, J. E., McCabe, K. P., Newell, R. T., Peterson, C. G., and Somma, R. D., "Network-Centric Quantum Communications with Application to Critical Infrastructure Protection," *arXiv/quant-ph:* **1305.0305** (2013).

[47] Sibson, P., Erven, C., Godfrey, M., Miki, S., Yamashita, T., Fujiwara, M., Sasaki, M., Terai, H., Tanner, M. G., Natarajan, C. M., Hadfield, R. H., O'Brien, J. L., and Thompson, M. G., "Chip-based Quantum Key Distribution," *arXiv/quant-ph:* **1509.00768** (2015).

[48] Schmitt-Manderbach, T., Weier, H., Fürst, M., Ursin, R., Tiefenbacher, F., Scheidl, T., Perdigues, J., Sodnik, Z., Kurtsiefer, C., Rarity, J. G., Zeilinger, A., and Weinfurter, H., "Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km," *Physical Review Letters* **98**(1), 010504 (2007).

[49] Westbergh, P., Gustavsson, J., Kogel, B., Haglund, A., Larsson, A., Mutig, A., Nadtochiy, A., Bimberg, D., and Joel, A., "40 Gbit/s error-free operation of oxide-confined 850 nm VCSEL," *Electronics Letters* **46**(14), 1014 (2010).

[50] Larsson, A., Geen, M., Gustavsson, J., Haglund, E., Joel, A., Westbergh, P., and Haglund, E., "30 GHz bandwidth 850 nm VCSEL with sub-100 fJ/bit energy dissipation at 2550 Gbit/s," *Electronics Letters* **51**(14), 1096–1098 (2015).

[51] Guillaumée, M., Dunbar, L. A., Santschi, C., Grenet, E., Eckert, R., Martin, O. J. F., and Stanley, R. P., "Polarization sensitive silicon photodiodes using nanostructured metallic grids," *Applied Physics Letters* **94**(19), 193503 (2009).

[52] Tamada, H., Doumuki, T., Yamaguchi, T., and Matsumoto, S., "Al wire-grid polarizer using the s-polarization resonance effect at the 0.8-microm-wavelength band.," *Optics Letters* **22**(6), 419–421 (1997).

[53] Matthews, J. C. F., Politi, A., Stefanov, A., and O'Brien, J. L., "Manipulation of multiphoton entanglement in waveguide quantum circuits," *Nature Photonics* **3**(6), 346–350 (2009).

[54] Silverstone, J. W., Bonneau, D., Ohira, K., Suzuki, N., Yoshida, H., Iizuka, N., Ezaki, M., Natarajan, C. M., Tanner, M. G., Hadfield, R. H., Zwiller, V., Marshall, G. D., Rarity, J. G., O'Brien, J. L., and Thompson, M. G., "On-chip quantum interference between silicon photon-pair sources," *Nature Photonics* **8**(2), 104–108 (2013).

[55] Davis, K. M., Miura, K., Sugimoto, N., and Hirao, K., "Writing waveguides in glass with a femtosecond laser," *Optics letters* **21**(21), 1729–1731 (1996).

[56] Valle, G. D., Osellame, R., and Laporta, P., "Micromachining of photonic devices by femtosecond laser pulses," *Journal of Optics A: Pure and Applied Optics* **11**(1), 13001 (2009).

[57] Keil, R., Heinrich, M., Dreisow, F., Pertsch, T., Tünnermann, A., Nolte, S., Christodoulides, D. N., and Szameit, A., "All-optical routing and switching for three-dimensional photonic circuitry," *Scientific reports* **1** (2011).

[58] Sansoni, L., Sciarrino, F., Vallone, G., Mataloni, P., Crespi, A., Ramponi, R., and Osellame, R., "Polarization Entangled State Measurement on a Chip," *Physical Review Letters* **105**(20), 1–4 (2010).

[59] Crespi, A., Ramponi, R., Osellame, R., Sansoni, L., Bongioanni, I., Sciarrino, F., Vallone, G., and Mataloni, P., "Integrated photonic quantum gates for polarization qubits," *Nature Communications* **2**, 566 (2011).

[60] Camacho, J. and Tentori, D., "Polarization optics of GRIN lenses," *Journal of Optics A: Pure and Applied Optics* **3**(1), 89–95 (2000).

[61] Tentori, D. and Camacho, J., "Ordinary and extraordinary rays in gradient-index lenses," *Applied optics* **42**(22), 4452–4462 (2003).

[62] Laing, A., Scarani, V., Rarity, J., and O'Brien, J., "Reference-frame-independent quantum key distribution," *Physical Review A* **012304**, 1–5 (2010).

[63] Zhang, P., Aungskunsiri, K., Martín-López, E., Wabnig, J., Lobino, M., Nock, R., Munns, J., Bonneau, D., Jiang, P., Li, H., Laing, A., Rarity, J., Niskanen, A., Thompson, M., and OBrien, J., "Reference-Frame-Independent Quantum-Key-Distribution Server with a Telecom Tether for an On-Chip Client," *Physical Review Letters* **112**(13), 130501 (2014).

[64] D'Ambrosio, V., Nagali, E., Walborn, S. P., Aolita, L., Slussarenko, S., Marrucci, L., and Sciarrino, F., "Complete experimental toolbox for alignment-free quantum communication," *Nature Communications* **3**, 961 (2012).

[65] Zhang, Y., Ning, Y., Zhang, L., Zhang, J., Zhang, J., Wang, Z., Zhang, J., Zeng, Y., and Wang, L., "Design and comparison of GaAs, GaAsP and InGaAlAs quantum-well active regions for 808-nm VCSELs.," *Optics express* **19**(13), 12569–81 (2011).

[66] Michalzik, R., *VCSELs: Fundamentals, Technology and Applications of Vertical-Cavity Surface-Emitting Lasers*, vol. 166 of *Springer Series in Optical Sciences*, Springer Berlin Heidelberg, Berlin, Heidelberg (2013).

[67] Soda, H., Iga, K.-i., Kitahara, C., and Suematsu, Y., "GaInAsP/InP Surface Emitting Injection Lasers," *Japanese Journal of Applied Physics* **18**(12), 2329–2330 (1979).

[68] Ortsiefer, M., Bohm, G., Grau, M., Windhorn, K., Ronneberg, E., Rosskopf, J., Shau, R., Dier, O., and Amann, M.-C., "Electrically pumped room temperature CW VCSELs with 2.3 m emission wavelength," *Electronics Letters* **42**(11), 640 (2006).

[69] Higuchi, Y., Omae, K., Matsumura, H., and Mukai, T., "Room-Temperature CW Lasing of a GaN-Based Vertical-Cavity Surface-Emitting Laser by Current Injection," *Applied Physics Express* **1**, 121102 (2008).

[70] Qiao, P., Su, G.-L., Rao, Y., Wu, M. C., Chang-Hasnain, C. J., and Chuang, S. L., "Comprehensive model of 1550 nm MEMS-tunable high-contrast-grating VCSELs.," *Optics Express* **22**(7), 8541–8555 (2014).

[71] Gierl, C., Gründl, T., Paul, S., Zogal, K., Haidar, M. T., Meissner, P., Amann, M.-C., and Küppers, F., "Temperature characteristics of surface micromachined MEMS-VCSEL with large tuning range," *Optics Express* **22**, 13063 (June 2014).

[72] Li, H., Cui, B., Zhang, M., Zhou, W., Chen, H., Zhang, C., Liu, Y., Tang, C., and Li, E., "Integration of 1550nm vertical-cavity surface-emitting laser with gratings on SOI," *Optics & Laser Technology* **64**, 333–336 (Dec. 2014).

[73] Ferrara, J., Yang, W., Zhu, L., Qiao, P., and Chang-Hasnain, C. J., "Heterogeneously integrated long-wavelength VCSEL using silicon high contrast grating on an SOI substrate," *Optics Express* **23**(3), 2512 (2015).

[74] Seong-Seok Yang, Jeong-Kwon Son, Young-Kyu Hong, Yong-Ho Song, Ho-Jin Jang, Seong-jun Bae, Yong-Ho Lee, Gye-Mo Yang, Hyun-Sung Ko, and Gun-Yong Sung, "Wavelength Tuning of Vertical-Cavity Surface-Emitting Lasers by an Internal Device Heater," *IEEE Photonics Technology Letters* **20**(20), 1679–1681 (2008).

[75] Davani, H. A., Kögel, B., Debernardi, P., Grasse, C., Gierl, C., Zogal, K., Haglund, A., Gustavsson, J., Westbergh, P., Gründl, T., Komissinskiy, P., Bitsch, T., Alff, L., Küppers, F., Larsson, A., Amann, M.-C., and Meissner, P., "Polarization investigation of a tunable high-speed short-wavelength bulk-micromachined MEMS-VCSEL," *Proceedings of SPIE* **8276**, 82760T (2012).

[76] Harrington, J. W., Ettinger, J. M., Hughes, R. J., and Nordholt, J. E., "Enhancing practical security of quantum key distribution with a few decoy states," *arxiv/quant-ph:* **0503002** (2005).

[77] Bäzner, T., *Decoy-Analyse und Photonenstatistik eines mikroskopischen QKD-Senders*, Bachelor's thesis, LMU München (2015).

[78] Brown, R. G. W., Ridley, K. D., and Rarity, J. G., "Characterization of silicon avalanche photodiodes for photon correlation measurements 1: Passive quenching," *Applied Optics* **25**(22), 4122 (1986).

[79] Nordin, G. P., Meier, J. T., Deguzman, P. C., and Jones, M. W., "Micropolarizer array for infrared imaging polarimetry," *Journal of the Optical Society of America A* **16**(5), 1168 (1999).

[80] Rakic, A. D., Djurišic, A. B., Elazar, J. M., and Majewski, M. L., "Optical properties of metallic films for vertical-cavity optoelectronic devices," *Applied Optics* **37**(22), 5271 (1998).

[81] Rytov, S. M., "Electromagnetic properties of a finely stratified medium," *Soviet Physics JETP* **2**(3), 446–475 (1956).

[82] Liao, Y.-L. and Zhao, Y., "Design of wire-grid polarizer with effective medium theory," *Optical and Quantum Electronics* **46**(5), 641–647 (2013).

[83] Adam, S. F. and Packard, H., *Microwave theory and applications*, Prentice Hall (1969).

[84] Snyder, A. W. and Love, J. D., *Optical waveguide theory*, Chapman and Hall, Boston, MA (1984).

[85] Wood, R., "On a remarkable case of uneven distribution of light in a diffraction grating spectrum," *Philosophical Magazine Series 6* **4**(21), 396–402 (1902).

[86] Rayleigh, L., "Note on the remarkable case of diffraction spectra described by Prof. Wood," *Philosophical Magazine Series 6* **14**(79), 60–65 (1907).

[87] Fano, U., "The theory of anomalous diffraction gratings and of quasi-stationary waves on metallic surfaces (Sommerfelds waves)," *Journal of the Optical Society of America* **31**(3), 213 (1941).

[88] Sommerfeld, A., "Über die Ausbreitung der Wellen in der drahtlosen Telegraphie," *Annalen der Physik* **333**, 665–736 (1909).

[89] Ghaemi, H. F., Thio, T., Grupp, D., Ebbesen, T. W., and Lezec, H. J., "Surface plasmons enhance optical transmission through subwavelength holes," *Physical Review B* **58**(11), 6779–6782 (1998).

[90] George, M. C., Bergquist, J., Wang, B., Petrova, R., Li, H., and Gardner, E., "An improved wire grid polarizer for thermal infrared applications," *Proceedings of SPIE* **8613**, 86131I (2013).

[91] Pendry, J. B., Martín-Moreno, L., and Garcia-Vidal, F. J., "Mimicking surface plasmons with structured surfaces," *Science* **305**(5685), 847–8 (2004).

[92] Barnes, W., Preist, T., Kitson, S., and Sambles, J., "Physical origin of photonic energy gaps in the propagation of surface plasmons on gratings," *Physical Review B* **54**(9), 6227–6244 (1996).

[93] Huang, X.-R. and Peng, R.-W., "General mechanism involved in subwavelength optics of conducting microstructures: charge-oscillation-induced light emission and interference," *Journal of the Optical Society of America. A, Optics, image science, and vision* **27**(4), 718–729 (2010).

[94] Liu, H. and Lalanne, P., "Microscopic theory of the extraordinary optical transmission," *Nature* **452**(7188), 728–731 (2008).

[95] Gan, C. H., Pugh, J. R., Cryan, M. J., Rarity, J. G., and Nash, G. R., "Role of quasicylindrical waves and surface plasmon polaritons on beam shaping with resonant nanogratings in the infrared," *Physical Review B* **89**(20), 2–5 (2014).

[96] Oskooi, A. F., Roundy, D., Ibanescu, M., Bermel, P., Joannopoulos, J. D., and Johnson, S. G., "MEEP: A flexible free-software package for electromagnetic simulations by the FDTD method," *Computer Physics Communications* **181**, 687–702 (2010).

[97] Wang, L., Schift, H., Gobrecht, J., Ekinci, Y., Kristiansen, P. M., Solak, H. H., and Jefimovs, K., "High-throughput fabrication of compact and flexible bilayer nanowire grid polarizers for deep-ultraviolet to infrared range," *Journal of Vacuum Science & Technology B: Microelectronics and Nanometer Structures* **32**(3), 031206 (2014).

[98] Ahn, S.-W., Lee, K.-D., Kim, J.-S., Kim, S. H., Park, J.-D., Lee, S.-H., and Yoon, P.-W., "Fabrication of a 50 nm half-pitch wire grid polarizer using nanoimprint lithography," *Nanotechnology* **16**(9), 1874–1877 (2005).

[99] Cetnar, J. S., Middendorf, J. R., and Brown, E. R., "Extraordinary optical transmission and extinction in a Terahertz wire-grid polarizer," *Applied Physics Letters* **100**(23), 102–105 (2012).

[100] Osellame, R., Cerullo, G., and Ramponi, R., *Femtosecond laser micromachining: Photonic and Microfluidic Devices in Transparent Materials*, Springer (2012).

[101] Sugioka, K., Masuda, M., Hongo, T., Cheng, Y., Shihoyama, K., and Midorikawa, K., "Three-dimensional microfluidic structure embedded in photostructurable glass by femtosecond laser for lab-on-chip applications," *Applied Physics A* **79**(4-6), 815–817 (2004).

[102] Ergin, T., Stenger, N., Brenner, P., Pendry, J. B., and Wegener, M., "Three-dimensional invisibility cloak at optical wavelengths.," *Science* **328**(5976), 337–339 (2010).

[103] Lapointe, J., Gagné, M., Li, M.-J., and Kashyap, R., "Making smart phones smarter with photonics.," *Optics express* **22**(13), 15473–83 (2014).

[104] Osellame, R., Taccheo, S., Marangoni, M., Ramponi, R., Laporta, P., Polli, D., De Silvestri, S., and Cerullo, G., "Femtosecond writing of active optical waveguides with astigmatically shaped beams," *Journal of the Optical Society of America B* **20**(7), 1559 (2003).

[105] Cerullo, G., Osellame, R., Taccheo, S., Marangoni, M., Polli, D., Ramponi, R., Laporta, P., and De Silvestri, S., "Femtosecond micromachining of symmetric waveguides at 1.5 micron by astigmatic beam focusing.," *Optics letters* **27**(21), 1938–1940 (2002).

[106] Corrielli, G., Crespi, A., Geremia, R., Ramponi, R., Sansoni, L., Santinelli, A., Mataloni, P., Sciarrino, F., and Osellame, R., "Rotated waveplates in integrated waveguide optics," *Nature Communications* **5**, 1–6 (2014).

[107] Heilmann, R., Gräfe, M., Nolte, S., and Szameit, A., "Arbitrary photonic wave plate operations on chip: realizing Hadamard, Pauli-X, and rotation gates for polarisation qubits.," *Scientific reports* **4**(10), 4118 (2014).

[108] Yan, Z., Duan, Y., Helt, L. G., Ams, M., Withford, M. J., and Steel, M. J., "Generation of heralded single photons beyond 1100 nm by spontaneous four-wave mixing in a side-stressed femtosecond laser-written waveguide," *Applied Physics Letters* **107**(23), 231106 (2015).

[109] Saleh, B. E. A. and Teich, M. C., *Fundamentals of PHOTONICS*, Wiley (1991).

[110] Sansoni, L., Sciarrino, F., Vallone, G., Mataloni, P., Crespi, A., Ramponi, R., and Osellame, R., "Two-Particle Bosonic-Fermionic Quantum Walk via Integrated Photonics," *Physical Review Letters* **108**(1), 1–5 (2012).

[111] Fung, C. H. F. and Lo, H. K., "Security proof of a three-state quantum-key-distribution protocol without rotational symmetry," *Physical Review A - Atomic, Molecular, and Optical Physics* **74**(4), 1–9 (2006).

[112] Rau, M., Vogl, T., Corrielli, G., Vest, G., Fuchs, L., Nauerth, S., and Weinfurter, H., "Spatial mode side channels in free-space QKD implementations," *IEEE Journal of Selected Topics in Quantum Electronics* **21**(3), 1–5 (2015).

[113] Sajeed, S., Chaiwongkhot, P., Bourgoin, J.-P., Jennewein, T., Lütkenhaus, N., and Makarov, V., "Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch," *Physical Review A* **91**(6), 062301 (2015).

[114] Weier, H., Krauss, H., Rau, M., Fürst, M., Nauerth, S., and Weinfurter, H., "Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors," *New Journal of Physics* **13**(7), 073024 (2011).

[115] Elmer, P., "SPCM-AQ4C Single Photon Counting Module Array," datasheet.

[116] Rau, M., *Title to be announced*, PhD thesis, LMU München (2016).

[117] Gebhardt, C., *Implementierung des Quantenschlüsselaustauschs auf einem mobilen Endgerät*, Bachelor's thesis, Ludwig-Maximilians-Universität München (2014).

Publications

This work has led to the following publications:

- *Integrated quantum key distribution sender unit for daily-life implementations*, **G. Mélen**, T. Vogl, M. Rau, G. Corrielli, A. Crespi, R. Osellame and H. Weinfurter. Proc. SPIE 9762, Advances in Photonics of Quantum Computing, Memory, and Communication IX, 97620A (2016)

- *Impact of the slit geometry on the performance of wire-grid polarisers*, **G. Mélen**, W. Rosenfeld and H. Weinfurter. Opt. Express **23**, 32171 (2015)

- *Design and Evaluation of a Handheld Quantum Key Distribution Sender module*, **G. Vest**, M. Rau, L. Fuchs, G. Corrielli, H. Weier, S. Nauerth, A. Crespi, R. Osellame and H. Weinfurter. IEEE Journal of Selected Topics in Quantum Electronics **21**(3):131-137 (2015)

Others articles:

- *Spatial Mode Side Channels in Free-Space QKD Implementations*, M. Rau, T. Vogl, G. Corrielli, **G. Vest**, L. Fuchs, S. Nauerth and H. Weinfurter. IEEE Journal of Selected Topics in Quantum Electronics **21**(3): 87-191 (2015)

- *Free space quantum key distribution over 500 meters using electrically driven quantum dot single-photon sourcesa proof of principle experiment*, M. Rau, T. Heindel, S. Unsleber, T. Braun, J. Fischer, S. Frick, S. Nauerth, C. Schneider, **G. Vest**, S. Reitzenstein, M. Kamp, A. Forchel, S. Höfling and H. Weinfurter. New Journal of Physics **16**(4) (2014)

Selected conference contributions

- *Integrated quantum key distribution sender unit for daily-life implementations*, SPIE Photonics West, San Francisco, CA, USA, February 13-18 2016

- *Micro-optics based Quantum Key Distribution sender unit for secure short distance communication* (Poster), Qcrypt 2014, Paris, France, September 1-5 2014

- *Quantum Key Distribution sender add-on for handheld devices*, CLEO Europe, Munich, Germany, June 21-25 2015

- *Design and evaluation of a handheld Quantum Key Distribution sender module*, DPG Spring meeting, Heidelberg, Germany, March 23-27 2015

- *Design and evaluation of a handheld Quantum Key Distribution sender module*, PICQUE Workshop in integrated photonics, Oxford, UK, January 7-10 2015

- Compact micro-optics based QKD unit towards secure short-range communications (Poster),
  SeQre 2014, Wroclaw, Poland, January 27-28 2014

Acknowledgements

Zum Abschluss möchte ich mich bei all jenen bedanken, die zum Gelingen meiner Doktorarbeit beigetragen haben. Auch wenn ich in den letzte vier Jahren öfters den Eindruck hatte, alleine in diesem Projekt zu stecken, muss ich rückblickend gestehen, dass ich doch Unterstützung und Hilfe bekommen habe. Es ist deshalb Zeit, mich bei denen zu bedanken, die mir besonders geholfen haben:

- Prof. Harald Weinfurter, der mir einen sanften Übergang von der Ingenieurwissenschaft in die Quantenphysik erlaubt hat. Ich bedanke mich für die persönliche Betreuung und für die Verantwortungen, die du mir schon am Anfang gegeben hast (und die ich zunächst nicht immer gut angenommen habe). Deine Leidenschaft für Physik und die Forschung werden mich noch lange begleiten, ebenso wie deine österreichischen Sprichwörter.

- qutools GmbH für die finanzielle Unterstützung duch das Marie-Curie Stipendium über das CIPRIS Projekt. Ein besonderer Dank geht an Henning, der die letzten Jahre sowohl beruflich als zweiter Betreuer als auch im persönlichen Rahmen als (frauenverstehender) Freund immer da war.

- Der Leiter des CIPRIS Projekts, Prof. Thomas Halfmann, und seine Doktoranden Daniel Schraft and Simon Mieth von der TU Darmstadt für die angenehme Zeit bei ihnen im Labor und bei den offiziellen Projekttreffen.

- Dr. Wenjamin Rosenfeld für seine wertvolle Hilfe im Laufe des letzten Jahres, und seine immer sinnvollen Antworten zu meinen (unter anderem wissenschaftlichen) Fragen. Danke für die konstruktiven, aber anscheinend *anstrengenden* Gespräche über Plasmonen und Atomphysik, die Schokoladenpausen und für die "Alles wird gut" (Selbst-)Motivationssprüche.

- Die andere *Cryptos*: Sebastian Nauerth und Markus Rau, die mir so viel über Elektronik und Programmierung beigebracht haben; die zahlreichen Bachelor- und Masterstudenten, insbesondere Tobias Bäzner und Tobias Vogl, die mir bei dem Projekt wirklich geholfen haben und mir gezeigt haben, dass fleißige Studenten zu betreuen auch Spass machen kann. Ich habe mich über unsere Zusammenarbeit wirklich gefreut und wünsche euch alles Gute für die Zukunft.

- Meine Bürokollegen Martin and Toshi für die lustige bayerische/japanische Umgebung; die andere Doktoranden (Daniel B., Robert, Julian, Lukas, Michael, Daniel L., Lars, Norbert, Kai, Daniel S., Christian), die dafür gesorgt haben, dass ich mich in der Gruppe als Ausländerin und auch als einzige Frau immer wohl gefühlt habe.

- Dr. Nathalie Picqué für ihre Hilfe mit den Spektrenmessungen, und für die interessanten und entspannenden Kaffeepausen auf Französisch.

- Philipp Altpeter für sein Engagement und seine Ratschläge bei der Elektronstahllithographie und allen anderen Sachen, die ich im Reinraum probieren wollte und nicht immer funktioniert haben. Sonja Matich and Peter Weiser vom Walter Schottky Institut für das FIB-Training und ihre weitere Hilfe beim Lösen von Problemen.

- VI-Systems für das Bereitstellen von Single-Mode VCSEL Matrizen.

- Meine Freunden, die mich meistens von weit weg unterstüzt haben (merci les filles... et Pierre !). Ein besonderer Dank an Anna und Meergul für die schöne Wochenendabwechslung, und an Marilena and Dorothee für ihre tägliche, ansteckende gute Laune.

- À ma famille, que j'aurais souhaité avoir près de moi durant cette aventure, mais avec qui les retrouvailles en France ou en Allemagne m'auront laissé des souvenirs impérissables. Merci à mes parents de m'avoir permis d'en être arrivée jusqu'ici, et à mon frère Jocelyn d'avoir partagé avec moi les déboires et frustrations du doctorat (bon courage pour la dernière ligne droite... en espérant que 2016 soit aussi l'année de ta thèse !). Enfin, un immense merci à mon mari Clément, pour son soutien quotidien, son calme et sa patience, ainsi que ses précieux conseils durant ces quatre années.

- Pour finir sur une note d'ironie bien propre à la culture française, je remercie tous ceux qui m'ont fait prendre conscience assez tôt d'une certaine facette de la recherche, et leur dédie cette citation d'Albert Einstein, tirée de *Comment je vois le monde*: "J'ai experimenté l'Homme, il est inconsistant".