Fast and Practical Integrated Quantum Communication Systems

Sax, Anna Rebecka

Université de Genève
Département de Physique Appliquée

Faculté des Sciences
Professeur Hugo Zbinden

Fast and practical integrated quantum communication systems

Thèse

présentée à la Faculté des sciences de l'Université de Genève
pour obtenir le grade de Docteur ès sciences, mention Physique

par

Rebecka Sax

de Bjärred, Suède

Thèse N° 5765

Genève
2023

UNIVERSITÉ DE GENÈVE
FACULTÉ DES SCIENCES

DOCTORAT ÈS SCIENCES, MENTION PHYSIQUE

Thèse de Madame Anna Rebecka SAX

intitulée :

«Fast and Practical Integrated Quantum Communication Systems»

La Faculté des sciences, sur le préavis de Monsieur H. ZBINDEN, professeur honoraire et directeur de thèse (Département de physique appliquée), Monsieur R. THEW, docteur (Département de physique appliquée), Monsieur D. RUSCA, docteur (Vigo Quantum Communication Center, Universida de Vigo, Vigo, Espagne), Monsieur G. BOSO, docteur (ID Quantique (IDQ), Genève) et Madame E. DIAMANTI, professeure (Laboratoire d'informatique, Sorbonne Université, Paris, France), autorise l'impression de la présente thèse, sans exprimer d'opinion sur les propositions qui y sont énoncées.

Genève, le 18 septembre 2023

Thèse - 5765 -

La Doyenne

N.B. - La thèse doit porter la déclaration précédente et remplir les conditions énumérées dans les "Informations relatives aux thèses de doctorat à l'Université de Genève".

When I was young, it seemed that life was so wonderful
A miracle, oh, it was beautiful, magical
And all the birds in the trees, well they'd be singing so happily
Oh, joyfully, oh, playfully watching me
But then they sent me away to teach me how to be sensible
Logical, oh, responsible, practical
Then they showed me a world where I could be so dependable
Oh, clinical, oh, intellectual, cynical

There are times when all the world's asleep
The questions run too deep
For such a simple man
Won't you please, please tell me what we've learned ?
I know it sounds absurd
Please tell me who I am

I said, now, watch what you say, they'll be calling you a radical
A liberal, oh, fanatical, criminal
Oh, won't you sign up your name ? We'd like to feel you're acceptable
Respectable, oh, presentable, a vegetable
Oh, take, take, take it, yeah

But at night, when all the world's asleep
The questions run so deep
For such a simple man
Won't you please (oh, won't you tell me)
Please tell me what we've learned ?
(Can you hear me ?) I know it sounds absurd
(Oh, won't you tell me) please tell me who I am
Who I am, who I am, who I am

Supertramp, "The Logical Song", *Breakfast in America*, A&M Records, 1979, CD.

Abstract

Quantum technologies are the main topic of more research projects than ever within the scientific community. The most mature examples of such technologies, in terms of commercialisation, are quantum key distribution (QKD) and quantum random number generators (QRNGs). At this point in their development, academia and industry are interested in a scalable, reliable and cheap production of such systems, which is where the usage of integrated photonic circuits (PICs) come in handy.

First, I will present the development of two fibre-based QKD systems, based on a simplified QKD protocol [1], which I took part in during my thesis. One system was implemented to operate in combination with classical communication through the usage of wavelength division multiplexing. The other one was made to achieve as high secret key rate as possible, achieved by employing multipixel superconducting nanowire single-photon detectors, among other improvements.

Secondly, the primary focus of my work, which resides in the development and implementation of a QKD system based on integrated photonics, using the simplified QKD protocol, will be presented. On the transmitter side, a silicon photonics PIC was developed and manufactured in close collaboration with IDQ SA and Sicoya GmbH. The PIC, when used with an external laser, allows for high-speed and accurate state preparation. On the receiver side, two distinct integrated photonic platforms were investigated. One was based on silica on silicon, established in collaboration with VLC photonics and the other one was based on silica, established in collaboration with the Institute for Photonics and Nanotechnologies (IFN) in Milano. The silica PIC was employed for the final integrated QKD setup thanks to its low loss and polarisation independence. Full secret key exchanges over hundreds of kilometers of single-mode fibre between the transmitter and receiver were performed, employing either superconducting nanowire single-photon detectors or single-photon avalanche diodes. The corresponding secret key rates obtained with the aforementioned detectors are 9.4 kbps over 202 km and 1.3 kbps over 151.5 km, respectively.

Finally, I introduce a recent project of my thesis, namely, the implementation of a QRNG in an integrated circuit. The QRNG is based on a self-testing protocol employing homodyne detection. We developed a PIC based on indium phosphide in collaboration with HHI Fraunhofer, which includes all the optics of the experimental setup. Investigations are currently ongoing and I will in this manuscript present the developed electronics, the schematics of the chip as well as some preliminary characterisations.

1. The 3-state time-bin Bennett-Brassard 1984 QKD protocol with 1-decoy state

Résumé

Les téchnologies quantiques sont plus que jamais au coeur de la recherche. Les plus matures des téchnologies sont : la distribution de clé quantique (QKD) et la géneration de nombre aléatoires (QRNG). Elles sont suffisamment avancées pour avoir trouvé leur place dans l'industrie et sont déjà produites et commercialisées. À ce stade de leur développement, les universités et les industries s'intéressent à une production de manière évolutive, fiable et bon marché. Les circuits photoniques intégrés (PIC) répondent à ce besoin. L'objectif principal de mon travail est de développer et mettre en œuvre un système QKD basé sur la photonique intégrée, utilisant un protocole QKD simplifié [2]. Côté émetteur, un PIC photonique en silicium a été développé et fabriqué en étroite collaboration avec IDQ SA et Sicoya GmbH. Le PIC, utilisé avec un laser externe, permet une préparation d'états rapide et précise. Côté récepteur, deux plateformes photoniques intégrées distinctes ont été étudiées. Une, à base de silice sur silicium, créé en collaboration avec VLC photonics, et l'autre à base de silice, fabriquée avec la technique de micro-usinage par laser femtoseconde, crée en collaboration avec l'Institut de Photonique et de Nanotechnologies (IFN) à Milan. Ce dernier a été utilisé pour l'implementation QKD intégrée finale grâce à sa faible perte et son indépendance à la polarisation. Des échanges de clés secrets complets sur des centaines de kilomètres de fibre monomode entre l'émetteur et le récepteur ont été effectués, en utilisant soit des détecteurs à photon unique à nanofils supraconducteurs, soit des diodes à avalanche à photon unique. Les débits de clé secrète obtenus avec les détecteurs susmentionnés sont respectivement de 9.4 kbps sur 202 km et de 1.3 kbps sur 151.5 km. Un autre intérêt de mon travail porte sur l'implémentation d'un QRNG dans un circuit intégré. Nous avons dévelopé ce PIC basé sur le phosphure d'indium en collaboration avec HHI Fraunhofer. Le QRNG est basé sur un protocole d'autotest employant la détection homodyne. Des analyses sont actuellement en cours. J'ai également participé au développement de deux systèmes QKD à base de fibre. L'un d'eux fonctionne en combinaison avec la communication classique grâce à l'utilisation du multiplexage en longueur d'onde. L'autre a été conçu pour atteindre un taux de clé secrète aussi élevé que possible, obtenu en utilisant des détecteurs à photon unique à nanofils supraconducteurs multipixels.

2. Protocole Bennett-Brassard 1984 à 3 états, avec 1-decoy.

Contents

Acronyms

A *anti-diagonal*. 11

AA *absorber attenuator*. 35, 39, 41–43, 85

ADC *analog-to-digital converter*. 43, 44, 75, 78

AES *advanced encryption standard*. 2, 19

AlGaAs *aluminuim gallium arsenide*. 6, 7

APCB *Alice printed circuit board*. 33, 53

bal-MZI *balanced Mach-Zehnder interferometer*. 35, 38, 39, 68, 71

BB84 *Bennett-Brassard 1984*. 8, 11, 12, 16–18, 25, 31, 44, 49, 54–56, 59, 81

BER *bit error rate*. 13

BOX *buried oxide*. 6, 37

BPCB *Bob printed circuit board*. 53

BPSK *binary phase-shift keying*. 67

CMOS *complementary metal–oxide–semiconductor*. 5, 7

CV *continuous variable*. 59

CWDM *coarse wavelength division multiplexer*. 28, 30

D *diagonal*. 11

DAC *digital-to-analog converter*. 19, 25, 33, 58

DC *direct current*. 39

DCF *dispersion compensating fiber*. 20, 52, 58, 82

DD *device-dependent*. 63

DFB *distributed feedback*. 5, 19, 71

DI *device-independent*. 63

DV *discrete variable*. 29

DWDM *dense wavelength division multiplexing*. 28, 29

EIC *electronic integrated circuit*. 4, 5, 33, 35, 53, 81

EOPS *electro-optic phase shifter*. 6, 34, 35, 38, 39, 44, 45, 71–74, 79, 82

ER *extinction ratio*. 41, 42, 45, 52, 54, 76, 79

FBG *fibre Bragg grating*. 29

Fe *iron*. 7

FPGA *field programmable gate array*. 18, 19, 21, 52–54, 73, 74, 131

FWHM *full width at half maximum*. 19, 22, 52

GaAs *gallium arsenide*. 6, 7

H *horizontal*. 11

HT *heater*. 35, 40–45, 49, 53

IC *integrated circuit*. 4, 5, 33

IM *intensity modulator*. 19, 20, 25, 33, 35, 39, 40, 44, 45, 52–54, 56

imb-MI *imbalanced Michelson interferometer*. 19–22, 25, 46

imb-MZI *imbalanced Mach-Zehnder interferometer*. 16, 29, 33, 35, 40–43, 45–53, 57, 86

InGaAs *indium gallium arsenide*. 23, 29, 54–56

InGaAsP *indium gallium arsenide phosphide*. 5

InP *indium phosphide*. 5–9, 23, 29, 54–56, 58, 70

ITU *International Telecommunication Union*. 28, 83

LDPC *low-density parity check*. 54

$LiNbO_3$ *lithium niobate*. 6, 8, 19

LO *local oscillator*. 67, 68, 71, 77

M *measurement*. 64, 66

MDI *measurement-device-independent*. 59

MMI *multi-mode interferometer*. 39

MoSi *molybdenum silicide*. 23

MPO *multiple-fibre push-on/pull-off*. 36

MZI *Mach-Zehnder interferometer*. 6, 38–41, 49, 53, 56, 71, 76, 79, 82

NbTiN *niobium titanium nitride*. 23, 31

OP-AMP *operational amplifier*. 74–76, 78

OTP *one-time pad*. 2–4, 13, 30

P&M *prepare-and-measure*. 64

PBS *polarising beam-splitter*. 69

PC *personal computer*. 1, 18, 53, 73, 78

PCB *printed circuit board*. 33, 36, 48, 49, 58, 70, 72–76, 79, 82

PD *photodiode*. 35, 43, 71, 73–76, 78, 79

PDL *polarisation dependent loss*. 41

PG *pulse generator*. 52

PIC *photonic integrated circuit*. 4–9, 30, 33–39, 41, 42, 44–53, 56–58, 60, 69–76, 78, 79, 81, 82, 86, 89

PID *proportional, integral, derivative*. 45

PNS *photon number splitting*. 16

PRNG *pseudo random number generator*. 3, 19, 61, 62

QBER *quantum bit error rate*. 13, 14, 19, 20, 22, 27, 30, 51, 59

QC *quantum channel*. 18

QCNR *quantum to classical noise ratio*. 75–77

QKD *quantum key distribution*. 3–9, 11, 18, 25, 27, 29–31, 33, 37, 46, 48–50, 52, 53, 55–61, 63, 81–83, 131

QRNG *quantum random number generator*. 4–9, 19, 63–65, 69–72, 75, 79, 82, 83, 89, 131, 132

RKR *raw key rate*. 54–57

RNG *random number generator*. 9, 61–63

RSA *Rivest-Shamir-Adleman*. 2, 81

S *source*. 64, 66

SC *service channel*. 18

SDI *semi-device-independent*. 63, 64, 66, 69, 70

SDP *semi-definite program*. 66, 67

SFP *small form-factor pluggable*. 18

Si *silicon*. 6–8, 38, 58

Si_3N_4 *silicon nitride*. 6, 7

SiGe *silicon germanium*. 6, 39

SiO_2 *silica*. 6, 7

SiO_xN_y *silicon oxynitride*. 6, 7

SKR *secret key rate*. 8, 16, 17, 21, 22, 24, 25, 27, 29–31, 45, 52–59, 81

SMA *sub-miniature version A*. 74

SMF *single-mode fibre*. 18, 20, 29, 30, 35–37, 48, 49, 52, 54–56

SNR *signal-to-noise ratio*. 74

SNSPD *superconducting nanowire single-photon detector*. 7, 8, 22–24, 31, 53–56, 58, 60, 81

SOA *semiconductor optical amplifier*. 71, 72

SOI *silicon on insulator*. 70

SPAD *single-photon avalanche diode*. 22–24, 53–56, 58, 81

SPD *single-photon detector*. 22, 30, 31, 46, 53, 82

TEC *thermoelectric cooling*. 45, 49

TIA *transimpedance amplifier*. 73–77, 79, 90

TiN *titanium nitride*. 38

TOPS *thermo-optic phase shifter*. 6, 35, 37–40, 49, 71

TRNG *true random number generator*. 3, 61, 63

UV *ultraviolet*. 48

V *vertical*. 11

VOA *variable optical attenuator*. 20, 39, 52, 54, 68, 70, 71, 76

WDM *wavelength division multiplexing*. 8, 28, 29, 31

1. Introduction

1.1. Secure communication

1.1.1. Motivations of investigating secure communication

The subject of secure communication is more than ever in the spotlight. In a world where almost everyone has a (smart)phone [1] and/or a *personal computer* (PC) it is hard to even imagine the number of messages, calls and emails that are sent on a daily basis, via internet or telecommunications. Many, dare I say most, of these messages are sent to a designated person or group, meaning that the communication is assumed to take place in a *private* manner. This means that a person who is not intended to receive the message, effectively does not receive it, nor can they actively see it, even though they try to. The issue, and desire, of secure (private) communication concerns not only civilians, but also, companies, banks, hospitals, governments and the military.

The major part (99%) of this constant communication takes place thanks to the vast network of fibre optic cables placed around the world [2]. For example, between Europe and the Americas thousands of kilometers of hundreds of fibre optic cables are placed on the bottom of the Atlantic ocean [3]. In between neighbouring countries or cities these cables are placed several metres underground. Ever since their placement, interested and malicious individuals, organisations or governments have actively tampered the lines to obtain access to the data passing through or to simply sabotage and destabilise economical markets [4–7]. Effectively, getting hold of data sent over a given fibre, which possibly contains highly confidential information sent between or within governments, could be incredibly harmful if leaked. Recently the European commission even published an in-depth analysis titled "Security threats to undersea communications cables and infrastructure: consequences for the EU" [8] with the goal to improve the resilience of the cable network by improving its surveillance and repairment.

Luckily, data sent on these lines are, in the case of private communication, *encrypted*, meaning that to read the message one has to first *decrypt* it. For a symmetric communication process, the sender and the receiver each have an identical *key* with which the sender encodes the message and the receiver decodes it. In more technical terms, the encrypted message is referred to as a *cipher*. Hence, the security of the communication process relies on a good encryption scheme, which should not be too simple to crack. There are many ways of encrypting a message, one can for example use a substitution cipher. The Caesar cipher is an example of such an encryption method. In this scheme, each letter in the message is replaced by another one by moving a fixed number of positions down the alphabet. The sentence "I love ice cream", can become something

1. According to Statistica [1] in 2022 there were 6.6 billion mobile network subscriptions.

as unreadable as "P svcl pjl jylht", by shifting the alphabet 7 steps [2]. The problem with this encryption method is that a simple study of the 25 possibilities [3] suffices to crack the key (find the shift parameter) and be able to read the message. As the name indicates, it was effectively used by Julius Caesar when corresponding with his army, giving evidence that the need for secure communication goes back at least 100 years B.C. Actually, the word cryptography, which encompasses the study of secure communication when a malicious party is present, comes from Ancient Greek. Crypto means "hidden" or "secret". Other examples of ways of producing a key includes coding letters in numbers, in binary, using symbols or via Morse code.

So, which method is used to produce a key with which we encrypt the data we send via internet and how can we be sure that the key is not easily decipherable? Nowadays, the employed symmetric key algorithm is the *advanced encryption standard* (AES) [9] [4]. With a short random key as input, the output of the AES protocol is an expanded random key. Presently it is made up of 256 bits. To crack the key via brute force, $2^{256} > 10^{77}$ steps have to be done, which would take many, many years using present-time top-performing computers. Another widely used encryption algorithm is the *Rivest-Shamir-Adleman* (RSA) asymmetric public-private key algorithm [10]. The security of this algorithm is based on the assumption that factoring large integers is computationally intractable. Indeed, the adversary has to find two prime numbers, p and q, given only their product $N(= p \cdot q)$ to crack the key.

As of today, no one has found a way to solve the aforementioned problem in a reasonable amount of time [5] on a classical computer [6]. However, there is absolutely no way of confirming that never in the future will someone think of a clever algorithm to solve the problem and so crack the key. Actually, all the transferred data can be stored and read later on in the future when the key can be hacked. This is the major issue of the key algorithms used today. As a matter of fact, back in 1994, mathematician Peter Shor developed a quantum algorithm [11, 12] for factoring a number N. This algorithm could hence be used to crack RSA. Given the advancements in the development of a quantum computer [13–15], the security of the present-day encrypted data is literally resting on a ticking time-bomb. The need for a key algorithm that does not rely on any computational complexities is imminent.

Already many years ago now, an ingenious non-crackable encryption method called the *one-time pad* (OTP) was thought of. First, by Frank Miller in 1882, whose goal was to secure telegraphy [16] and then by Gilbert Vernam who placed a patent on it in 1919 [17, 18]. Finally, in 1940, the mathematician and cryptographer Claude Shannon proved OTP to be information-theoretically secure [19]. Such security is the strongest type, meaning that an adversary with even the most amount of computational power cannot crack the key. Actually, an adversary cannot obtain any information about the message sent, except its maximum length. Requirements for unconditional

2. The key is the shift parameter, 7 in this case.

3. For the English alphabet.

4. Sometimes the term AES expansion is also heard of. The AES key encryption steps includes one step of key expansion in order to properly encrypt all data blocks.

5. It is hard to estimate the time it would take as it depends on the algorithm used and the computational power of the used machine. However currently, this time is certainly longer than the life-time of several generations of humans. The factoring of RSA numbers has been solved several times: `https://en.wikipedia.org/wiki/RSA_numbers`, visited 29/07/23.

6. Meaning a PC sold in electronics stores in the year of 2023, which can even be the most computationally powerful one on the market.

security on the pad (key) is that it is at least as long as the message and that it is renewed for each message (*one-time* pad). Additionally, the pad values have to be truly random.

Despite the obvious advantage of using OTP, it's practical implementation is complicated to realise in a real-world scenario. For instance, given the high bandwidths (around the mega bit per second) of data sent and secured today per person, the sender and receiver would have to store a huge amount of secret keys. Also, the possession of the keys have to happen before the communication, which also brings about the problem of key exchange at a distance. In this scenario they effectively have to meet and share the keys before they want to communicate at a distance, which is not possible, nor the goal, in the multi-user environment used today (the internet). More than that, the randomness of the key is crucial and has to come from a *true random number generator* (TRNG), as opposed to a *pseudo random number generator* (PRNG). The latter provides numbers coming from a deterministic algorithm whereas the numbers produced by the former come from a truly random physical process. For now there is no practical software solution of a TRNG, whereas the usage of PRNGs are widespread.

Currently, there exists a secure method to overcome the issue of key exchange at a distance, called *quantum key distribution* (QKD) [7]. OTP and QKD employed together bring about information-theoretically secure communication. The security of the key produced and distributed when adopting QKD is based on the laws of quantum mechanics, as opposed to complicated mathematical problems. In other words, security is ensured by the laws of nature and does not rely anymore on the limitation in computational power of an adversary. Highly different rules from what we are used to govern in the quantum regime, notably any measurement that is performed on the system will necessarily perturb it. Hand in hand with this, comes the impossibility to perfectly copy any quantum states, referred to as the no-cloning theorem [20].

In classical information theory, the framework which allows to describe for example how a classical computer transmits and stores data, encodes information in *bits*, which are 0s or 1s. In quantum information theory, *qubits* are used instead. Here qubits are represented as: $|0\rangle$ and $|1\rangle$. Additionally, they can live in a superposition of both states, for example the state $|+\rangle$ is defined as: $|+\rangle = \frac{1}{\sqrt{2}}[|0\rangle + e^{i\phi}|1\rangle], \phi \in [0, \pi]$. The basic ingredients of a QKD protocol include thus *quantum states* encoded in a specific degree of freedom of a quantum entity. In the scope of this work *photons* are used and information can be encoded, for example, in their phase, polarisation or time of arrival. A *quantum channel*, where the photons travel between sender and receiver, is also necessary. This is usually the free-space or a fibre-optic cable. Another important matter concerns the authentication between the sender and receiver. If the channel is not authenticated, an adversary can impersonate one of the parties and render the communication unsure, called a *Man-in-the-middle* attack. Authentication can be done by having a pre-shared key or through the usage of other protocols which are not the focus of this work. We assume throughout the thesis that the sender and the receiver are authenticated.

QKD being an example of a cryptographic protocol, inherits the traditionally used names for the sender or transmitter of the message and its receiver, namely, *Alice* and *Bob*, respectively. For the rest of the thesis when mentioned, Alice and Bob carry these same roles. A third role is

7. Another proposed method is called Post Quantum Cryptography, which focuses on developing classical encryption methods that are secure against quantum computers.

the one of the (malicious) eavesdropper of the private communication, called *Eve*.

Similarly to OTP, a QKD protocol, requires the generation of true random numbers, which is based on a random physical process. Examples of classical physical processes which can be adopted for such usage are thermal or atmospheric noise. Although their processes are highly unpredictable, their unpredictability is based on the lack of knowledge of the user on the initial conditions and the various parameters of the system. As a result, modelling the system is quite unfeasible and the process output is thus considered random. The insurance of the randomness of the produced numbers coming from such a device is based on a computational limitation. Indeed, with perfect knowledge of the initial conditions and the different parameters these numbers can be precisely predicted. Hence, to improve the security of the random numbers, i.e. to render them genuinely random, we use quantum physics. There are various processes that can be described by quantum mechanics and that are fundamentally random. Examples of such are a nuclear decay [21], the detection of photons passing through an ideal 50/50 beam-splitter [22–24], vacuum fluctuations [25, 26] or shot noise [27]. Random number generation with one of these processes is called a *quantum random number generator* (QRNG).

1.2. Integrated photonics

1.2.1. Motivations utilising integrated photonics

Another topic, which all of the readers of this thesis are close to on a everyday basis, concerns the one of *integrated circuit*s (ICs). An IC can be defined as a collection of elements, which are inseparable and connected together such that the IC would no longer function if divided. The first industrial breakthrough of the IC took place in 1958 when Texas Instruments employee Jack Kilby invented the hybrid IC [8]. Not long after, Robert Noyce invented the first monolithic IC, which is the foundation of the present-day ICs.

Commonly called an IC, more specifically refers to an *electronic integrated circuit* (EIC), as it constitutes of electronic elements (transistors, resistors, capacitors, etc.) placed and connected together on a small chip. The miniaturisation of electronic circuits, essentially meaning fitting more transistor nodes on smaller circuits, has allowed for an incredible expansion and development in electronic systems. Moore's Law [28], asserting an exponential increase in number of transistors per unit area as a function of time [9], is actually still (in 2023) held true. The main advantages of integrating electronic components, despite the obvious reduction in size, is the lowering of cost of production when producing more EICs on the same wafer and also its indisputable scalability. EICs are found in all electronic devices that are sold today (computer, playstation, smartphone, washing machine, bike lamp, etc.).

Not many years after the EIC, another domain of ICs emerged, notably that of *photonic integrated*

8. He was awarded the Noble Prize in 2000 "For his part in the invention of the integrated circuit.": `https://www.nobelprize.org/prizes/physics/2000/summary/`.

9. In his article in 1965 he predicted that: "Cramming more components onto integrated circuits would lead to wonders such as home computers—or at least terminals connected to a central computer—automatic controls for automobiles, and personal portable communications equipment.".

*circuit*s (PICs). The first research paper on integrated photonics came out in 1969 by Stewart E. Miller, worker at Nokia Bell Labs [29] and the first PIC was based on the integration of an *indium gallium arsenide phosphide* (InGaAsP)/*indium phosphide* (InP) *distributed feedback* (DFB) laser and an electro-absorption modulator [30]. Integrated photonics deals with the creation, manipulation and detection of photons confined and guided in a waveguide. For comparison, EICs are based on the flow of electrons in a chip. A PIC consists of passive and/or active elements that are connected together via waveguides on a chip. Passive components include for example couplers or multiplexers and active components are for example lasers, amplifiers, detectors or modulators. The advantages of PICs are similar to those of EICs. Additional advantages that have not yet been mentioned include for example stability, robustness, lower power consumption, simple temperature stabilisation. Depending on the platform, techniques of manufacturing PICs are *complementary metal–oxide–semiconductor* (CMOS) compatible, a well-established IC fabrication process. PICs are in most cases larger than EICs, however the size of a PIC is, depending on the components that are integrated, around 1-3 orders of magnitude smaller than their corresponding bulk versions.

Examples of usages of PICs are found in the telecommunications industry (for (de)multiplexing purposes), in the sensing industry (for the production of cheap biomedical instruments, determining soil qualities and detecting diseases in food) and in the automobile industry (for Lidar [10] applications). Not long ago, thanks to their practicality, versatility and other aforementioned qualities, PICs have also been applied in the world of quantum communication. The technologies we are interested in here are those of QKD and QRNGs, which correspond to two of the most mature technologies within quantum communication. This means that they are not far away of being utilised in an industrial, real-world, scenario. Some examples of field-trials and use-cases of the technologies include [31–37] and the work [38] provides a recent review. Additionally, several companies already sell such systems [11]. In order to industrialise these systems in a cost- and power-efficient, scalable and smooth [12] manner, the integration of them into PICs is unavoidable.

As opposed to the integrated electronics industry, which is mostly based on silicon photonics and transistors, the integrated photonics industry does not rely on one main platform nor component. The variety of implementations and applications has generated a broad range of research and development on multiple integrated photonic platforms, each of which comes with a distinct set of advantages and disadvantages. Thus, depending on the application, one might opt for one platform or another, or even consider a hybrid or heterogeneous solution [13]. The first implementation of a QKD system [14] using PICs is the work of [40] from 2004 and the first integrated QRNG setup, the work of [27] [15] from 2014, to our knowledge. Since then several research groups have undertaken this challenge with excellence. These works are composed of a large range of different platforms and protocols. We recommend [41, 42] for complete reviews of integrated QKD and QRNG works and [43] for a review of the different platforms used for quantum technologies. The reader will also find table 4.7, in chapter 4, which contains the performances of a

10. Light detection and ranging.
11. For example: IDQ SA or Toshiba.
12. Meaning to minimise the disturbance on the existing fibre optical network.
13. A hybrid and a heterogeneous solution are not the same, for further information we suggest the work [39].
14. The receiver was integrated, in a hybrid manner, using a planar light-wave circuit.
15. They used an integrated camera from a mobile phone.

selection of integrated QKD works.

1.2.2. Details of various integrated photonics platforms

The main platforms which are used for integrated QKD and QRNG are: *silicon* (Si), *silica* (SiO_2), *silicon nitride* (Si_3N_4), *silicon oxynitride* (SiO_xN_y), *gallium arsenide* (GaAs), *aluminuim gallium arsenide* (AlGaAs), *indium phosphide* (InP) and *lithium niobate* ($LiNbO_3$). In the following, we provide a brief discussion on the advantages and disadvantages of each material with respect to their application.

Si

There are many reasons for working with Si. Namely, common fabrication technology with electronics, compact, relatively cheap and suitable for telecommunication wavelengths. Its compactness comes from the high refractive index contrast [16] of around 2.2 ($n_{Si} \sim 3.5$ and $n_{SiO_2} \sim 1.45$) [39]. The propagation loss of Si is typically 3 dB/cm [17]. In a usual silicon photonics PIC, SiO_2 composes the *buried oxide* (BOX). Components such as *thermo-optic phase shifter*s (TOPSs) and *electro-optic phase shifter*s (EOPSs), often placed in the arms of a *Mach-Zehnder interferometer* (MZI), as well as tunable microring resonators and *silicon germanium* (SiGe) photodiodes can readily be integrated. All of which are highly valued for most QKD and QRNG implementations. There are also reasons for not wanting to utilise silicon as integrated photonics platform. The monolithic integration of light sources and telecommunication wavelength detection is not possible using solely silicon photonics, due to its indirect bandgap. Fortunately, interest in hybrid or heterogeneous integrated solutions [18] of light sources and detectors is increasing [41]. Thus, when planning to integrate components of an experimental setup in silicon, one has to compromise on the non-integration of an eventual light source or single-photon detector. We suggest the review [45] for information on the current status of silicon photonics, as well as the various foundries producing such PICs. Most integrated QRNG works are based on Si [41], which thus are composed of off-chip lasers and detectors.

SiO_2

One of the main advantages of using a SiO_2 (silica) platform [19] is its extremely low propagation loss (usually < 0.05 dB/cm). Additionally, the coupling losses are very low (less than 0.1 dB), as the modes of the waveguides are large, and therefore match the fibre-optic modes well. A disadvantage of this platform comes from its relatively "large" footprint, due to its low index contrast (around 2-3 orders of magnitude smaller than that of the Si platform). Other disadvantages are the absence of active devices and low thermo-optic coefficient (one order of magnitude smaller

16. The refractive index contrast corresponds to the relative difference in refractive index of the core and cladding.
17. Lower loss has been achieved, for example 0.5 dB/cm of [44].
18. Meaning silicon in combination with another material.
19. The silica is grown on a silicon substrate.

than that of Si), in particular it has the lowest one of all the platforms that are discussed here. A method for inscribing waveguides in SiO_2 is through the femtosecond laser micro-machining technique. We recommend the work [46] for more information.

Si_3N_4

The silicon nitride platform [20] comes with advantages such as low propagation loss (typically < 1 dB/cm) and a large transparency window (visible to mid-infrared). Additionally, the hybrid and heterogeneous integration of laser has been presented in Si_3N_4 [47, 48]. A disadvantage of this platform is its low thermo-optic coefficient, compared to silicon it is around an order of magnitude lower. Thus any temperature controlled phase modulators integrated on-chip are slow and ineffective. The usage of the Si_3N_4 platform for the receiver of an integrated QKD setup could be exemplary, thanks to the low loss of the optical waveguides. For example, the work of [49], presented an integrated QKD receiver in this platform. Here, *superconducting nanowire single-photon detector*s (SNSPDs) were integrated on-chip. Additionally, the platform SiO_xN_y, the intermediate state of SiO_2 and Si_3N_4, has been used as receiver of QKD integrated systems [50, 51].

GaAs

The platform GaAs [21] carries a high refractive index ($n_{GaAs} \sim 3.67$ [39]) and thus a large integration potential. Most of the necessary ingredients of a complete quantum PIC can be integrated in its platform. Namely, single-photon sources (often via quantum dots), detectors, most passive components and rapid phase modulators. The latter comes from its large electro-optic effect. Additionally, its thermo-optic effect is the largest of all the presented material platforms [39]. The platform AlGaAs, with similar characteristics as GaAs, has been implemented in a hybrid QKD setup as an entangled photon-pair source [52]. Low propagation loss (< 0.2 dB/cm) has been proven in AlGaAs [53], however, its loss is typically around 2 dB/cm. For further information on AlGaAs and GaAs we suggest the works [54, 55].

InP

Together with Si, InP is one of the main platforms for photonics technologies. In terms of QKD and QRNG integrated systems, it is one of the few platforms that can host all active components. Meaning, laser, amplifier, detector, modulators and other passive elements. Similar to Si, InP has a high integration density ($n_{InP} \sim 3.2$ [39]). Additionally, this platform presents a high thermo-optic coefficient as well as the possibility to integrate high bandwidth electro-absorption modulators. The propagation loss of InP is around 1-3 dB/cm [41] [22]. As opposed to Si, whose integration process can be run by a CMOS foundry, the InP integration process is less established,

20. Grown on top of a silica substrate.
21. Usually placed on a silica or an AlGaAs substrate.
22. For example, proper confinement can be achieved by stacking the InP layer with a *iron* (Fe)-doped InP layer [56].

limiting thus its current scalability. Additionally, InP is a scarce compound, mainly due to the rare element indium. Hence, this already expensive platform will not be any cheaper in the future, limiting thus further its scalability and mass production. We recommend the work [57] for information on the status of the InP-technology. The works [50, 58–60] utilised an InP PIC for the integration of the laser, among other components, in QKD experiments. The work [61] is one of a few to have produced a QRNG setup based on InP.

$LiNbO_3$

Before being used as a material platform for integrated photonics, $LiNbO_3$ was, and still is, widely used for modulators, as bulk material. When integrated, $LiNbO_3$ is placed as a thin-film on an insulator (usually silica). This platform comes with many advantages, such as a high electro-optic effect, a large transparency window ($0.35 - 4.5$ μm) and low loss ($<$ 1dB/cm). Compared to Si, its refractive index contrast is not as high. For the integration of lasers and detectors, heterogeneous solutions are available [41]. The work [62] integrated a QRNG system on a $LiNbO_3$ platform. We refer to the work [63] for a review on the integration of lithium niobate on insulator.

1.3. Summary of chapters

The thesis is organised in the following way. Chapter 2 is dedicated to explaining the utilised QKD protocol and its experimental implementation. We start by presenting an example of a QKD protocol in 2.1, namely through the *Bennett-Brassard 1984* (BB84) polarisation-based QKD protocol [64]. Then we explain in section 2.2 how the QKD protocol used in this thesis works, notably the 3-state time-bin BB84 protocol with one-decoy state [65, 66]. Section 2.3 goes into detail about the implementation of this protocol in a fibre-based experimental setup [67]. Chapter 3 presents two fibre-based experimental QKD implementations, which the author collaborated on. In section 3.1, we present a variation of implementation of the aforementioned protocol, which is adapted to working alongside a strong classical channel through the usage of *wavelength division multiplexing* (WDM) [68]. Another variation of implementation of the protocol is presented in section 3.2, where the goal was to achieve a record-high *secret key rate* (SKR) [69]. This was done through the usage of a multipixel-SNSPD, among other developments and modifications of the experimental setup.

Chapter 4 presents the integrated QKD setup, which was developed and experimentally implemented to work with the aforementioned protocol. This work corresponds to the main focus of the thesis of the author [70]. Section 4.1 presents the integrated transmitter, based on silicon photonics. This includes discussions about its schematics, the working of the integrated components as well as characterisations of them. Section 4.2 presents two integrated receivers, based on silica and silica-on-silicon, respectively. We present their schematics as well as important characterisations of their respective components. The fully integrated experimental setup is presented in section 4.3 and the results of several SKR exchanges are presented in section 4.4.

Chapter 5 discusses a recently started project based on an integrated QRNG. In section 5.1 we begin by giving an introduction to *random number generator*s (RNGs). The applied QRNG protocol, a self-testing semi-device independent QRNG protocol [71–73] is then presented in section 5.2. The integrated QRNG experimental setup is presented in section 5.3. Here we introduce the integrated PIC based on InP, which hosts all the necessary optics. A set of preliminary measurements is presented in section 5.4.

Finally, a conclusion is provided in chapter 6, where we discuss the previously mentioned experiments and give an outlook on the future research in the group regarding integrated QKD and QRNG, as well as on their technologies in general.

2. Quantum Key Distribution Protocol and Experimental Setup

The need and motivation for QKD was established in section 1.1. In section 2.1, we will explain how it works, via the first QKD protocol proposal, named BB84, from its inventors Charles Bennett and Gilles Brassard in 1984 [64]. Further on, in section 2.2, the QKD protocol, *3-state time-bin BB84 with 1-decoy state* [65, 66], used in the research group and thus in this thesis will be presented, including its experimental setup [67]. This protocol corresponds to an improved version of the original BB84 protocol.

2.1. Bennett-Brassard 1984 protocol

2.1.1. Example of key establishment

As mentioned in section 1.1, a QKD protocol is used by two parties (Alice and Bob), to establish a secret key for preforming private communication. The BB84 protocol [64] will be used as an example of how to do so. Photons are the preferred choice of information carrier for both classical and quantum communication, since they are easy to generate and control, and can be sent over large distances. It is important to note the difference in number of photons per bit sent in classical communication and quantum communication. For example, in the former around 1 mW of power is sent at a rate of 10 Gbps, which corresponds to around 80'000 photons per bit, whereas in the latter no more than one photon per bit is sent.

Regarding the protocol we use here as an example [64], information is encoded in the photon polarisation degree of freedom. Encoding information means that one defines, for example, that the bit 0 is related to the *horizontal* (H) polarisation state and the bit 1 to the *vertical* (V) one and similarly for the *diagonal* (D) and the *anti-diagonal* (A) polarisation states. The states are noted: $|H\rangle$, $|V\rangle$, $|D\rangle$ and $|A\rangle$ in Dirac notation. The two latter polarisation states are defined as: $|D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$ and $|A\rangle = (|H\rangle - |V\rangle)/\sqrt{2}$. The two orthogonal bases in which the transmitter will encode the information are the linear basis, noted $+$, which includes $|H\rangle$ and $|V\rangle$ and the diagonal basis, $\times$, including $|D\rangle$ and $|A\rangle$. The bases, states and their corresponding bit values are summarized in table 2.1.

Basis	**Polarisation State**	**Bit**	
+	Linear	H	0
+	Linear	V	1
×	Diagonal	D	0
×	Diagonal	A	1

Table 2.1.: Encoding of photons in the BB84 polarisation-based protocol.

In the following it is assumed that Alice has access to single-photons. The making of a secret key starts with Alice, *randomly*[1], selecting the basis and polarisation state with which she will encode her first photon. Once the photon is encoded, she sends it off to Bob via a dedicated quantum channel, which can be an optical fibre or the free-space. She will do this subsequently for each photon, one by one. On Bob's side, as soon as a photon arrives, a choice between the linear and the diagonal measurement basis is done and a measurement is performed. The measured polarization and its corresponding bit value are registered. An example of what Alice sends and Bob detects is shown in table 2.2.

Chronological order	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Alice Basis	+	×	+	×	×	+	×	+	+	+
Alice State	H	A	V	A	D	V	D	H	V	H
Alice Bit	0	1	1	1	0	1	0	0	1	0
Bob Basis	×	×	×	+	×	+	+	+	×	+
Bob Measurement Outcome	D	A	D	H	D	V	V	H	A	H
Bob Bit	0	1	0	0	0	1	1	0	1	0

Table 2.2.: Example of the encoding of photons by Alice and the detection by Bob with the BB84 polarisation-based protocol.

As can be seen from table 2.2, when Bob does not choose the same measurement basis as Alice, the measurement outcome is completely random[2] (this is the case for photons 0, 2, 3, 6 and 8). The next step of the protocol is to perform *basis reconciliation*. Here, and from now on, the quantum communication is over and Alice and Bob communicate publicly via a service channel (for example, via a fibre containing classical communication or over the phone). In this step, Alice and Bob compare the choice of the measurement bases for each photon and if it does not match they get rid of the result, thus keeping only the measurements with identical measurement bases. At this point Alice and Bob have their *raw key*. This would look for example like in table 2.3.

1. Meaning in a completely unpredictable way. If this choice is not random, the security of the protocol is compromised.
2. Additionally, the measurement outcome is unrelated to what Alice sent.

Chronological order	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Alice Basis	+	×	+	×	×	+	×	+	+	+
Alice State	H	A	V	A	D	V	D	H	V	H
Alice Bit	0	1	1	1	0	1	0	0	1	0
Bob Basis	×	×	×	+	×	+	+	+	×	+
Bob Measurement Outcome	D	A	D	H	D	V	V	H	A	H
Bob Bit	0	1	0	0	0	1	1	0	1	0
Raw Key		1			0	1		0		0

Table 2.3.: Example of basis reconciliation between Alice and Bob. Measurements in the red boxes are thrown away and those in the green ones are kept to produce the raw key.

Once the raw key is obtained, there can still be discrepancies between the key obtained by Alice and the one obtained by Bob. This means that that even though the bases chosen by Alice and Bob are the same, Bob does not obtain the same bit as Alice. Such errors could come from, for example, eavesdropping attempts, noise in the channel/external environment or due to imperfect hardware. This noise is quantified in terms of *bit error rate* (BER), meaning that if the BER is 0, there are no bit-flips, and if it is 1.0, all the bits are flipped. More precisely, the BER can be defined as: BER $= \frac{e}{n}$, where e represents the bit errors and n is the total number of transferred bits, including the wrong bits. In the realm of QKD, the term *quantum bit error rate* (QBER), is employed. In order to assure that Alice and Bob have the same key, *error correction* is performed on the raw key. Now, an eavesdropper might still have some partial information about the key. Hence, a way to minimize this knowledge and so render the key as secure as possible is necessary. This is done through performing *privacy amplification*. Once executed, the key becomes a proper *secret key* and can be used without compromise for private communication between distant parties and for maximal security, in combination with OTP.

2.1.2. Error correction and privacy amplification

The goal of the error correction is to identify and correct all of the potential bit-flips in the raw key. The central difficulty when performing it, is to not to leak (and so disclose) too much information to a possible eavesdropper. It is not possible to not leak anything, therefore the leaked bits are disregarded in the next step in order for the resultant key to be still considered secure. For the main work in this thesis the error correction protocol used was Cascade [74]. The input of this protocol is the raw (noisy) key and it outputs a *corrected* key and the number of leaked bits. It works in the following way: Alice and Bob divide their key into blocks. For a given block they compare the parity of their respective block. If the parity is different, then an odd number of errors are present in the block of the raw key of Bob. A binary search is at this point performed within the block and the position of the error is exposed. This is done with all the blocks until they all have an even number of errors. Then, these blocks will be sub-divided to smaller blocks to again identify any odd number of errors and perform binary search to identify the error. This is repeated until, in principle, all wrong bits are flipped (corrected). The block

size is inversely proportional to the QBER. A large QBER will force a smaller block size and more blocks will thus be needed. However, the smaller the blocks the more the leakage, hence a low QBER is desired.

After the error correction has been executed, privacy amplification is performed. The goal here is to nullify (with an ϵ-probability of failure) the information that Eve has about the key (from the leakage during the error correction and possible eavesdropping). Using a two-universal hash function, the corrected key of Alice and Bob will turn into a *secret key* where the price to pay is the shortening of the key. The amount of shortening depends on the information Eve has. Now Alice and Bob share a secret key where the information that Eve holds is negligibly small.

2.2. 3-state time-bin Bennett-Brassard 1984 with 1-decoy state protocol

In this thesis, the employed QKD protocol is based on the one in section 2.1, with some modifications. The revisions are done with mainly simplicity and practicality of the experimental implementation in mind. The establishment of the protocol goes back many years (before even the author of the thesis started in the group) and its foundations are based on works [65–67] and doctoral theses [75–77]. In the following, this protocol, the *3-state time-bin Bennett-Brassard 1984 with 1-decoy state protocol*, will be explained.

2.2.1. Creation and encoding of qubits

First, it should be mentioned that photons are no longer supposed to come from a perfect single-photon source. Instead, weak coherent pulses and decoy-states [3] are used as they are much easier to produce. A pulsed laser and an attenuator are the sole two optical ingredients for a weak coherent pulse.

Previously, in section 2.1, the encoding of the bit was done through the polarisation degree of freedom. In the protocol used here, photons are instead encoded in *time-bins*. In this context, a qubit is defined to constitute of two time-bins, an *early* and a *late* one, where a photon lives in a coherent superposition of the two. Here the involved bases are the Z and X bases. The Z basis is formed of two states, $|0\rangle$ and $|1\rangle$, which are defined as follows:

$$|0\rangle = |\alpha\rangle_E |0\rangle_L , \tag{2.1}$$

$$|1\rangle = |0\rangle_E |\alpha\rangle_L . \tag{2.2}$$

3. Decoy-states are discussed in more detail in section 2.2.2.

E stands for *early*, L for *late*, $|\alpha\rangle$ for a weak coherent state and $|0\rangle$ for the vacuum state (the absence of a weak coherent state). Hence in the Z basis, the weak coherent pulse occupies either the early or the late time-bin. The states forming the X basis are

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tag{2.3}$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{2.4}$$

In this basis, the weak coherent state is in a superposition of both time-bins, with a defined phase difference (π or 0).

Given that the main medium for the transport of photons, used in the scope of this thesis and most of the previous works in the group, is optical fibre, encoding bits in time-bins is highly advantageous. Firstly, with this encoding no information is contained in the polarisation of the photon. Hence no active (nor passive) polarisation control is needed since, for example, polarisation mode dispersion has a negligible effect on the time-bin qubit. Also, simple measurements, like the time-of-arrival of the photons, can be performed to distinguish the early and the late pulse. Finally, there is in general little cross-talk in between the states of the qubit and it is straightforward to detect any loss [4].

So, how is a time-bin qubit created? The necessary ingredients are: a pulsed laser with frequency Y Hz and an imbalanced interferometer with delay line of length $2\frac{1}{Y}$ s. The laser pulses should have a uniformly distributed phase. This simple setup is represented in figure 2.1, where the imbalanced interferometer is a Mach-Zehnder one.

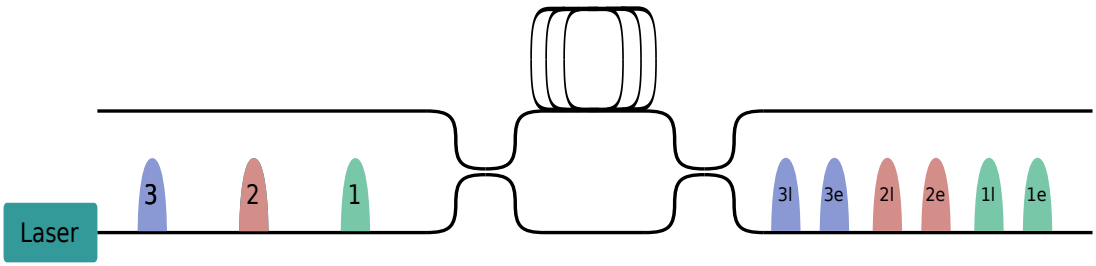


Figure 2.1.: Example of creation of time bin qubits, where e stands for early and l for late. The laser is pulsed. The numbers denote their chronological order of production and the pairs of numbers correspond to the two pulses constituting one qubit.

Thus, upon encounter with the first beam splitter, which has a perfect 50/50 splitting ratio, half of the pulse train will pass through the shorter arm and the other half, through the longer arm. This creates a train of pairs of pulses (qubits) as illustrated in figure 2.1. The pulse travelling

4. Since the time-bin is either occupied or not, which is also the case for polarisation encoded qubits, either the qubit is in one type of polarisation or not.

through the short arm corresponds to the one occupying the early time-bin and similarly for the long arm and the late time-bin. The phase between the states within the qubit is given by the phase of the interferometer and the phase between the qubits is random, as the laser is pulsed. As an example, let the laser be pulsed at 2.5 GHz, hence the separation in time of pulses 1, 2 and 3, entering the *imbalanced Mach-Zehnder interferometer* (imb-MZI), is 400 ps. Upon exit of the second beam splitter, the qubits produced are thus 1e and 1l, 2e and 2l as well as 3e and 3l. Given the repetition rate of the laser, the length of the delay line is most optimised when equal to 200 ps. Thus, the separation between the qubits (for example 1e and 1l and all the following pairs) is 200 ps in this case.

In the present protocol, detections of states in the Z basis constitute the raw key. Regarding the X basis, it is proven in [65] that only one of the two states is necessary. Hence the name of the protocol: *three-state* BB84. The state $|+\rangle$ is the one that is used. Detections of this state are used for verifying the security of the protocol. The intuition to why three states are sufficient, compared to the usual four, is that the information gained by a second detector in the X basis is redundant. In other words, knowing that no detections arrived in one detector implies that all the counts are in the other one, them being complementary to each other. Of course, simplicity comes with a price, which is to find a work-around to obtain all the necessary measurement results in order to estimate the phase error rate with only information from one detector. For the passionate reader, the works [65, 76–78] are recommended.

2.2.2. Decoy-states

Before going into the details of the experimental setup related to the protocol, important information regarding the usage of weak coherent states instead of single-photons should be acknowledged. As mentioned, due to the non-existence of a single-photon source with the characteristics necessary for the experimental setup [5], weak coherent pulses are employed instead. These are produced by attenuating a pulsed laser to single-photon level. If the attenuation is set such that on average one photon per pulse is sent, occasionally pulses with two or even more photons will be sent due to the Poissonian statistics of such a pulse. A critical issue that comes with this, is that when a multi-photon pulse is produced, Eve can get hold of one of the photons without Alice or Bob noticing. By storing the photon in a quantum memory until she learns the corresponding basis (from the basis reconciliation step) and make a correct measurement on it, Eve can obtain exact information about the state and so the key. Such an attack is called a *photon number splitting* (PNS) attack [79] and can be prevented by the use of decoy states. Without such states, the transmission distance or SKR would be heavily limited as an extremely low number of photons per pulse would be necessary.

Their usage works in the following way (in the case of one decoy state): Alice randomly sets the mean photon number of her photons to be either of two values, called a signal or a decoy state, such that the mean photon numbers of the outgoing photons from Alice to Bob are randomly one of the two values. By verifying the statistics of the mean photon number at Bob's, a potential eavesdropper performing a PNS attack can be identified. The idea of decoy states started with

5. Meaning pulses at high speed and high production efficiency.

works [80, 81], from 2003 and 2005, respectively, and has since been further developed [66, 82, 83]. The first security proof [81] required an infinite amount of intensities (decoys). Later on, in the work of [84], two decoys and one signal was found to be enough. The work in [85] then showed that for best performance, one of the decoys should be the vacuum state. They also studied the possibility of having only two intensities, one signal and one decoy (non-vacuum), called the 1-decoy protocol, which was found to perform less well than the 2-decoy state version (three intensities). However in the work of [66], the analysis of the 1-decoy method was refined and showed that for most experimental configurations, this method is the most favorable one [6], in terms of both performance and simplicity. The latter quality is because only two intensity levels have to be implemented. Therefore, the 3-state time-bin BB84 protocol with 1-decoy state is used. Figure 2.2 shows the states and their two intensities, that are implemented for the protocol.

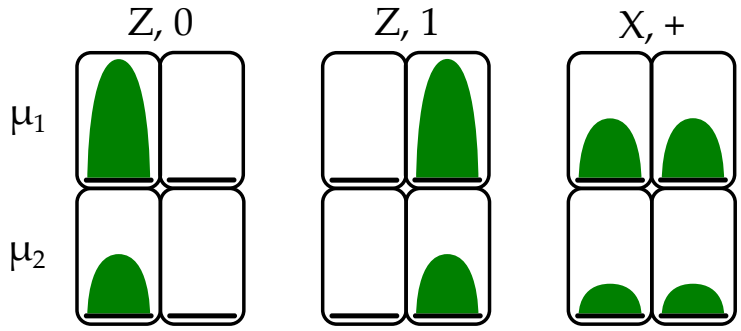


Figure 2.2.: Encoding of the states sent by Alice. Z and X are the bases in which the states $|0\rangle$, $|1\rangle$ and respectively $|+\rangle$, live. μ_1 and μ_2 correspond to the two mean photon numbers used for the 1-decoy state protocol [66].

2.2.3. Secret key rate formula

The security proof of the used protocol is based on [65] and the final formula for the SKR per privacy amplification block is based on the security analysis of the one-decoy state protocol [66] and given by

$$\mathrm{SKR} = \frac{1}{t}[s_0 + s_1(1 - h(\phi_z)) - \lambda - 6\log_2(19/\epsilon_{sec}) - \log_2(2/\epsilon_{corr})], \tag{2.5}$$

where t is the block acquisition time, s_0 is the lower bound on the number of vacuum events and s_1 that of the single-photon events, both in the Z basis, $h(\cdot)$ is the binary entropy defined as $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$, ϕ_z is the upper bound on the phase error rate, λ is the leakage of the bits during the error correction process and ϵ_{sec} and ϵ_{corr} are the secrecy and correctness parameters, respectively. They are both set to 10^{-9}. Next, the experimental setup associated with the explained protocol will be presented.

6. The 2-decoy state method has the advantage over the 1-decoy state one at either very high ($>$ 60 dB) or very low attenuations ($<$ 5 dB).

2.3. Fibre-based implementation

2.3.1. Experimental setup

The first implementation and usage of the 3-state time-bin BB84 protocol with 1-decoy state was in the work [67]. Since then it has been extensively used in different ways, for example, over long distances [86], in combination with classical communication [68] (see section 3.1), at extremely high secret key rates [69] (see section 3.2) and finally using integrated photonics [70] (see chapter 4). The full experimental setup of the protocol is depicted in the schematics of figure 2.3.

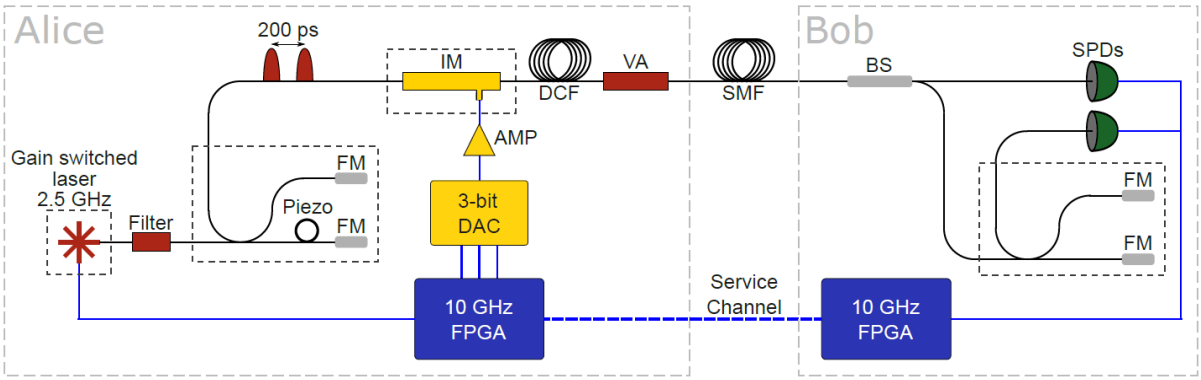


Figure 2.3.: Schematics of the experimental setup of the employed protocol [67]. FM = Faraday mirror, IM = intensity modulator, AMP = amplifier, DAC = digital-to-analog converter, FPGA = field programmable gate array, DCF = dispersion compensating fibre, VA = variable attenuator, SMF = single-mode fibre, BS = beam splitter, SPD = single-photon detector. Black lines correspond to optical fibres and blue lines to electrical connections. The service channel constitutes of a single-mode fibre. Dotted boxes means temperature stabilized.

Primarily, Alice and Bob have to be synchronized in time. This is done via *field programmable gate arrays* (FPGAs) [7], one on each side. They are connected via a "classical" fibre optic *service channel* (SC), which includes standard *small form-factor pluggable* (SFP) modules, at 10 Gbps, as represented in figure 2.3. The FPGAs are connected to one PC each and have many central tasks in the QKD setup. On Alice's side, the FPGA allows for the random choice of the states and their decoys and on Bob's side the FPGA takes care of sampling the detections. More precise information on the working of these tasks is given in the following text. Additionally, the FPGAs of Alice and Bob allow for sifting, error correction and privacy amplification, performed thanks to communication between them via the SC.

It should be noted that in the presented experiments the length of the SC was not as long as the *quantum channel* (QC) *single-mode fibre* (SMF) between Alice and Bob in figure 2.3. Actually the SC is more often only around 2 m, while the QC is in the order of hundreds of kilometers. Via the use of time-tracking throughout the secret key exchange, the temporal drifts of the two fibres can be balanced.

7. Xilinx, Kintex7

On Alice's side of the setup, the goal is to produce and encode single photons. For this, a gain-switched DFB laser [8] at around 1551 nm [9], with a repetition rate of 2.5 GHz is used to produce phase-randomised pulses. The latter means that each consecutive pulse carries a random phase. If no photons from the previous pulse resides in the laser cavity when switching the laser on [10], only photons from spontaneous emission will trigger the pulse, which will give rise to a random phase of each pulse. In the thesis of [75], their phase correlation was tested and concluded to be non-existent. The dotted box around the laser in figure 2.3 means temperature stabilised, which is important for the laser to keep its spectrum and power stable. Since the pulses coming from the laser are chirped, a narrowband filter is added to narrow their spectrum. The *full width at half maximum* (FWHM) of the pulses is around 30 ps.

The pulses then pass through a temperature stabilised *imbalanced Michelson interferometer* (imb-MI) with a delay line of 200 ps. A piezo controller is placed in one arm, allowing to alter the relative phase between the arms (by changing the path length difference). Hence, as shown in figure 2.3, qubits constituting of a pulse in the early and in the late time-bin, separated by 200 ps are produced. It is important to note that the intensity of the pulses should be the same at both outputs of the interferometer in order for the highest visibility (V) to be achieved. Therefore the loss should be the same in the two arms. The visibility is measured by changing the phase (using the piezo controller) and finding the maximum and minimum output power, while injecting a continuous wave laser in the imb-MI. A reduced visibility corresponds to an increase in QBER according to

$$\mathrm{QBER} = \frac{1 - V}{2}. \tag{2.6}$$

Additionally, a difference in loss of the two arms would correspond to distinct losses of the pulse in the early and the pulse in the late time-bin. Meaning that the states $|0\rangle$ and $|1\rangle$ would have different mean photon numbers. Yet, the mean photon number should be independent of the state.

The qubits then pass through an *intensity modulator* (IM), based on $LiNbO_3$ [11] (in the fibre-based version of the setup), where the three states (and their decoys) are randomly encoded, via the FPGA. The user can set the probability of Alice to choose a state in the Z or X basis, p_z^A and p_x^A, respectively, as well as the probability to choose the two decoys, p_{μ_1} and p_{μ_2}. The random bits, which are used to select the decoy and the state, come either from a QRNG (Quantis, IDQ SA) or a PRNG, which seed AES cores. It is important to note that since only three states are produced, only one IM is necessary, and not an IM and a phase modulator, as the phase of the state $|+\rangle$ does not need to be modulated at high-speed. However, the intensity modulator has to be driven at 5 GHz. This is done thanks to the high-speed driving electronics, notably the *digital-to-analog converter* (DAC) and the amplifier, AMP in figure 2.3. In the fibre-based version of the setup, the signals of the FPGA enter a programmable DAC (to define the amplitudes of the

8. Gooch & Housego AA0701
9. At 25°C, the laser is it 1550.92 nm.
10. By applying an electric pulse.
11. iXBlue (MXER-LN-10).

pulses) followed by an amplifier before entering the IM.

At the end of Alice's setup, *dispersion compensating fiber* (DCF) is placed to pre-compensate for the chromatic dispersion created during the trip from Alice to Bob. The chromatic dispersion of SMF at 1550 nm is around 17 ps km^{-1} nm^{-1}. Thus, given the high rate of the setup, and the spectrum of the filter of around 200 pm, at only a few tens of km the dispersion is around 200 ps, which would render completely impossible the exchange of key. The DCF used comes from Corning and has a negative dispersion of -130 ps km^{-1} nm^{-1} at the employed wavelength. Obviously it comes with an extra loss to the system. Luckily, this is not a problem on Alice's side as the pulses have to be attenuated to single-photon level and the loss due to the DCF takes a part of the total amount that is needed. The rest of the necessary loss, in order for the qubits to be at single-photon level, is taken care of via a *variable optical attenuator* (VOA).

Now the encoded qubits are ready to be sent off to Bob. This is done via SMF fabricated by Corning with loss of around 0.2 dB/km. The usage of fibre optics for the transmission of photons has several advantages. Firstly, it goes well in hand with time-bin encoding, as mentioned in section 2.2.1. Secondly, it allows the direction of propagation of the photons to not be limited to a direct line of sight, or even the weather, as is the case for free-space transmission. Lastly, it is highly convenient to use, as a huge part of the current classical telecommunications in between cities, countries and even continents is performed via fibre optics. Thus, the implementation of a QKD system in two buildings with access to a fibre optics network would be fairly smooth. This is, if the system is small, practical and essentially plug-and-play. The goal being for the user to plug in the QKD system to the fibre optics network as if they were plugging in a modem for internet connection.

Upon arrival at Bob's the qubits enter a passive beam splitter, whose splitting ratio corresponds to the choice of the Z and X basis. The part of the qubits that goes towards the Z basis will go straight to a single-photon detector, associated with the Z basis. Here, detections corresponding to the time-of-arrival of the photons will take place. A detection of a photon in the early time-bin is associated to the state $|0\rangle$ and bit 0 and a photon in the late time-bin is associated to the state $|1\rangle$ and bit 1. Errors detected in this basis are quantified via the Z basis QBER, noted q_z. It is defined as

$$q_z = \frac{e}{e + cc}, \tag{2.7}$$

where e stands for errors and cc for correct counts. A high q_z will increase the number of leaked bits (λ), according to the definition $\lambda = n_z f h(q_z)$, where n_z is the total number of counts ($e + cc$ in equation (2.7)), f is the error correction efficiency and $h(\cdot)$ is the binary entropy as defined in section 2.2.3.

The part of the qubits that goes towards the X basis will pass through an identical imb-MI to the one on Alice's side, before detection in the X basis single-photon detector. Supposing that the X basis state $|+\rangle$ passes here, by going through an identical imb-MI a second time, the pulses early and late composing $|+\rangle$ will each have a component that goes through the short or the long

arm of the imb-MI. This results in the production of three possible detection times, early-short (eS), late-long (lL) and a superposition of early-long (eL) and late-short (lS). Depending on the relative phase of the interferometers of Alice and Bob, the superposition state will undergo destructive or constructive interference [12] in either of the two output arms, respectively, as shown in figure 2.4.

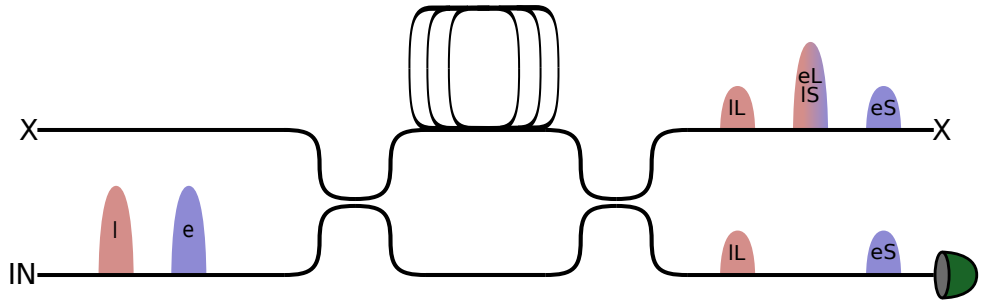


Figure 2.4.: Produced X basis measurement after going through a second identical imbalanced interferometer, where e stands for early and l for late, referring to the time-bin position and S for short and L for long, referring to the imbalanced interferometer arms. The interferometer presented is a Mach-Zehnder one.

The side peaks, seen in the arm without a detector, in figure 2.4 correspond to either a component of the early pulse passing through the short arm or the late pulse passing through the long arm. The central interfering peak corresponds to pulses early and late passing through the long and short arm, respectively. The relative phase of the imbalanced interferometers (of Alice and Bob) is set such that the central interfering peak is destructive at the output where a single-photon detector is connected, as shown in figure 2.4. We remark that only one of the two possible outputs at Bob's is monitored. The intuition to the security of the protocol comes from the non-expected counts in the destructive interference detector (the only one), which are associated with an eavesdropping attempt. More specifically, the errors in this basis are used to calculate a quantity called the phase error rate, ϕ_z, which is used in the SKR formula, equation (2.5), further information can be found in [65].

Another important feature of the implementation of the optics at Bob's, is that it is passive and independent of the polarisation. The latter referring to the initial splitting ratio as well as the imbalanced interferometer. Hence no active control of the polarisation is needed, which largely simplifies the setup. Actually, if for example the splitting ratio of the Z and X bases were dependent on the polarisation, Eve would have full control of the basis selection, and thus the secret key by controlling the input polarisation. In the fibre-based setup, a imb-MI was utilised for both parties, where Faraday mirrors were placed on the ends of each arm. Additionally, the loss of Bob should be as low as possible, as this directly relates to a reduction in the achievable key length.

The detections are sampled using the transceiver of the FPGA on Bob's side. Given the clock repetition rate of 2.5 GHz of our system, only 5 GHz sampling rate would be required. However, we (over-)sample and work at 10 GHz. In this situation, a detection window is defined in a

12. Or a mixture of the two.

time-bin duration of 100 ps. A qubit constitutes of four time-bins, where only two time-bins will contain any information. These bins are necessarily separated with 200 ps. Therefore every second time-bin can be discarded during sifting. This is advantageous in terms of robustness related to the uncertainties in the timing of the detection (see section 2.3.2).

In order to keep the SKR high, q_z and ϕ_z should be low, as according to equation (2.5). Factors that contribute to worsening these quantities are mainly: detector-based (see section 2.3.2) or linked to poor preparation of the states, meaning low extinction ratio between the different states or laser pulses with a high FWHM. Regarding the preparation of the states, the former effect will increase the number of false counts in the various time-bins, directly increasing the error rates. The latter will broaden the pulse, which will inevitably increase the errors in neighbouring, non-discarded, time-bins. This effect is amplified when in combination with a non-negligible timing-jitter of the detectors, further discussions are presented in section 2.3.2. Additionally, if the delay lines of the imb-MI at Alice's and Bob's are not precisely the same and the laser pulse is slightly chirped, an increase in ϕ_z will occur. This is because the interference at the imb-MI at Bob's is worsened, thus also the visibility (linked to the QBER via equation (2.6)). Therefore, substantial efforts are placed into making the delay lines the same length. The usage of a proper filter after the laser is also important to minimise the effect of the chirp.

2.3.2. Single-photon detectors

A crucial part of the QKD experimental setup are the *single-photon detector*s (SPDs). If the encoded qubits cannot be detected properly then a decent SKR will not be achieved and more interestingly, if detected well, a higher SKR can be achieved. What are then the demanded characteristics from such detectors in terms of a time-bin based QKD setup? The main requirement for the SPD is for it to be able to count individual photons, at the working wavelength (around 1550 nm). This means to be able to detect energies in the region of $1.3 \cdot 10^{-19}$ J, which is not a triviality even though it is a wide-spread technology today. Once this is confirmed, one can start to ask for characteristics that would help improve the SKR, these are: high detection efficiency, low dark count rate, low recovery time, little afterpulsing and low timing jitter. The details of each characteristic will be explained in the following when discussing the used SPDs.

Depending on the application and goal of the QKD experiment, one of two distinct types of SPDs are used in this thesis. These are either *single-photon avalanche diode*s (SPADs) or *superconducting nanowire single-photon detectors* (SNSPDs). Both can count single photons at the desired wavelength, however, they are quite different one from the other and therefore come with separate advantages and disadvantages. These, and brief comments on their working principles are explained next. More detailed information on their characterisations and functioning can be found in [87–89].

QKD with single-photon avalanche diodes

The essential goal of a SPD is to convert the very low energy of an incident photon to a detectable electrical signal. A SPAD manages to do this via the usage of a pn-junction, reverse-biased above

its breakdown voltage. A structure containing an absorption and a multiplication region is used. Upon arrival in the absorption region, if absorbed, a photon will create an electron-hole pair. In the case of *indium gallium arsenide* (InGaAs), the hole will drift to the multiplication region, where a high electric field will accelerate it. If its velocity is high enough, the hole will create a cascade of free carriers via impact ionization, which is called an avalanche. The avalanche will translate into an electrical signal, which can be discriminated via appropriate electronics. The absorption and multiplication regions can be based on different materials, depending on the application. In this thesis we use InGaAs for the absorption region, thanks to its sensitivity of wavelengths around 1550 nm and InP for the multiplication region. The detectors used for the discussed experiments (in section 3.1 and chapter 4) are based on works [90, 91], where the SPADs were operated in a free-running negative feedback mode.

Advantages of using such SPADs are the relatively easy-to-reach temperature at which they are operated. This means temperatures of around $-85°$C, achieved through the usage of a free-piston Stirling cooler (which can go down to $-130°$C). The SPADs present low dark count rates (around 100-200 Hz) and relatively low timing jitter (around 100 ps), corresponding to the uncertainty of the detector on the recorded time of arrival of the incident photon and thus the electric signal output. Disadvantages include the rather high afterpulsing probability, which corresponds to the creation of avalanches due to de-trapping of carriers originated during photon detection, as well as the not-so-high detection efficiency (around 20 %). The former will contribute to false counts in each of the bases, increasing thus the q_z and ϕ_z. Finally, the dead time, the time during which the detector is "off" (below breakdown voltage), will limit the maximum amount of countable detections. For SPADs, this value is relatively high (between 5-20 μs), as otherwise the afterpulsing probability will increase to non-sustainable values. The saturation rate of the SPAD occurs when the counts approach the inverse of the dead time.

All the previously mentioned characteristics are deeply interlaced, meaning that improving one will decrease the performance of another [13]. Hence, these parameters are carefully optimised depending on the distance (meaning the attenuation of the line and therefore the amount of counts arriving at the detectors) at which one works, as well as the splitting ratio of the two bases at Bob's.

QKD with superconducting nanowire single-photon detectors

As hinted by its name, SNSPDs consist of a thin nanowire, which is cooled down to its superconducting state [14] and biased close to, but less than, the superconducting critical current of the nanowire. The SNSPDs used in the presented works are based on either *molybdenum silicide* (MoSi) (work of [92]) or *niobium titanium nitride* (NbTiN) (used in work [69]). In brief terms, the conversion of the absorption of a photon to a measurable current is done in the following way (for more information, the interested reader is invited to read [88]). The absorption of an incident photon by the nanowire (often placed in a meander form) will create a non-superconducting

13. Example of trade-offs: $\eta \uparrow \implies$ DC and APP $\uparrow$, Temperature $\uparrow \implies$ DC $\uparrow$ and APP $\downarrow$, $V_b \uparrow \implies \eta$, DC and APP $\uparrow$, $V_b \downarrow \implies$ APP $\downarrow$. Where: η is the efficiency, DC = dark counts, APP = afterpulsing probability and V_b = bias voltage.

14. Meaning a temperature of around 7 K for amorphous *molybdenum silicide* (MoSi), but used at 0.8 K.

region (hotspot) with a fixed resistance (around 1 kΩ). This will redirect the current to the read-out electronics, producing hence a short voltage pulse that can be amplified and discriminated. Thanks to the short intrinsic thermal time constant of the material of the nanowire (a few hundreds of ps), it re-cools promptly, allowing all the current to flow back in (after a few tens of ns) and the system can once more detect.

Such detectors come with several advantages, notably, low dark count rates, high detection efficiency (typically around 80%), low timing jitter, negligible afterpulsing probability and low recovery time. The latter helps to increase the counting rate, further information about this can be found in section 3.2. It is therefore safe to say that SNSPDs are, in terms of performance, the best choice of detector for a QKD system. However, as there are no flowers without rain, SNSPDs also come with a disadvantage, namely, the complexity of the whole system. The temperatures needed for superconducting behaviour are cryogenic and hence highly sophisticated systems are necessary. Again, depending on the motivation of the QKD experiment, using SNSPDs might be a very suitable choice (like in the work presented in section 3.2). But, works whose motivations are simplicity, practicality and eventually the integration in real-world networks (for example the work in section 3.1 and the main work of the author in chapter 4) don't go hand in hand with SNSPDs. Thus, SPADs are used for these works and SNSPDs for their system characterisation, to understand their optimal performance.

Influence of detector characteristics on the SKR

The general behaviour of the SKR due to the detectors can be understood by the means of the graphs in figure 2.5.

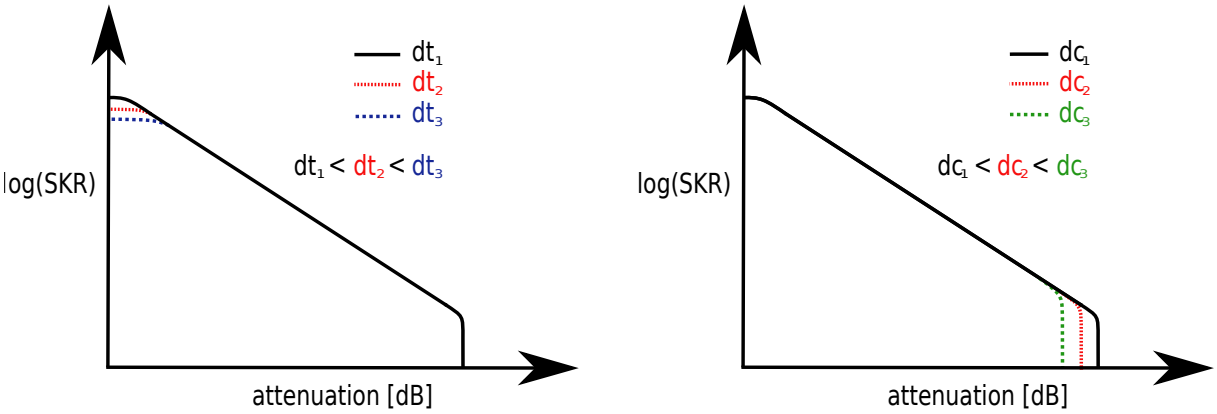


Figure 2.5.: Typical behaviours of the secret key rate as a function of attenuation when using a real set of detectors.

Looking at the black (filled) curve of the graph on the left hand side of figure 2.5, it can be concluded that at low attenuations, a saturation of the SKR occurs. This is due to the non-zero recovery time (or dead-time, noted dt in the graph) of the detectors. As a result, a part of the incoming photons will not be recorded. A higher dead time will result in a lower amount of counts before saturation. This will subsequently lower the detection efficiency and shift the

curve vertically down in this regime (i.e. red and blue curves, densely dotted and medium dotted curves, respectively, with respect to the black, filled, one).

Looking now at the black (filled) curve of the graph on the right hand side of figure 2.5, interesting effects appear also towards high attenuations. In this regime, a small amount of photons will arrive upon the detector until a cut-off occurs in the SKR. This is due to the constant amount of dark counts (noted dc in the graph). When the signal arriving at the detector is reduced, the signal-to-noise ratio will decrease to a point where the q_z and ϕ_z are too high to produce a SKR. A higher dark count rate will produce an earlier cut-off, which is illustrated with the red and green curves (densely dotted and medium dotted curves, respectively).

At "middle-like" distances, the SKR scales logarithmically with the attenuation, as in this regime the available SKR is proportional to the loss in the fibre-channel (around 0.2 dB/km).

2.4. Intermediate conclusion

The presented QKD protocol and its corresponding experimental setup display simplicity, thanks to an uncomplicated state preparation. Notably because only three states with two mean photon numbers are needed, which is enough to be prepared with solely one IM. Robustness of the state encoding over several hundreds of kilometers of fibre is also a meaningful characteristic, stemming from the time-bin encoding. Additionally, no active nor passive polarisation control is needed, as the encoding is completely independent of it. The polarisation independence of the various components (especially the beam splitter and the imb-MI at Bob's) should therefore be confirmed. Finally, thanks to the high clock rate, a high SKR is intrinsically achieved. It can thus be concluded that this implementation of the 3-state BB84 time-bin QKD protocol, with one-decoy state, consists of ordinary components brought together in an extra-ordinary way. Advocating that QKD is not far from being smoothly integrated in a real-world network.

Despite the simple state preparation, in the fibre-based version of the experimental setup (see section 2.3.1) particularly expensive components (amplifier and DAC) are needed in combination with the IM for the encoding of states. Regarding the imb-MIs on Alice's and Bob's side, as mentioned in section 2.3.1, their delay lines should be the same for best performance. In the fibre-based implementation, the imb-MIs were in-house-made. It is not trivial to manually obtain the exact same delay line lengths, as it is a matter of measuring and cleaving incredibly precisely [15]. Even though all concerned workers in the laboratory managed this task well, the production of the fibre-based imb-MIs does not ease much with quantity and its reproducibility is not guaranteed. Concerning the polarisation independence of Bob's imbalanced interferometer, the solution of using an imb-MI is excellent as the two Faraday mirrors perfectly compensate any polarisation rotation created in any of the arms.

Improvements of the implementation of the mentioned protocol are hence needed in order to obtain a setup that is even more practical and easy to use in real-world networks. Managing to bring this fibre-based setup towards an integrated one was the main motivation of this thesis.

15. Within the millimeter.

Discussions of different integrated platforms and their advantages and disadvantages are presented in section 1.2 and how this protocol was implemented to an integrated one, in chapter 4.

In order for this protocol and its implementation to be widely used in a real-world telecommunications network, other obstacles than performing photonic integration are still to be surpassed. Notably, the questions of how to combine quantum and classical communication in the same fibre, as well as, of how to generate ultra-high secret key rates. Discussions and proposals of the two are found in chapter 3.

3. Fibre-based implementations

This chapter will present works, of which the author of the thesis collaborated, that are based on the described protocol and whose goals were to address issues related to implementing the presented QKD setup (section 2.2) in a real-life network. In particular, issues involving the co-existence of a quantum channel with a classical one, which is an important problem to tackle when wanting to marry QKD systems and current fibre-based networks (presented in section 3.1). As well as the concern of SKRs, more precisely, in a more and more connected world, the rate of secret keys has to follow to reply to the needs of the current systems. Further discussions are found in section 3.2.

3.1. Combining quantum and classical communication

This section is based on the paper [68]. One of the main goals when developing a QKD system is to make sure it can be used in a real-world network. The QKD system presented in section 2.3.1 is fibre optics based, as is a huge part of the telecommunications network around the world. Therefore it would not seem too complicated to plug in this type of system in an existing network node [1]. Actually, already in 2009 a long-term QKD system was setup for over 1.5 years in the Geneva-area [93]. For this experiment, dark fibres, i.e. fibres solely dedicated to the transmission of quantum information, were used in between the different nodes. This means that no other classical communication can take place in these fibres whilst being used for QKD. Blocking an entire optical fibre in between two important nodes is incredibly expensive for the networking company [2] as other fibres would have to be installed to be used for other clients or simply less amount of clients can operate with their fibres. Also, actively placing a new fibre dedicated for quantum communication is also very expensive. Therefore a solution on how to combine quantum and classical communications in the same fibre needs to be thought of. Before briefly going into the current proposed solution [68], it is important to understand why it is complicated to combine classical and quantum communication in the same optical fibre.

The fundamental reason is that the average power of a channel in classical communication is around 1 mW, whereas in quantum communication, this value is less than 1 nW. Only a tiny fraction of the classical power, corresponding to noise from the quantum channel's perspective, is needed to worsen the quantum signal. A degrade in the quantum signal corresponds to a higher QBER, which, if high enough, would eventually hinder a secret key to be produced. Therefore,

1. For this, the QKD system in question has to first be plug-and-play, meaning that it should be brought in to a box as opposed to taking the space of an entire table, an ongoing project of the group, by Pereira et al.
2. Swisscom in the case of [93].

the dominant physical issues related to the high classical power and low quantum one and their precautions have to be studied.

For the sake of clarity, regarding the rest of the discussion, it is important to mention that information in a classical communication network is usually combined via WDM. For example, via *dense wavelength division multiplexing* (DWDM), where information is encoded in close neighbouring channels. Following the *International Telecommunication Union* (ITU), the standard 100 GHz or 0.8 nm spacing is used [3]. There are also standards, from the ITU, that define the band (the range of wavelength) in which a collection of channels are placed. The two main bands that are examined for our purpose are the original, the O-band situated between 1260 nm and 1360 nm and the conventional band, the C-band, accommodating wavelengths from 1530 nm to 1565 nm. The O-band is characterised by low chromatic dispersion and higher propagation loss compared to the C-band, which is defined by its low propagation loss. When combining a quantum channel with a classical one, an important decision to make is to choose in which channel band to place the two channels. It was decided to place the quantum channel in the O-band and the classical channel in the C-band. The reasoning will become clear from the following.

The first and perhaps the most obvious physical issue is the one of inter-channel cross-talk. This means noise due to non-perfect isolation between the channels, which can easily be solved by using proper filtering, namely using *coarse wavelength division multiplexer*s (CWDMs) [4]. Another source of noise is due to Brillouin scattering. Fortunately, a separation of two DWDM channels between the channels in question, allows this noise source to become negligible. Additionally, spontaneous four-wave-mixing could create noise in the O-band from the C-band, however it is found that the effect is negligibly low [77]. The main noise contribution is hence from Raman scattering. It was found that the scattering cross-section in the O-band was 10^3 times lower than in the C-band. Given that the Raman noise is much lower in the O-band, it might be tempting to assume the choice of quantum and classical channels in the O- and C-band, respectively, to be the most favourable. However, this choice also depends on the distance and the amount of classical launch power, as will be mentioned later on.

It was also established that having the classical and quantum channel co-propagating would improve the resilience to the Raman noise (as opposed to having them counter-propagating). In the co-propagating case, for a fixed classical launch power, the Raman noise will increase with the distance until a maximum noise contribution is achieved. At this point the fibre is long enough for the Raman scattering to create a lot of noise, but short enough for the classical signal to not suffer excessively from propagation loss in the fibre. At further distances, the Raman noise will decrease for two reasons. Firstly, the amount of Raman scattering will be less and less from this point, due to the decrease in the classical power, from propagation loss. Secondly, the Raman noise created in the initial part of the fibre will experience propagation loss, thus less of this noise arrives at the quantum detector.

In the counter-propagating scheme, for a fixed classical launch power, the Raman noise will follow a similar behaviour to that in the co-propagating case for short distances. However, when a maximum is reached in the aforementioned case, the Raman noise will continue to increase in

3. ITU-T G.694.1
4. They correspond to the multiplexing of channels separated by 20 nm, from 1270 nm to 1610 nm.

the counter-propagating case, until a certain distance. From this distance and further, the noise experienced by the quantum detector will increase asymptotically. This is because the additional Raman noise created beyond this distance will be low, due to the lower classical power available. Additionally, the noise will experience propagation loss when travelling back to the quantum detector. Hence, the contribution of Raman noise at further distances is negligible, and therefore the Raman noise increases asymptotically after a certain distance. For further discussions, we suggest the thesis [77].

The work in [68] thus implemented the protocol explained in section 2.2 with the quantum channel in the O-band and the classical channel in the C-band. Two separate situations were studied for the secret key exchange. One consisted of placing 51.5 km of SMF with 15 dB of excess loss in the channel, in order to simulate a real-world network where losses due to deviation of amplifiers and various fibre connectors occur. The other one consisted of placing 95.5 km of SMF and was performed in order to compare this work with previous studies. The maximum classical launch power was 16.7 dBm in the former case and a SKR of 172.2 bps was achieved. In the latter case, the numbers were 8.9 dBm and 42 bps, respectively, corresponding to state-of-the-art *discrete variable* (DV)-QKD performances using DWDM. The detectors used were free-running InGaAs/InP negative-feedback avalanche diodes (detection efficiency of 25% and temporal jitter of 50 ps at -85° [68, 90]).

It should be noted that many combinations of distances, classical launch power and channel band-placement will question the choice of the quantum channel in the O-band and the classical one in the C-band. The works [94, 95] achieved a successful SKR exchange with both the classical and the quantum channel in the C-band [5] and that works [96–98] used, similarly to [68], the quantum channel in the O-band and classical one in the C-band. However, it could be concluded that above a threshold of around 0 dBm of classical pump power at distances around 50-100 km the choice of this work [68] is the most suitable one in order to have the highest SKR [98].

Interestingly one of the main hurdles of the experimental setup was the non-optimal filtering. Indeed, with a filter after the laser on the transmitter side matching the one at the receiver, a higher classical launch power could have been accepted. A *fibre Bragg grating* (FBG) filter was first placed at the transmitter, but it was removed as it was found to be chirped. Since our laser is already slightly chirped, their combination, with the existing detector timing jitter, would lead to a higher probability of counts outside the detection window, which is equal to loss. Thus, no filter was placed at the transmitter and a FBG filter was only placed at the receiver [77].

Therefore, it can be concluded that using a QKD system like this one is not far away from being readily implemented in a real-world network. Of course, a smoother implementation would use integrated photonics as opposed to fibre-based optics for reasons such as uncomplicated handling and installing, lower power consumption and straightforward mass-fabrication. To the knowledge of the author, there has never been any work done on an integrated QKD system with coexisting classical and quantum channels. Works of [99, 100] have performed secret key exchanges with multiple channels via integrated platforms using WDM. Demultiplexing was done through ring-resonators in [99] and through the usage of imb-MZIs in [100]. However, in both works all the multiplexed channels were dedicated for quantum communication, leading to

5. It is interesting to study the classical channel launch power and distance linked to each SKR of these works.

higher secret key rates, as well as potential multi-user operation but no classical communication was sent. Therefore, these works did not address the problems of combining a strong and a weak channel over the same fibre. Nevertheless, integrated photonic circuits have been produced with the capacity to multiplex and demultiplex channels in the O- and C-band [101–103]. It is therefore yet to be confirmed if such PICs could be used for QKD coexisting with classical communication. One important figure of merit for such a PICs to make the scene is the channel cross-talk. Recalling that only a fraction of the classical power is needed to worsen the QBER, an excellent channel isolation is hence needed [6]. For now, the found integrated works present a maximum extinction ratio of only 23 dB.

3.2. Maximising the rate of secret key generation

This section is based on the paper [69]. Again, the goal being to use QKD in a real-world network, the question of how fast such a system can generate secret keys is important to examine. Depending on the application, a certain minimum threshold of secret key generation is required. For example, the US federal communications commission suggests a download rate of 6 Mbps during an encrypted video conference [7]. If one would combine the SKR generated with OTP, for total information-theoretical security, a SKR of 6 Mbps per user would be needed. Therefore there is solid motivation to work towards providing high secret key rate systems. Prior to the work in [69], 14 Mbps SKR over a distance of 10 km of SMF was the record [104]. Hence the goal of this work was to see if the record could be broken and to what extent the SKR can be improved.

The protocol and experimental setup that was used was again the fibre-based version presented in 2.2. However, in order to obtain extremely high-secret key rates there are few changes on the receiver side that have to be done to fulfill the new stringent criteria. The first one resides on the SPDs, as they have to be able to count at extremely high count rates. This means they should have a short recovery time, whilst still having a low timing jitter and high detection efficiency. Secondly, the rate of sifting and the speed of the readout electronics are required to increase, according to the higher detection rate. It is reasonable to demand this as it is not useful developing fast-counting detectors when its readout nor its sifting can follow. Finally, for the same reason, fast post-processing and real-time privacy amplification, adhering to the speed of the previous elements are equally a must-have. In the following, some details on the first criteria (the development of the fast counting detectors) will be presented. For the interested reader, specifics on the resolution of the other criteria can be found in [69] and [77].

On the optical side of the experimental setup (figure 2.3), two main physical changes on the receiver side were done. One, regarding the splitting ratio between the Z and X bases. Since the goal is to have a high amount of key, the splitting is now heavily biased towards the Z basis, thus a 99/1 (Z/X) splitting ratio is employed. Given the high detection rate, 1% of the detections is enough in the X basis in order to keep the signal-to-noise ratio acceptable, thereupon keeping the phase error rate (ϕ_z) low. The other change concerns the SPDs, where details about the

6. In the work of [68] almost 200 dB isolation was achieved with a cascade of CWDMs and filters.
7. https://www.fcc.gov/consumers/guides/broadband-speed-guide

extremely fast counting Z basis detector will be given in the following.

The SPDs used are SNSPDs in a multi-pixel configuration. They are in-house-made by the detector-side of our group [8], in close collaboration with IDQ. The superconducting material of the Z basis detector is NbTiN, whose operating point is at 0.7 K. The multipixel configuration of this detector refers to 14, independently biased, pixels, placed in an interleaved configuration. As mentioned, to count at high rates, the detector is required to have high efficiency and short recovery time. Additionally, low timing jitter would increase the detector performance. To achieve this, the idea of an interleaved geometry was thought of. The two main reasons for its advantage are explained in the following. Firstly, this configuration allows all pixels to have close to the same probability to be illuminated, which would maximise the count rate. Secondly, since this multipixel detector covers the same area (around 200 μm^2) as that of a singlepixel SNSPD, the length of each nanowire is reduced and so the recovery time and timing jitter is better [9]. Actually each pixel takes less than 8 ns to go back to full efficiency, allowing hence for ultra-high count rates, above 80 % efficiency at 400 Mcps [105].

The experiment was performed at two distinct working points of the detectors. One at a fibre distance of 100 km, hence at a lower count rate and the other one at extremely high count rate with only 10 km of fibre. At the former working point, an extraordinarily low timing jitter of 36 ps was achieved. At the the latter working point, the detector was pushed to its limit and a count rate of around 330 Mcps was achieved whilst keeping the timing jitter to only 58 ps and the efficiency high (around 63 %). The final SKR obtained at this working point was 63.6 Mbps, which is a new SKR record for a QKD system [10].

The presented work shows that QKD systems can be well optimised for high secret key rate implementations. The work in [69] should be considered as a reference mark and a proof of principle. However, for now, in order to implement QKD systems in a current real-world network, they should ideally consist of standard 19" racks that are WDM-compatible. The first step of trying to fit a system in such a rack is to miniaturise the whole experimental setup as much as possible. The following chapter goes into detail about the integration of a QKD system, more specifically, the one used here (in section 2.2). This corresponds to the main work of the author of the thesis.

8. Meaning: Giovanni Resta, Matthieu Perrenoud and Lorenzo Stasi.

9. The recovery time is proportional to the kinetic inductance of the created RL circuit when a photon strikes the active area and a hotspot is created, breaking the superconductivity. The time it takes to deviate the current to the read-out circuit is of the order of L/R. Shortening the length, allows for a lower kinetic inductance (L_K), which is actually proportional to the length of the nanowire from: $L_K = \frac{m_e}{ne^2}\frac{l}{A}$, with m_e the effective mass of the electron, n the carrier density, e the electron charge, l the length of the conductor (the nanowire) and A the cross-sectional area of the wire.

10. The work [106] published simultaneously a paper giving evidence for high-SKR QKD with rates over 110 Mbps using a polarisation-based BB84 protocol, implemented with an integrated transmitter.

4. Integrated Quantum Key Distribution System

4.1. Integrated QKD transmitter

4.1.1. General requirements for the transmitter platform

Motivations regarding the conversion of the fibre-based transmitter, whose schematics are presented in figure 2.3, to an integrated one, are many. One of the most important reasons is the general reduction in size and the integration of the expensive and cumbersome electronics (DAC and amplifier) for the state modulation. As will be presented in section 4.1, the imb-MZI and the IM, including its required electronics, are integrated on a photonic or an electronic integrated circuit, respectively. Meaning that components such as: external temperature controller, piezo controller, fibre-based temperature-stabilised interferometer, fibre-based IM, DAC, amplifier (the two latter with a control *printed circuit board* (PCB)) and power supplies for all components are now replaced with: an integrated PIC and EIC, controlled with a PCB. The laser is kept external as it is complicated to integrate it in the chosen platform. Given the huge step down in size, cost and number of components, the trade-off of keeping the laser external is permitted. Furthermore, regarding the required characteristics of the transmitter of this protocol, a high-speed production and encoding of qubits in an accurate manner is essential. Hence, this has to be kept in mind when choosing the integrated transmitter platform.

4.1.2. Silicon based integrated transmitter

The transmitter PIC used for the QKD protocol is based on silicon photonics and was developed in collaboration with Sicoya GmbH. It consists of a PIC and an EIC, both glued and bonded to a first PCB, hosting the two ICs, as can be seen in figure 4.1. The sizes of the PIC and the EIC are 4.50 mm $\times$ 1.10 mm and 4.50 mm $\times$ 0.75 mm, respectively. The advantages of using silicon as material for the ICs are many (as mentioned in section 1.2). Most importantly, the expensive electronics that were used in the fibre-based setup (see section 2.3.1) are now on-chip. Therefore a high component density is achieved, leading thus to a small footprint. The PCB shown in figure 4.1 is bonded and glued to a larger one (named *Alice printed circuit board* (APCB) in figure 4.17). The intention of this PCB is to provide the control and the interface between the chip and a computer of the different components of the PIC. It is additionally in-house-made. As can be seen from figure 4.1, a grating coupler and a fibre array assures the coupling of light in to the PIC, more details are presented in 4.1.4.

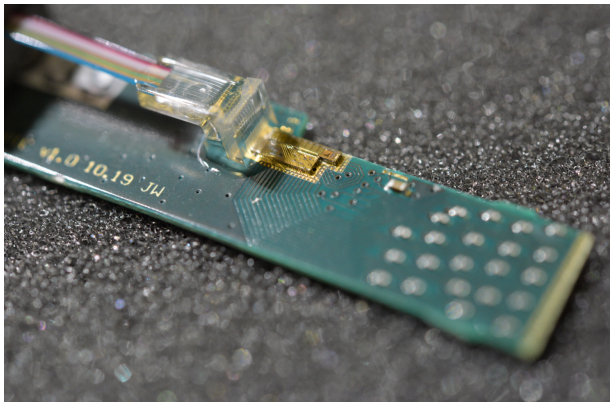


Figure 4.1.: Photo of the transmitter integrated circuit in silicon photonics.

4.1.3. Structure of transmitter

Figure 4.2 presents a practical scheme of the transmitter PIC. It should be noted that the input and output are on the same side, as according to the image in figure 4.1, but drawn here on separate sides for clarity.

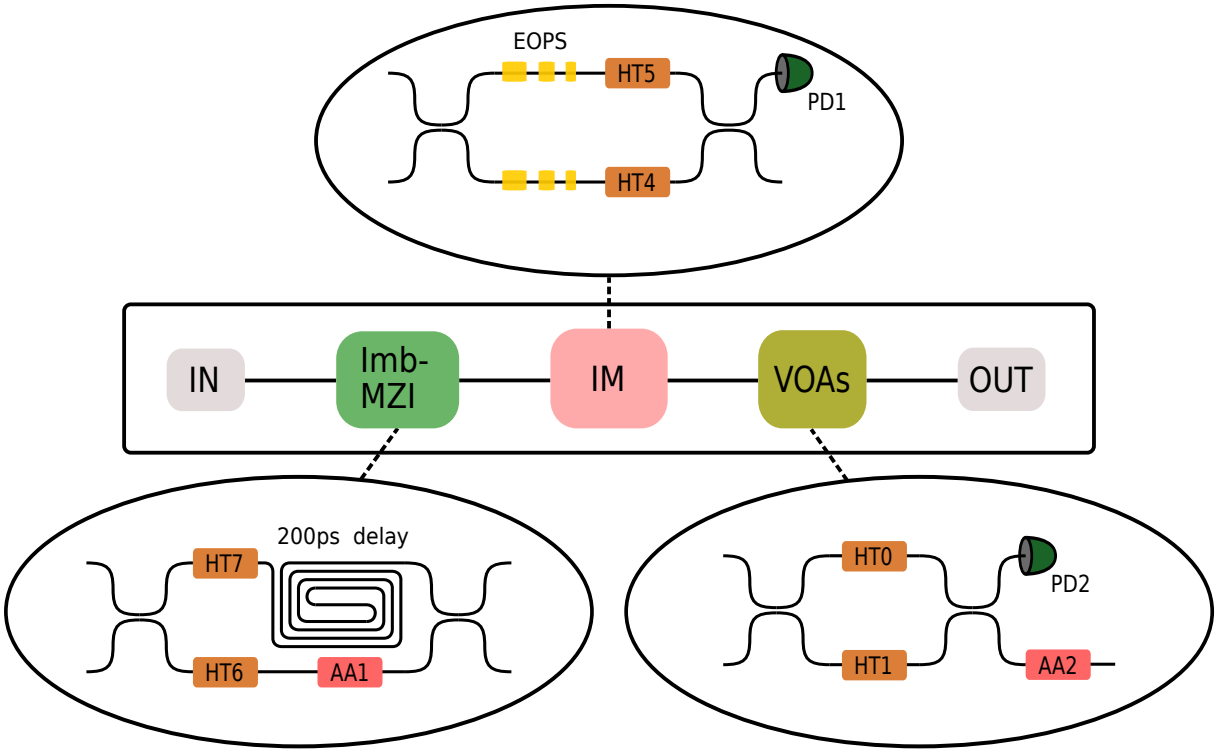


Figure 4.2.: Structure of the integrated transmitter circuit. Imb-MZI = imbalanced Mach-Zehnder interferometer, IM = intensity modulator, VOAs = variable optical attenuators, HT = heater, AA = absorption attenuator, EOPS = electro-optic phase shifter, PD = photodiode. The lengths of the three EOPSs are 200 μm, 400 μm and 600 μm.

According to the utilised protocol, pulsed light at a repetition rate of 2.5 GHz will enter the transmitter PIC, whose structure is presented in figure 4.2. The first component that the stream of pulses passes through is the imb-MZI. The delay line of the imb-MZI is 200 ps long, in accordance with the qubit repetition rate. The shorter arm of the imb-MZI includes an *absorber attenuator* (AA), noted AA1 in figure 4.2. Its goal is to achieve identical loss in the two arms of the interferometer, in order to maximise the visibility of the imb-MZI. In each arm of the imb-MZI there is a *heater* (HT), or more specifically a TOPS, HT7 and HT6 in figure 4.2. They are used to set the relative phase between the imb-MZIs of the transmitter and receiver. It should be noted that only one of the two are used at a time. As discussed in section 2.3.1, upon exit of the imb-MZI, qubits formed of two weak coherent pulses separated by 200 ps are produced. Next, these qubits enter the intensity modulator, formed by a *balanced Mach-Zehnder interferometer* (bal-MZI) with EOPSs and a heater in each arm. Three distinct EOPSs are needed in order to create the full combination of states for the protocol in a linear independent way. The difference of the three is based on their length and therefore on their range of phase modulation [1]. Each EOPS can be actuated individually, as they are all connected to the analog driver circuit on the EIC via wire bondings. The heaters HT4 and HT5 adjust the working point of the IM. Lastly, light passes through variable attenuators. A first one, which is based on a bal-MZI with a heater in each arm (HT0 and HT1) to change the phase of the light and so decide how much continues to flow towards the output of the PIC. A second one corresponds to an identical AA as in the imb-MZI, namely AA2. Two *photodiode*s (PDs) are also present in the chip, one after the IM and another one close to the exit (PD1 and PD2, respectively). Their purpose is to monitor the quantity of light present in the PIC.

The total loss of the PIC, including coupling loss, is 27.1 dB and for testing purposes it is possible to enter via an input that bypasses the imb-MZI, arriving thus directly at the IM. Entering from here gives rise to, at minimum, 20 dB loss. The relatively high loss is absolutely not a problem on this side as the qubits have to be attenuated down to single-photon level before leaving to the receiver (Bob), more information is given in section 4.3.

4.1.4. Working principle of the transmitter components

Working principle of grating coupler and waveguide

The first component that has to function properly in order for the PIC to be exploitable is the coupling of light from a SMF to the PIC, and vice versa, without an excessive amount of loss or major modification of the mode or other properties of the light. It is notably important here as the laser is off-chip. The core in which light travels from the laser is the core of a SMF, which has a diameter of 9.3 μm. The integrated waveguide has dimensions of: $h = 220$ nm, $w = 450$ nm. Thus, given the difference in the size of their cores (around one order of magnitude), it does seem quite a challenge to couple the light from one to the other (without an excessive amount of loss) and a clever way to do so is needed. Luckily, this has been thoroughly studied, particularly via usage of a grating coupler [107–109]. Here, an off-plane (vertical) grating coupler is used.

1. A given EOPS will thus give rise to a specific amplitude modulation at the output of the bal-MZI of the IM.

In general terms, a grating coupler manages to couple light from a SMF to an integrated circuit by the means of a varying periodic structure, called grating, made either by etching or deposition. The varying property throughout the structure is the refractive index. The Bragg (or phase-matching) condition describes which order of diffraction allows for coupling of light into the PIC (or inversely), for more information about grating couplers with silicon photonics, refer, for example, to the work [110].

A fibre-array consisting of several SMFs are coupled into the chip. A visualisation of the fibre array unit mounted on the PIC is given in figure 4.3, where it can be seen that the vertical grating coupler manages to change the incoming direction of the light to in the in-plane waveguide direction. Standard SMFs are connected to the fibre-array via an *multiple-fibre push-on/pull-off* (MPO) connector [2]. Photos of the chip with and without its connector is shown in figures 4.4a and 4.4b, respectively.

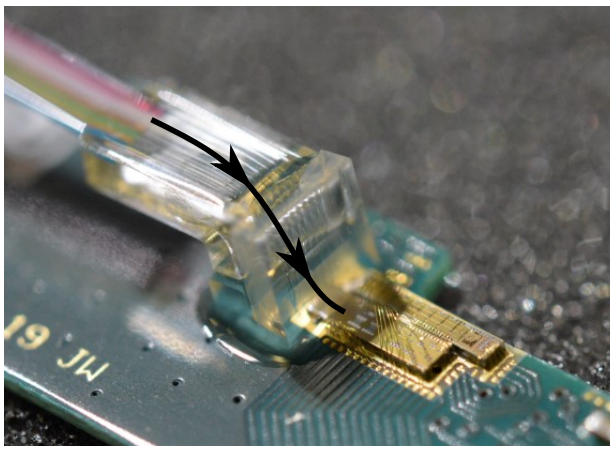
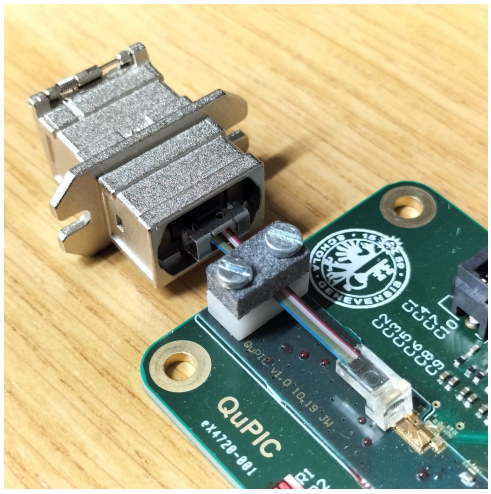
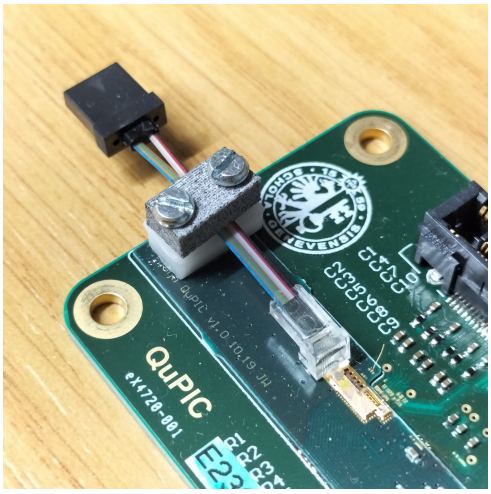


Figure 4.3.: Photo of the vertical fibre array unit of Alice and added arrows to visualize the flow of the incoming light from the fibre array to the PIC.



(a) Photo of fibre array with Molex MPO connector.



(b) Photo of fibre array without connector.

Figure 4.4.: Photos of PCB and PIC of transmitter.

2. Molex MPO connector.

In general, disadvantages of the used grating coupler are its relatively high loss and its sensitivity of wavelength and polarisation. With respect to the usage of the PIC in the QKD setup, these are not major issues as the wavelength of the laser is constant (around 1551 nm), the temperature of the laser is carefully stabilised (at 30°C) and a polarisation controller is used before the input of the PIC (see section 4.1.5). According to the manufacturer (Sicoya GmbH) the coupling loss of the grating coupler is 2.7 dB.

To finalize this subsection, a few words will be said on the confinement of light in the PIC. In the most intuitive way, confinement of light in a SMF is done by fulfilling the condition of total internal reflection, described by Snell's law. This means that a high refractive index core is surrounded by a low refractive index cladding. The same idea is followed for the confinement of light travelling through waveguides in a PIC. In this particular case, the waveguide is based on a rib structure, as shown in figure 4.5. Light travels through the rib waveguide, in silicon ($n_{Si} \sim 3.5$), under which a BOX layer in silicon dioxide ($n_{SiO_2} \sim 1.44$) is placed. The same oxide is also on top of the waveguide. The bulk silicon wafer substrate is placed under the BOX. The high refractive index contrast leads to a high mode confinement.

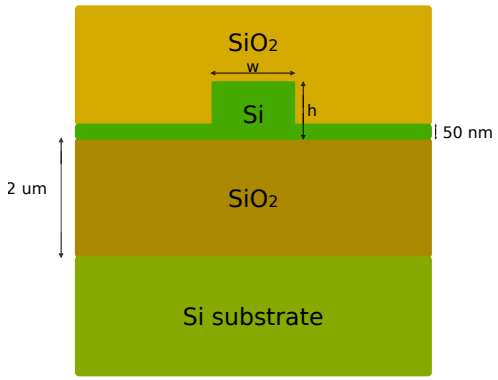


Figure 4.5.: Rib structure of the waveguides of the transmitter PIC, where w corresponds to the width of the core of the waveguide and h the height of it. Si = silicon and SiO_2 = silica.

Working principle of thermo-optic phase shifter

The goal of a TOPS is to control the phase of the optical signal in the PIC. In general they work at relatively low speeds (1-10 kHz), which is not a problem in this particular usage case as the phase control does not have to be monitored at high frequency. Additionally, such components come with low loss, which is in most cases an advantage.

The working principle is based on a temperature change of the waveguide resulting in a change of refractive index and therefore a change in phase of the propagating light. Given the thermo-optic coefficient of silicon ($\frac{dn}{dT} \sim 1.8 \cdot 10^{-4}$ K^{-1}), L, the length of the TOPS and λ, the working wavelength ($\sim$ 1551 nm), the change in phase ($\Delta\phi$) for a change in temperature (ΔT) is

$$\Delta\phi = \frac{2\pi L}{\lambda}\frac{dn}{dT}\Delta T. \tag{4.1}$$

The small distance between the waveguides in question (due to the small footprint of the PIC) gives rise to the concern of cross-talk of a TOPS on a neighbouring waveguide due to heating. From the formula in equation (4.1), increasing the length of the TOPS will decrease the necessary temperature change for a given phase change, which will decrease the lateral cross-talk. However, the device's footprint, loss and V_π [3] will follow proportionally to L, hence a trade-off has to be decided upon. In order to not heat up neighbouring waveguides, a solution is also to use deep trenches for thermal insulation and to maximise the distance between the components (few 100-200 μm) [4] [111].

In order to change the temperature of the waveguide, in silicon photonics two main approaches are used, either via the usage of a resistive metal, usually *titanium nitride* (TiN), placed above/near the waveguide, which will heat up the surrounding area when current is sent through (via Joule effect) or by using highly doped or salicided Si-strips placed at both sides of the waveguide. The approach used in this work is based on the latter one with highly doped resistive Si-strips. They are placed on each side of the rib waveguide, such that the overlap of the optical mode (of the waveguide) and the thermal profile (due to current flowing through the doped Si-strips) is high.

It should also be noted that ΔT is proportional to the power consumed by the heater (P), where $P = I^2/R$, R is the resistance of the TOPS and I the current sent through it. The change in the optical power output from the MZI with a TOPS in each arm, is proportional to $\sin^2\phi$. The interested reader is invited to read the following review on TOPSs in silicon platforms [112].

Working principle of electro-optic phase shifters

In general terms, an optical modulator is designed to encode information on an optical signal by imprinting an electrical signal on it [113]. The encoding of the optical signal can be done via its different characteristics, for example via its amplitude, phase, frequency or polarisation. The optical change in the waveguide, and so also the signal passing through it, takes place thanks to the electro-optical effect, thus the foundation of the name EOPS. In this particular case, this is done via the free-carrier plasma dispersion effect, through carrier-injection. Here, a change in the concentration of carriers will affect the optical absorption, as well as its refractive index. A scheme with a forward biased p-i-n junction is used for carrier injection, the intrinsic zone being a thin undoped Si-region and p- and n-doped semiconductors (Si for example) sandwiching it. Opposite charge carriers will accumulate on each side upon connection with an external voltage. A careful phase control is hence achieved in the bal-MZI, which results in a precise amplitude control at the output of the bal-MZI.

As will be further discussed in the sub-section 4.1.5, three distinct EOPSs are used in the transmitter. Each EOPSs has a given length with loss of 3.8 dB/mm. They are operated in a push-pull configuration, in order to lower the voltage needed to change the phase by a given amount. More specifically, in such a configuration one arm is biased with a positive voltage and the opposite arm with a negative voltage, resulting in a factor of two decrease of the required

3. V_π corresponds to the voltage needed to change the phase of the optical signal of π, which is proportional to the length as $L \propto R_{TOPS}$.

4. This is far given that the waveguides have the dimensions: $h = 220$ nm, $w = 450$ nm.

voltage. The interested reader is invited to consult the work in [114] for further details of the employed EOPSs.

Working principle of MZI

Another crucial component of the transmitter PIC is the MZI. An integrated MZI consists (similarly to the usual free-space or fibre-based MZI) of two integrated beam splitters (50/50), two inputs and two outputs, as well as two waveguide arms in between, with either the same length or not, and containing TOPSs or EOPSs in the arms, depending on the application.

The integrated beam splitters work in one of the two main ways: through evanescent coupling or via *multi-mode interferometer*s (MMIs). The former way consists of two waveguides, designed to have an overlap in the field amplitude. By carefully selecting their shape and the distance between them, the splitting ratio can be tuned. The MMI, which is used here, is based on a waveguide with several guided modes. Upon the arrival of the incoming light, the eigenmodes of this light will travel through the MMI waveguide. By carefully tuning its length to width ratio, the interference can be tuned and the splitting accordingly. The interested reader is invited to read the work of [115] for more information.

Looking more specifically into the Mach-Zehnder variable attenuator (VOA in figure 4.2), it should be made clear that it consists of a bal-MZI with TOPSs in each arm to alter the phase of the light flowing through and therefore adjust the output power of the PIC. Regarding the IM (see figure 4.2), it consists of three EOPSs and two TOPSs, one in each arm. The latter components are used to select the working point, *direct current* (DC) bias, of the IM.

Working principle of photodiodes

The transmitter PIC also includes two photodiodes, as can be seen in figure 4.2. The goal of the photodiode is to obtain an electrical current from the conversion of an optical signal. The working of the photodiodes is based on a germanium p-i-n junction in forward bias operation. Incident light upon arrival at this region will create electron-hole pairs that will migrate following the direction of an applied electrical field, generating thus a current [116]. The photodiodes of this PIC are based on SiGe, for the interested reader, the works [117, 118] are recommended.

Working principle of absorber attenuators

The AA working principle is based on, similarly to the EOPS, the free-carrier plasma dispersion effect, in carrier injection mode, where the injected free carriers will absorb the light [5]. In the following section, 4.1.5, examples of usages of the AAs and some of their characterisations are shown.

5. As opposed to the EOPSs, no modulation of the applied current occurs.

4.1.5. Characterisations of the transmitter components

Heater characterisations

A selection of characterisations of the different TOPSs which, from now on, we call heaters, are presented. According to figure 4.2, we will refer to the exact heater via its number (HT#). As previously explained, when current is applied to the heater, a change of phase of the light passing through it will occur. For all characterisations, if not indicated otherwise, light is sent in through the input and detected at the output, as they are noted in figure 4.2. The light source is a laser at around 1550 nm, in either continuous or pulsed mode and for monitoring the output intensity a power meter is used.

First, we analyse the output power as a function of the current flowing through the heaters of the IM (HT4 and HT5) as well as the heaters of the last MZI (HT0 and HT1) [6]. It should be noted that when scanning a specific heater, all other heaters were kept with constant current flow (0 mA in this case). For this characterisation, the laser was pulsed in order to discard any interference effects from the imb-MZI. The graph of the power out as a function of the applied current is shown in figure 4.6.

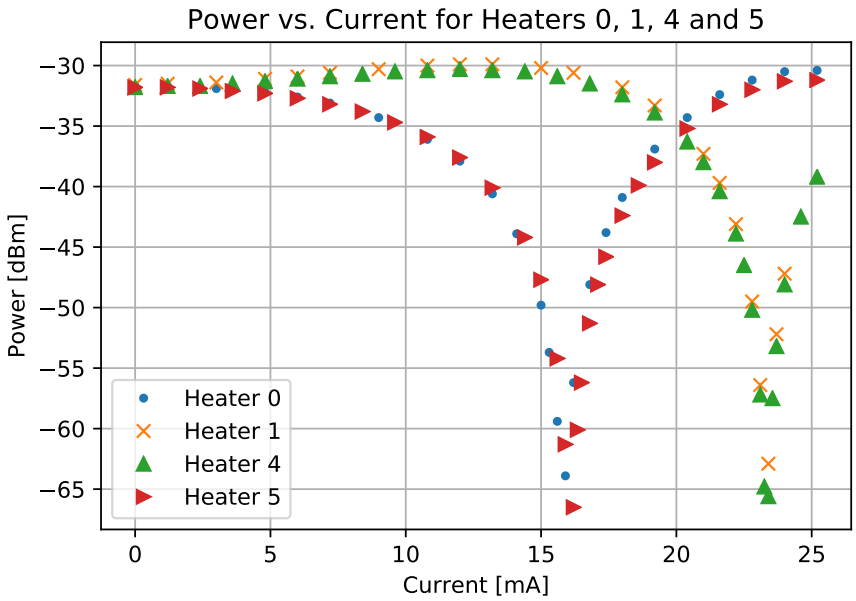


Figure 4.6.: Power out as a function of applied current for heaters 0, 1, 4 and 5.

By precaution, we limited the applied current to 25 mA. From the graph in figure 4.6 we see that the behaviour of the optical output power proportional to $\sin^2\phi$, where $\phi \propto i^2$. It can also be noticed that the pairs of heaters (0,1 and 4,5) behave in opposite ways, meaning the minimum output power of one heater setting corresponds to the respective heater maximum output power setting of the pair, as is expected from their location in the MZI. Lastly, it is concluded that the

6. The same characterisations were done for heaters HT6 and HT7, which performed similarly.

heaters 0 and 5 work in the same way, and 1 and 4 too, due to the them being in the same arm of the MZI (upper or lower with respect to the input of the light). The corresponding *extinction ratios* (ERs) that can obtained with the aforementioned heaters are presented in table 4.1.

HT value	**ER [dB]**
0	32.7
1	30.0
4	35.3
5	35.3

Table 4.1.: Extinction ratios when scanning heaters 0, 1, 4 and 5 (from figure 4.6).

The *polarisation dependent loss* (PDL) of the PIC was also examined and found to be 42.9 dBm. Hence a polarisation controller is placed in between the laser output and the input of the PIC of Alice.

Lastly, the cross-talk between the heaters is examined. Little cross-talk is found between the heaters 0, 1, 4 and 5. Another interesting cross-talk measurement that was performed consisted of sending light through the input bypassing the imb-MZI and monitor the output power when sending current through HT6, HT7 and the attenuator (AA1) of the imb-MZI. The corresponding graph is presented in figure 4.7.

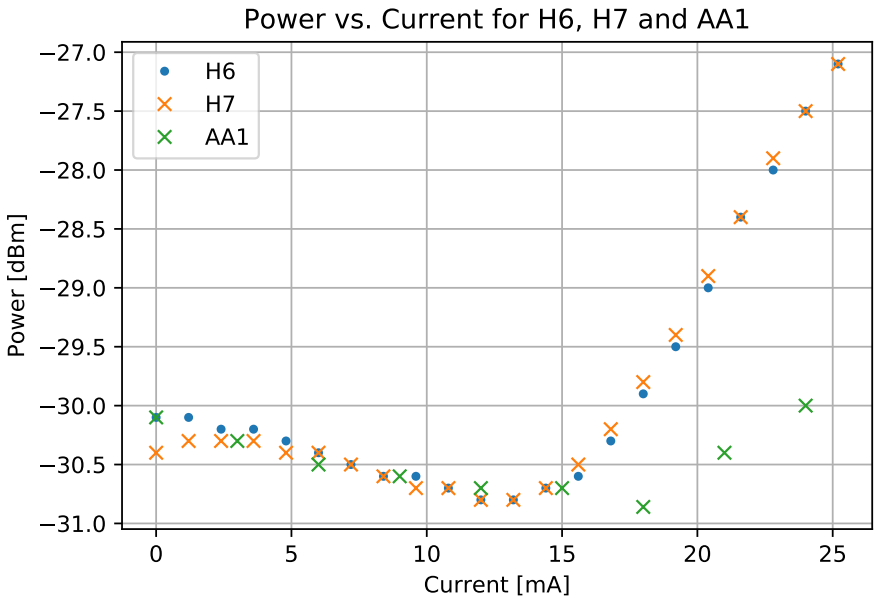


Figure 4.7.: Power out as a function of current when using the input bypassing the imb-MZI and scanning heaters 6 and 7 as well as AA1.

As can be seen from figure 4.7, a clear change in optical output power is observed when current above 15 mA is sent through HT6 and HT7. This corresponds to cross-talk, as these heaters should have no effect at all on the light travelling from this entrance. It should hence be kept

in mind that at high values of current flowing through HT6 and HT7, a change in output power might occur compared to when the current is lower. As the output power can be monitored, this is not a huge problem. However, during the experiment the current flowing through HT6 and HT7 was set below 15 mA. Less effect is seen from AA1, where less than 1 dB of change in power is recorded over the range of applied current. The set point of AA1 is set to a constant value of current during the experiment, to obtain the best visibility of the imb-MZI, as will be discussed in the next part.

Characterization of the absorber attenuators and visibility of imb-MZI

As mentioned in section 4.1.3, two absorber attenuators are placed in the PIC (see figure 4.2). One is found just before the exit of the PIC (AA2), for overall attenuation of the exiting light and one is put in the shorter arm of the imb-MZI, for compensation of the higher amount of loss in the longer arm. The behaviour of AA2 is examined by applying a range of currents and analysing the corresponding change in the optical output power, all the other heaters had no current applied to them. The corresponding graph is presented in figure 4.8.

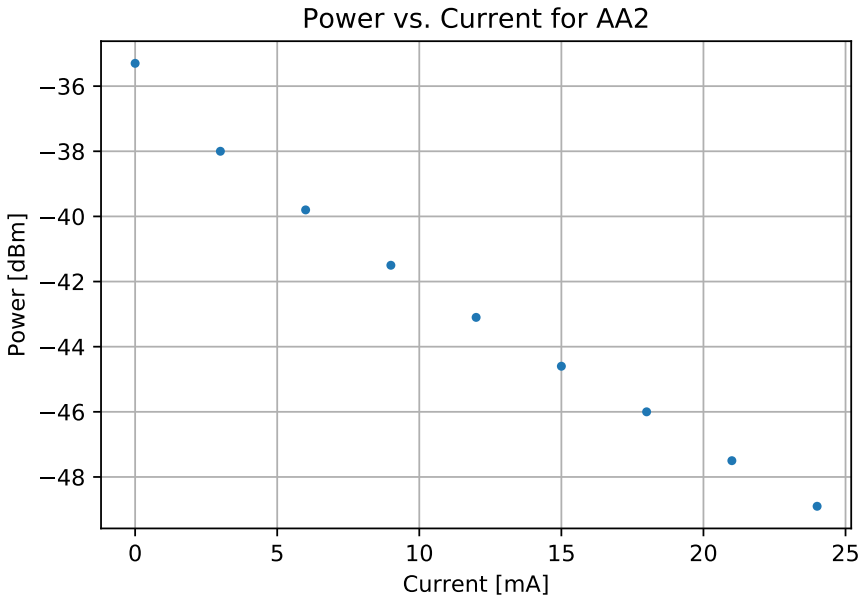


Figure 4.8.: Power out as a function of current applied to AA2.

As expected, from previous discussions, with increasing current, the attenuation increases. From the graph in figure 4.8, an ER of 13.6 dB characterises this attenuator. As suggested by the graph, a higher ER could be found if more current could be applied. As mentioned, by precaution the current flow was limited to 25 mA.

The goal of AA1 is to improve the visibility of the imb-MZI by compensating for additional the loss in the longer arm. The maximum visibility of the imb-MZI was found when 2.16 mA of current is applied to AA1, giving rise to 99.6% visibility. This was done by sending continuous light through the PIC, changing the phase of the imb-MZI (with the help of HT6 or HT7) and

recording the maximum and minimum output powers for different values of AA1. Other examples of visibility for different AA1 values can be found in the appendix (table A.1). To visualise the effect of the AA1 value on the visibility of the imb-MZI, a graph of the power out as a function of the current applied to HT7 for two different attenuations of AA1 (0 mA and 12 mA) is shown in figure 4.9. From the graph it can be concluded that when AA1 has 12 mA of current flowing through, a worse visibility is found (88.1%) due to an overcompensation of loss compared to when AA1 has 0 mA applied (97.3%).

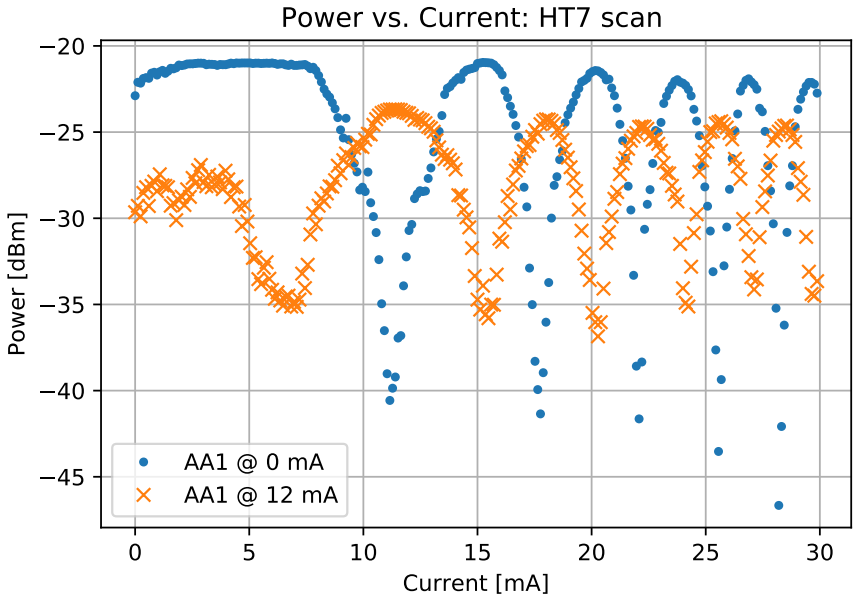


Figure 4.9.: Power out as a function of current applied to heater 7 at different AA1 currents.

Photodiode characterisation

The transmitter also includes two photodiodes (PD1 and PD2), as seen in figure 4.2. They are useful for monitoring purposes, in terms of stability and for eavesdropping attempts. Depending on the distance between the parties, they could even be used for setting the attenuation of the weak-coherent pulses down to single-photon level. Here, an example of characterisation is presented, notably for PD2 when scanning HT0. The measurement was done with AA1 at its optimal value (at 2.16 mA). The readout circuit of the PDs is composed of an amplifier and an *analog-to-digital converter* (ADC). Via a micro controller, we read a value from the ADC, which consists of a number between 0 and 32768, where the higher the number the more light there is in the PD. The relationship between the received light (in terms of the response of the ADC) at PD2 and the output power is plotted in the graph 4.10.

To use PD2 for monitoring purposes, a linear fit, like in figure 4.10, should be done when scanning HT0 and HT1, separately. The corresponding equation of the output power (P_{out}) given the PD2 ADC response (PD_{value}) is: $P_{out} = m \cdot PD_{value} + c$, where m and c are average values obtained from the scan of HT0 and HT1. They are: $m = 4.1 \cdot 10^{-12}$ W/PD_{value} and $c = 1.2 \cdot 10^{-7}$ W.

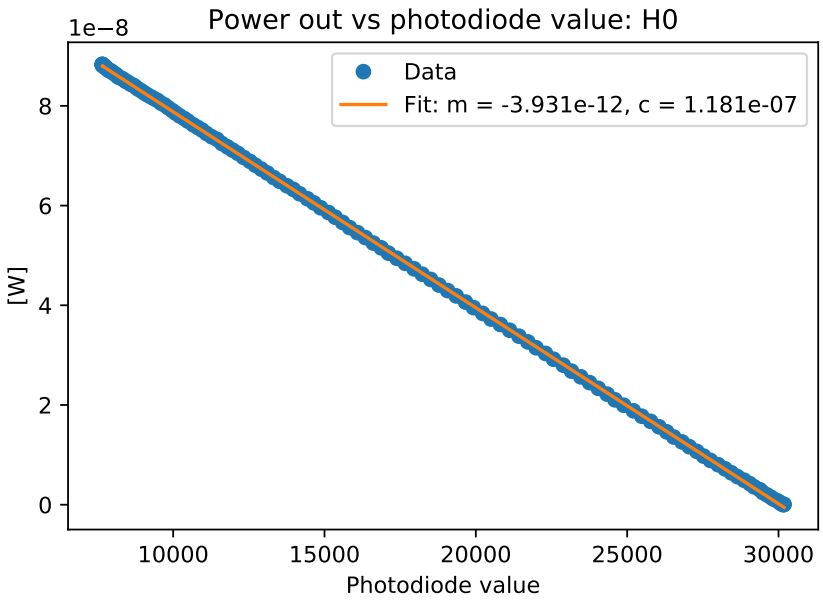


Figure 4.10.: Power out of the PIC when changing HT0 as a function of the photodiode ADC response, noted photodiode value.

Encoding of the three BB84 states and their respective decoy

The IM, which includes three EOPSs and two heaters (HT4 and HT5), from figure 4.2, is used to produce the three states and their respective decoys, presented in figure 2.2. From this figure it is clear that four distinct intensity levels are needed to produce the full combination of states. In particular, to produce the states Z_{0,μ_1} and Z_{1,μ_1}, a maximum amplitude is applied. The states Z_{0,μ_2}, Z_{1,μ_2} and X_{+,μ_1} carry half of the maximum amplitude and the state X_{+,μ_2}, a quarter. The fourth amplitude level is the zero-level one, corresponding to the absence of a pulse.

The various levels are created by actuating a combination of the three EOPSs, which we note E0, E1 and E2. Their relationship is: E2 > E1 > E0, meaning that the EOPS E2 is the longest and has therefore more effect than E1 and E0. The combination of the three, which provides the best preparation of the four intensity levels, is presented in table 4.2.

EOPS	Relative Amplitude
- - -	0
- E1 -	1/4
- - E2	1/2
E0 E1 E2	1

Table 4.2.: The combination of actuated EOPSs (E0, E1 and/or E2) and the corresponding relative amplitude. E2 is the EOPS with most effect and E0 is the one with the least.

It should be noted that to improve the state preparation it is not enough to just turn on or off an

EOPS, the setting of each should be carefully set. The setting can be set via some parameters, for example the maximum current flowing through, the ER, the amplitude swing or the bandwidth. Some can be coarsely tuned and others more finely tuned. Also, for a given setting of the EOPSs, a specific heater working point will improve the result. The heater, acting like a bias, will set the overall phase of the IM. For this, either HT4 or HT5 is used.

For a SKR exchange to take place, one also needs to keep in mind the values of ratios of the Z and X states, more precisely: μ_1/μ_2, for the Z and the X basis. The ratio should be close to 1/2, to make sure that the EOPSs are set such that the levels (1, 1/2, 1/4 and 0) are respected. Also, the mean intensity per state in X and Z basis should be the same. Hence, the best settings of the EOPSs, with a given heater working point, are those where the decoy ratios are as close to their desired values as possible and the q_z and ϕ_z are as low as possible. This is not quite straightforward to obtain. However, once the settings are found, they can be used for several SKR exchanges at various distances.

Once the states are encoded properly, one last condition has to be fulfilled for a SKR exchange to be done, namely to send the correct mean photon number to Bob. For this, the power is measured at the output of Alice, noted P_A and the amount of attenuation that should be added to the optical signal is found using the equation: $P = E_\gamma \cdot f \cdot \mu_1(p_{\mu_1} + rp_{\mu_2})$, where E_γ is the energy of the photon at the given wavelength, f is the repetition rate of the laser, μ_1 is the value of the decoy one (given by our simulation after optimising the SKR), p_{μ_1} and p_{μ_2} are the respective probabilities of sending decoy one or two, set by the user and r is the ratio of the decoys μ_2/μ_1. This ratio should be close to 1/2 and is found using the detections on Bob's side before starting the SKR exchange. The attenuation, α, in dB, that should be set on the variable attenuator is hence given by: $\alpha = 10\log\left(\frac{P}{P_A}\right)$. One should be careful to take into account the intrinsic attenuation of the attenuator too.

Handling the thermal stability of the PICs

Efforts to obtain thermal stability (within the 0.1°C) of the PIC were done. One of the most important reasons for this stability comes from the need to stabilise the relative phase of the imb-MZIs of the transmitter and receiver. It should be fixed such that destructive interference takes place in the monitoring detector (X basis), on the receiver side (further information is found in section 2.3.1). The relative phase is set with one of the heaters of the imb-MZI on Alice's side (HT6 or HT7). An automatic feedback loop, using the side-peak detections (see figure 2.4) as inputs is used to keep the phase, and so the error in the X basis, ϕ_z, stable.

To temperature stabilise the PIC, a Peltier and a thermistor were placed under the chip. A *thermoelectric cooling* (TEC) driver from Thorlabs [7] was used to monitor and actively stabilise the temperature. The latter was done via a *proportional, integral, derivative* (PID) controller. In order to isolate the PIC from any changes in temperature of the external environment and to protect it from the touch of clumsy hands, a home-made case for it was designed. A radiator was placed on top of it for heat evacuation. The PIC was stabilised at 45°C. A photo of how the

7. MTD415T

chip was used when mounted with the case and the radiator is shown in figure 4.11.

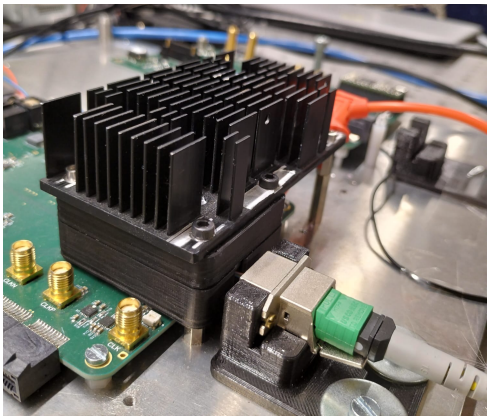


Figure 4.11.: Photo of the PIC of Alice in its case with the radiator on top. The fibre connector with the fibre and holder can be spotted in front of the case.

4.2. Integrated QKD receiver

4.2.1. General requirements for the receiver platform

According to the adopted protocol and as previously mentioned in section 2.2, the receiver constitutes of an initial beam splitter, sending light to either the Z or the X basis. In the former basis, light is sent directly to a SPD and in the latter basis, light passes first through an imb-MZI before detection by a SPD. The receiver is passive and is required to be polarisation insensitive. Additionally, it should carry as low loss as possible. Thus, efforts were placed into producing a PIC with the these characteristics.

The demand of low loss is important, as any loss of light on this side corresponds to a loss in the number of available bits for the production of the secret key. The polarisation independent condition holds for both the initial splitter as well as the imb-MZI. If the first beam splitter would be dependent on the polarisation, careful control of the input polarisation would be equivalent to a complete control of the basis, which would make the key exchange insecure against attacks. The polarisation independence of the imb-MZI is characterised via its visibility, which should be as close to 100% as possible for any incoming polarisation state. It is complicated to achieve polarisation independence in PICs due to the intrinsic waveguide birefringence, which is particularly difficult to control in an imb-MZI [119–121]. Regardless, polarisation independent QKD receiver chips have been demonstrated [122, 123]. However, the important characteristics of a maximum visibility close to 100% and low insertion loss were unfortunately not well achieved (98% with 6 dB and 98.7%, respectively). A hybrid version consisting of a imb-MI with Faraday mirrors glued to the exterior of the PIC has also been shown [124]. The following two sub-sections, 4.2.2 and 4.2.3, present two integrated receivers based on two different platforms and subsection 4.2.4 presents their individual characterisations.

4.2.2. Silica based receiver

One proposal of a polarisation independent receiver PIC came from the group of Roberto Osellame at the CNR-IFN [8] in Milano. They fabricated a PIC using a femtosecond laser micromachining technique [46]. The material used was aluminum borosilicate glass [9]. Low propagation loss (< 0.2 dB/cm) and low birefringence ($< 3 \cdot 10^{-5}$) characterises the waveguides. A photo of the PIC is shown in figure 4.12 and its schematics, in figure 4.14.

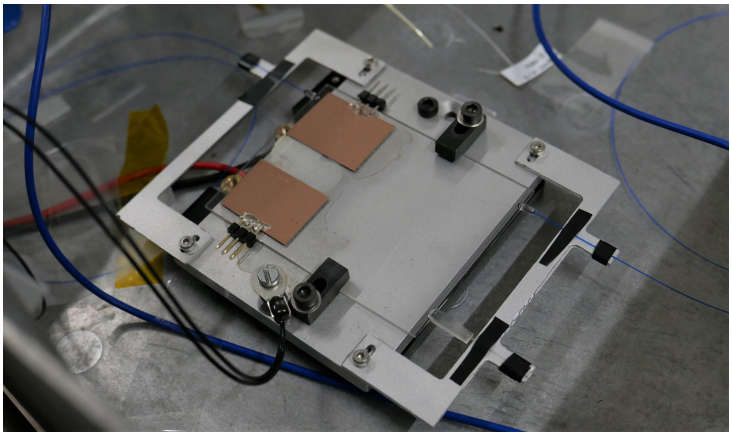


Figure 4.12.: Photo of the PIC of Bob from CNR-IFN in Milano placed in a metallic box.

The footprint of the receiver PIC is around 6 cm $\times$ 8 cm. To keep the PIC temperature stabilised, it was placed in a metallic box with fibre connectors on the edges and holes for cables, shown in figure 4.13. A Peltier and a thermistor were also used here for temperature stabilisation, which was dependent on an external temperature controller [10].

Figure 4.13.: Photo of the metallic box containing the PIC of Bob.

In figure 4.14 the schematics of Bob are presented. As is expected from the receiver of the protocol, according to figure 2.3, light coming from Alice, enters the PIC and passes first by a polarisation independent and passive beam splitter. It will make the choice of the light to go straight through the chip out to the Z basis detector, or to go through an identical imb-MZI as on Alice's side before exiting the chip and going to the X basis detector. The splitting ratio is

8. National Research Council-Institute of Photonics and of Nanotechnologies.
9. EAGLE XG, from Corning Inc.
10. Stanford Research Systems PTC10.

94/6 (Z/X), which is not optimal but good enough for performing QKD exchanges over several distances, see section 4.4. It can also be noticed that the first splitter of the imb-MZI is 55/45, this is to compensate for the additional loss in the longer arm.

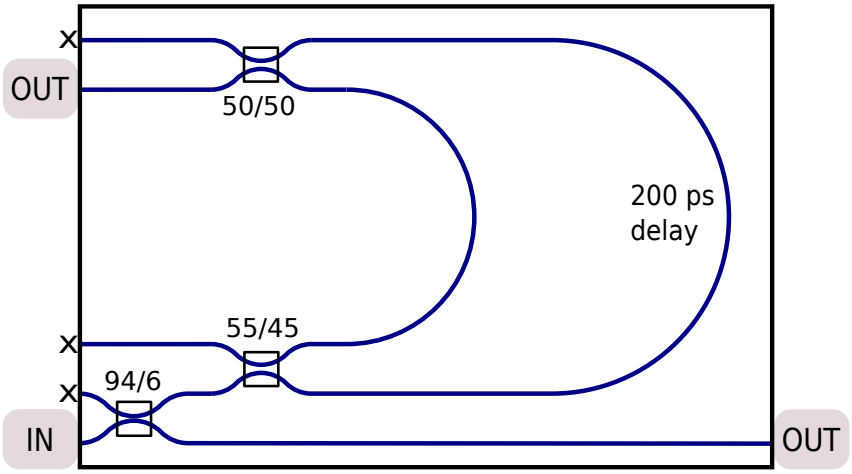


Figure 4.14.: Structure of the receiver integrated circuit. X means non-fibre-coupled ports. Fibres are butt-coupled to the waveguides and permanently pigtailed with *ultraviolet* (UV)-curing, index-matching glue. Fibre to waveguide coupling losses are better than 0.3 dB/facet.

4.2.3. Silica on silicon based receiver

Another version of the receiver PIC, made in silica on silicon, by VLC Photonics was considered. The dimensions of the PICs are: 11 × 35 mm^2 and a photo of one of the PICs is shown in figure 4.15.

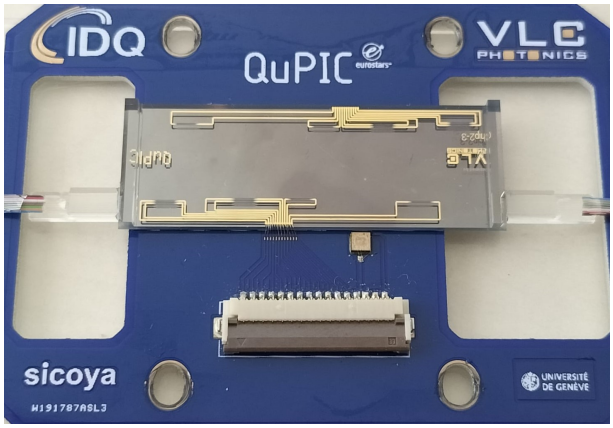


Figure 4.15.: Photo of the PIC of VLC Photonics, including butt-coupled SMFs, placed on a host-PCB. Bondings link the PIC to the host-PCB, which is connected to the main control PCB via a ribbon cable connected to the electronic connector (below the PIC on the photo).

In total, three versions of the receiver were produced and characterised. Their differences are:

System 1: All waveguides are rectangular (4.0 × 4.5 μm^2).

System 2: All waveguides are rectangular ($4.0 \times 4.5\ \mu m^2$), except for the ones of the interferometer, which are square ($4.5 \times 4.5\ \mu m^2$).

System 3: All waveguides are square ($4.5 \times 4.5\ \mu m^2$), except for the couplers, which are rectangular ($4.0 \times 4.5\ \mu m^2$).

A sketch of the lay-out of the PICs is shown in figure 4.16.

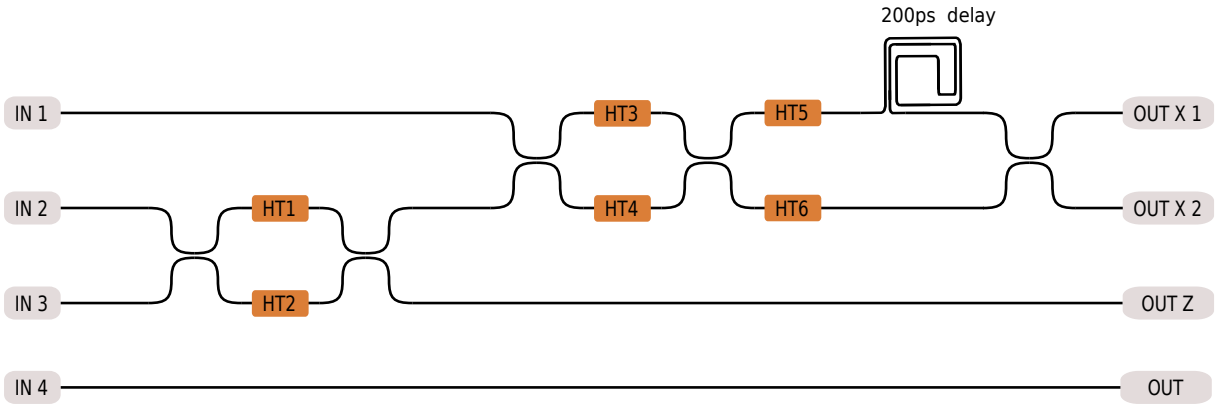


Figure 4.16.: Schematics of Bob from VLC Photonics. HT# corresponds to heaters along the waveguides and IN and OUT correponds to fibre-coupled inputs and outputs of the chip.

Standard SMF pigtails are butt-coupled on both ends of the PIC, corresponding to the in- and outputs. As can be seen in figure 4.16, inputs *2* and *3* correspond to the entrance of the light from Alice to Bob [11] and *IN 1* and *IN 4* are useful for testing purposes. On the output side, the single *OUT* is used with *IN 4* to check for straight waveguide loss. *OUT Z* is used for detecting the Z states and either one of *OUT X 1* or *OUT X 2* for detecting the X states. In accordance with the 3-state BB84 time-bin protocol that is adopted, the imb-MZI contains a 200 ps delay line. Heaters (*HT#* in figure 4.16) are TOPSs whose working principle is explained in sub-section 4.1.3. They are placed in each arm of the different MZIs of the chip and are used to change the phase of their corresponding interferometer. This would consequently lead to a change in the splitting of the light in the second splitter of each interferometer, respectively. Thus, heaters *1* or *2* are used to adjust the splitting ratio between the Z and X basis. Heaters *3* or *4* are set such that the greater amount of light passes through the longer arm, compensating thus for the higher amount of loss in this arm. Finally, heaters *5* or *6* can be used to control the relative phase of the imb-MZI at Alice's and Bob's. The current flowing through the heaters is controlled via an in-house-made PCB and a microcontroller [12], which also both handle the temperature stabilisation of the PIC via a Thorlabs TEC driver [13] in combination with a Peltier. The PIC is placed in the box in figure 4.13.

11. Only one is necessary for the experimental setup of the QKD system.
12. Teensy 3.2
13. MTD415T

4.2.4. Characterisations of the integrated receivers

In this section, the characterisations of the two most important features of the integrated receiver, the loss and its polarisation independence, are presented for both PIC suggestions. Discussions regarding the length of the delay line for the utilised PIC will also be presented.

Characterisations of the loss

The total loss of the Z and X basis, respectively, of the proposed receiver PICs is presented in table 4.3. These values exclude the loss of the splitting ratios of the first and last beam splitters, but include the loss of the input/output coupling.

Platform	Loss Z basis [dB]	Loss X basis [dB]
Silica	2.75	3.50
Silica on Silicon	2.7	7.0

Table 4.3.: Loss of the Z and X basis of the silica and silica on silicon PIC. The input used for the silica on silicon PIC is *IN 3* and the outputs are *OUT Z* and *OUT X 1*, for the Z and X basis, respectively.

The results of table 4.3 show that the loss of the PICs are particularly low, which is much in our favour for this experiment. Comparisons of the loss of other integrated receiver QKD systems are found in section 4.5. Thanks to the additional inputs and outputs of the silica on silicon PIC, the average[14] straight waveguide loss could also be obtained (using *IN 4* and *OUT*). It was found to be 1.3 dB and includes coupling and propagation losses. The average polarisation dependent loss of the straight waveguide on this platform was also measured and found to be 0.2 dB.

Characterisation of the polarisation independence

Regarding first the polarisation independence of the initial beam splitter of the PICs. For the silica PIC, this was assured by the team of Roberto Osellame by using the multiscan inscription technique, followed by a thermal annealing process, a well-known approach within their community, established in their group. The interested reader is invited to read the work [125]. For the silica on silicon PIC, this was confirmed experimentally with the first MZI, which was found to be independent of the polarisation.

Following with the polarisation independence of the imb-MZI. We decided to quantify this via the visibility obtained for different incoming polarisations. The minimum visibility, $V_{\min}$, corresponds to the visibility obtained when light enters with the most unfavorable polarisation. Experimentally, by adjusting the polarisation of a coherent laser in continuous mode with a man-

14. Taking into account the three systems.

ual polarisation controller, the maximum ($V_{\max}$) and minimum visibilities could be found when scanning the phase of the imb-MZI. If the imb-MZI is polarisation independent, $V_{\max} = V_{\min}$. The relationship between the visibility and the QBER was defined in equation (2.6), where a high visibility minimises the QBER. The maximum and minimum visibilities of the silica and the silica on silicon PICs are presented in the table 4.4.

Platform	$\mathbf{V_{min}}$ **[%]**	$\mathbf{V_{max}}$ **[%]**
Silica	98.9	99.7
Silica on Silicon	94.5	99.8

Table 4.4.: The maximum and minimum visiblities of the silica and silica on silicon PICs.

Starting with the results of the silica on silicon PIC, it should be noted that the V_{min} presented in table 4.4 corresponds to the best one of all the versions of the PICs. A table of the results of V_{min} obtained for all systems is found in the appendix (B.1). We can conclude that for this PIC, a high V_{max} is obtained and a moderate V_{min}. Unfortunately, it is sufficiently low to give rise to a non negligible contribution of 2.8% to the QBER. Hence, this PIC presents a too high polarisation dependence and is not good enough to be a receiver in the full experimental setup. It should also be remarked that the values of V_{min} between the different silica on silicon PICs are highly diverse (going from 26.3% to 94.5%, see table B.1). Hence, the birefringence of the imb-MZIs can be concluded to be non-negligible, and the discrepancies of the results between the systems render it difficult to give a conclusive reason for this birefringence.

Regarding the results obtained with the silica PIC, a high minimum and maximum visibility is obtained, 98.9% and 99.7%, respectively, as seen in table 4.4. This PIC therefore guarantees its spot as the integrated receiver PIC used in our experimental setup. The polarisation independence of the imb-MZI was achieved by the team of Roberto Osellame by fabricating compensation tracks above the waveguide of the longer arm of the imb-MZI [125, 126] and controlling the temperature of the PIC. At a specific temperature (around room temperature), the same polarisation rotation occurred in both arms of the interferometer and almost perfect interference could be obtained. It should be noted that the minimum visibility corresponds to the case where the input light is composed of the most unfavorable input polarisation state. Thus, the average visibility will be higher. For the interested reader, a table of the minimum visibility as a function of the several set temperatures is placed in the appendix (table B.2).

To finish this section, the difference in the delay lines of Alice and Bob was also analysed, where Bob corresponds to the silica PIC, officially used for the setup. Ideally, the delay lines should both be of the same length, meaning precisely 200 ps. However, due to fabrication errors and uncertainties, their values can differ. The error in the X basis will suffer if there is a difference in delay, as it leads to a worsened interference of the pulses in the imb-MZI at Bob's. A difference of around 1.6 ps was measured between the integrated Alice and Bob. Doing a second or even third run of fabrication would allow for an improvement in the understanding of the imb-MZI, necessary for simulating and fabricating the PIC, which would eventually lead to a negligible delay difference between Alice and Bob.

4.3. Experimental setup based on an integrated transmitter and receiver

Overall, the experimental setup using an integrated transmitter and receiver is very similar to the fibre-based one (see figure 2.3), but with less amount of separate components and most of the optics integrated. Therefore some details will be omitted in the following discussion, if they were already mentioned in sections 2.3, 4.1.3 and 4.2.2, novelties and important information will however be acknowledged. A general overview of the integrated QKD setup is presented in figure 4.17.

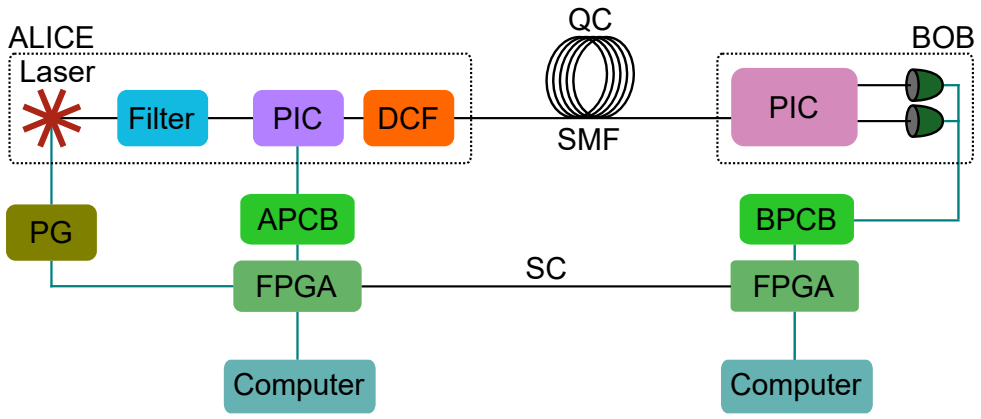


Figure 4.17.: Simplified schematics of the experimental setup. PIC = photonic integrated circuit, DCF = dispersion compensating fibre, QC = quantum channel, SMF = single-mode fibre, PG = pulse generator, APCB = Alice printed circuit board, BPCB = Bob PCB, FPGA = field-programmable gate array, SC = service channel. Black lines correspond to optical links and blue lines correspond to electrical connections.

The dotted boxes in figure 4.17 correspond to the optics comprised in the setups of Alice and Bob, respectively. Regarding Alice, as for the fibre-based setup, the laser is pulsed at 2.5 GHz and works at around 1551 nm. The FWHM of the pulses is around 31 ps and the laser is temperature stabilised at 30°C. An external *pulse generator* (PG), provides synchronised pulses to the laser, via a clock from the FPGA. An external filter is placed to narrow the spectrum of the pulses and improve the interference of the X state at Bob's. This filter wavelength was found, experimentally, to be the best when optimising for the highest ER of states in the X basis.

The pulses then enter the PIC, where they first pass through the imb-MZI (to create the pairs of qubits) and then the IM, where the different states are randomly encoded. The probabilities to select the Z and X basis are 0.67 and 0.33, respectively. These numbers are found to be the best ones from a simulation when optimising the SKR. DCF is placed before the exit of Alice. The loss of this fibre is rather high (2-20 dB, depending on the distance). Hence, the attenuation of the qubits down to single-photon level was done with the VOAs of the transmitter PIC. If the attenuation of the DCF and the VOA on the PIC was not enough, an external variable attenuator [15] was placed after the DCF. As much SMF (loss of around 0.2 dB/km) as is wished for is then placed at the output of Alice and connected to Bob.

15. Exfo FVA-3100.

The control of the components on the tranmitter PIC is done through APCB and the FPGA, both interfaced with a PC. More specifically, the FPGA provides the high-speed RF signals that are sent to the EIC, via APCB as an interface, to drive the IM. A microcontroller provides the SPI communication to the IM driver (in the EIC), for the setting of its parameters. APCB provides the necessary current sources for the working of the heaters of the PIC. Additionally, APCB handles the reading of the PDs.

As previously mentioned, upon arrival at Bob's, the light passes either through the Z or X basis arm and exits to a corresponding SPD. The pulses in the X basis imb-MZI should interfere destructively in the output that is monitored. This is assured by actively adjusting the relative phase of the interferometers of Alice and Bob, which is done by acting on the phase of Alice's interferometer (using HT6 or HT7). A feedback loop on the corresponding heater is locked to ensure the low amount of detections in the monitoring output. This active adjustment will be harder to perform the more loss the channel has, due to the low number of statistics.

The *Bob printed circuit board* (BPCB) will be able to control the detectors, notably the delay of the detection pulse with respect to the timing window of the FPGA, used for alignment purposes. The detections will also be able to be interfaced with the FPGA through BPCB. All components can be monitored and controlled via another PC on this side. Additionally, for synchronisation and post-processing purposes, Alice and Bob are connected via the service channel, as mentioned in section 2.3.1.

The detectors used are either SPADs or SNSPDs (presented in section 2.3.2). The latter set of detectors, being the most performant set of the pair, is used to characterise our QKD system and to understand to what extent the SKR can be pushed. They feature low timing jitter (around 40 ps), negligible after-pulsing probability, high detector efficiency (around 80%) and low dark count rates (dc_z = 200 cps, dc_x = 100 cps). The former set of detectors are used for the experiment as they are more practical than SNSPDs for practical real-world applications and allow thus to understand what results can be expected if the system were to be deployed in an actual network. These detectors have a timing jitter below 100 ps, dark count rates of around 120 cps and a detection efficiency of around 20%.

A brief comment on the fixed 94/6 splitting ratio between the Z and X basis, respectively, at Bob's side should be mentioned. This splitting ratio is well suited for intermediate distances. However, for short distances, the Z basis detector will rapidly saturate due to the large number of photons arriving at it and for long distances, the X basis detector will suffer of too few detections, giving rise to a non-negligible dark count contribution. In a future run of the receiver PIC, having a tunable MZI would increase the range of distances that the system could handle.

For the full secret key exchange, error correction was performed in real-time using the Cascade algorithm, presented in 2.1.2. An error correction block size was taken to be 8192 bits and privacy amplification was executed after 1000 error correction blocks. The final SKR was calculated using the formula (2.5), presented in section 2.2.3.

4.4. Secret key exchanges

In this section results of complete secret key exchanges using both the SNSPDs and the InGaAs/InP SPADs are presented, for emulated fibre distances, using a VOA, and employing standard SMF.

4.4.1. Using superconducting nanowire single-photon detectors

First, results obtained when using the SNSPDs are presented. As previously mentioned, SKRs obtained with these detectors are among the best that can be obtained with this experimental setup given the high performance of these detectors. The emulated distances at which SKRs were evaluated are 30, 36, 38 and 40 dB. Additionally, a SKR was also evaluated using 202.0 km of standard SMF. A summary of the corresponding results is presented in table 4.5.

Length [km]	Attenuation [dB]	q_z [%]	ϕ_z [%]	SKR [kbps]
-	30	0.9	1.0	91.0*
-	36	0.8	1.1	28.3
-	38	0.8	1.4	17.2
-	40	0.8	2.1	10.6
202.0	39.5	0.9	2.2	9.4
[86]: 251.7	42.7	0.5	2.2	4.9

Table 4.5.: Parameters and results of secret key exchanges when using SNSPDs. * signifies estimated SKR from raw data. For comparison, the last line presents data from reference [86] which implemented a fibre-based setup of the 3-state BB84 time-bin protocol with 1-decoy state using SNSPDs. SKR = secret key rate, q_z is the quantum bit error rate in the Z basis and ϕ_z, the phase error rate, in the X basis.

For the interested reader, additional results like the block time and the *raw key rate* (RKR), corresponding to each distance, can be found in the table C.1 in the appendix. A first remark to make regarding the results in table 4.5 concerns the 30 dB emulated fibre distance. At such low attenuation, the real-time error correction Cascade couldn't be performed, due to a too high number of detections. Thus, for this measurement point, the SKR was estimated from the raw data. An implementation of a *low-density parity check* (LDPC) error correction code on the FPGA could solve this problem [69].

Concerning the results of the emulated fibre distances, in general, the q_z is found to be strikingly low for all measurements. Its main contribution comes from the timing jitter of the SNSPD, which is low (< 50 ps). Additionally, the ER of the IM contributes to the q_z. In static mode an ER of 40 dB is measured and in active mode it is lower. Continuing with the phase error rate, ϕ_z, low values are also obtained in general, however more disperse values between the emulated distances are seen. The main contribution on ϕ_z depends on the interferometers of Alice and Bob, notably their visibilities and the active phase stabilisation between them. At low attenuations, a lot of counts are registered in the detectors, notably on the X detector for the ϕ_z calculation.

Hence, it is straightforward to perform active phase stabilisation for these attenuations. The low value of ϕ_z arises thanks to the high visibilities of the two interferometers. At increasing attenuations, the visibilities obviously stay high, however the active phase stabilisation becomes more and more tricky due to the lower number of counts in the X detector. Especially since the passive splitter defining the Z and X basis is heavily biased towards the Z basis (the splitting ratio being 96/4). More detailed information about the phase stabilisation is found in section 4.3. Additionally, at high attenuations the dark count contribution is non-negligible and also causes an increase in ϕ_z. Regarding the SKRs, high values are recorded, for the different emulated distances, thanks to the low q_z and ϕ_z, corresponding well to the state-of-the-art integrated QKD, using SNSPDs. More information about comparisons of other integrated works is found in section 4.5.

Regarding the measurement using 202.0 km of standard SMF, similar values, although ever so slightly higher, of q_z and ϕ_z and thus lower SKR, are found. Here, length fluctuations in the fibre will occur and are compensated with active time-tracking (as mentioned in section 2.3.1). The minor change in q_z and ϕ_z is most certainly due to non-perfect time-tracking.

Finally, the last line of table 4.5, presents the results obtained with the fibre-based setup (as described in 2.3.1), employing SNSPDs and the same protocol (the three-state time-bin BB84 with 1-decoy state), the corresponding work is [86]. It is added to compare the fibre-based work with the integrated one. Using 251.7 km of ultra low-loss SMF (around 3 dB more attenuation than the fibre distance of integrated setup), similar mean photon numbers and the same error correction block size, it can be concluded that the integrated setup performs as well as its fibre-based counter-part. However, the integrated setup is of course more attractive thanks to its enhanced practicality, among other advantages.

4.4.2. Using InGaAs/InP single-photon avalanche photodiodes

In this section, results obtained using the InGaAs/InP SPADs are presented. As previously mentioned, thanks to their less complicated cooling process, compared to SNSPDs, these detectors are more interesting for industrial implementations. However, they come with higher dark count rates, after-pulsing probabilities and timing jitters, as well as lower efficiencies, compared to the SNSPDs. The results of the secret key exchanges using these detectors are shown in table 4.6.

More detailed information on the parameters of the detectors for each measurement, such as the dead time and the temperature of the detectors, as well as the corresponding block time and RKR can be found in the table C.2, in the appendix. Not surprisingly, analogous conclusions to the results presented in table 4.5 can be drawn. From table 4.6, it is clear that the q_z values are higher when using SPADs, this is due to the higher timing jitters and afterpulsing probabilites of these detectors. Additionally, a faster saturation in the Z basis detector is recorded due to the high bias towards this basis with the 96/4 splitting ratio, which also accounts for a non-negligible dark count rate contribution at high attenuations in the X basis. Thus, higher values of ϕ_z are seen, especially at 40 dB emulated fibre distance and the SKR follows accordingly. It should also be noted that the efficiency of the SPADs is around 20%, a fourth of the one of the SNSPDs.

Length [km]	Attenuation [dB]	q_z [%]	ϕ_z [%]	SKR [kbps]
-	30	3.6	2.1	2.9
-	35	3.1	4.5	1.3
-	40	4.4	6.0	0.2
151.5	29.7	3.3	2.7	1.3
[67]: 151.6	30.2	3.2	2.1	7.2

Table 4.6.: Parameters and results of secret key exchanges when using InGaAs/InP SPADs. For comparison, the last line presents data of the fibre-based implementation of the 3-state BB84 time-bin protocol with 1-decoy state using also InGaAs/InP SPADs [67]. SKR = secret key rate, q_z is the quantum bit error rate in the Z basis and ϕ_z, the phase error rate, in the X basis.

151.5 km of SMF was also placed in between Alice and Bob. It can be seen that ϕ_z is higher than its attenuated analogue, this is again due to the non-perfect time-tracking, which is especially hard at low count rates.

For completeness, the integrated results are compared with their fibre-based correspondent using the same detectors and protocol (work of [67]). It can be concluded that the fibre-based setup performs slightly better than the integrated one with slightly lower values of q_z and ϕ_z and thus a higher SKR. However, the difference in results can be mainly associated with a different set of detector parameters. The fixed and non-optimal splitting ratio obliged the dark counts in the X basis to be kept low, which was done by setting a lower bias voltage, lowering the detector efficiency. To minimise the afterpulsing contribution, a higher dead time was set. Also the temperature of the detectors in the Z and X basis is forced to be at the same value with the experimental setup of the detectors as it is. However, the close values of q_z and ϕ_z of the integrated setup with respect to the fibre-based one, of course still show evidence of the interest of deployment of the integrated setup. As previously mentioned, a higher range of distances and most probably improved results would be found when replacing the first beam splitter of the receiver PIC with a tunable MZI. This has already been developed with satisfying results on the same platform [127].

4.4.3. Long term stability

A stability measurement was the final measurement that was performed with the integrated QKD setup. For this, 202.0 km of standard SMF was placed in between Alice and Bob and secret key exchanges using SNSPDs were performed over 80 minutes. The figure below (4.18), shows the q_z, ϕ_z, RKR and SKR over time.

Highly stable RKRs and SKRs are observed, around 25 kbps and 9 kbps, respectively, reflecting the good thermal stability of the setup, as well as stable working of the IM. Similarly, q_z is stable (around 0.9%), thanks to the fine time-tracking, which is relatively simple due to the high number of detections in the Z basis. Slightly more fluctuations are present for the ϕ_z, due to the lower detection rate in the X basis and thus a less trivial active phase adjustment.

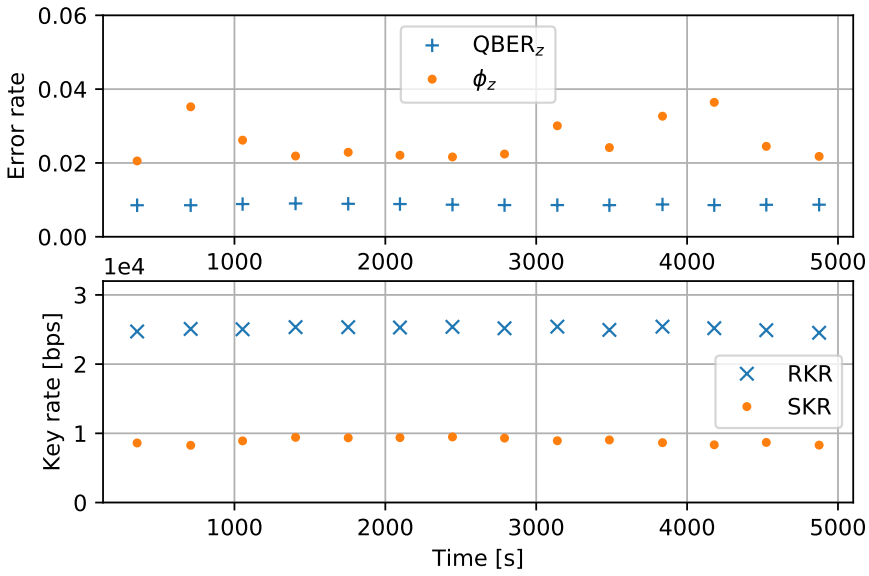


Figure 4.18.: QBER$_z$ (quantum bit error rate, Z basis q_z), ϕ_z (phase error rate, X basis), RKR (raw key rate) and SKR (secret key rate) during several secret key exchanges over 80 min using superconducting nanowire single-photon detectors at a distance of 202.0 km single-mode fibre.

4.5. Discussion

Firstly, some remarks on the advantages and disadvantages of the integrated setup with respect to a fibre-based one (especially its fibre-based analogue, presented in figure 2.3) will be reviewed. In general, a simpler production for industrial applications is expected with the integrated setup. Not only are there fewer discrete components to characterise during the assembly, but also, there are fewer components to trouble-shoot. Of course the size is also a non-negligible feature. For example, in terms of the fibre-based components that were replaced by an integrated version on the transmitter side, a down-size is achieved without doubt. The exact space that would be gained in a standard rack used for a QKD system by using an integrated transmitter PIC depends highly on its packaging. The packaging of the PIC is crucial (especially since the PICs tend to be fragile) and has to be carefully thought of. On the receiver side, a down-sizing (of the initial beam-splitter and imb-MZI) by using a PIC is not enormous in this specific case, due to the material choice, which comes with other advantages. The benefits of low loss and polarisation independence were particularly favoured. Scalability and mass-production are substantial advantages of the integrated setup too. Additionally, the more PICs that are made, the lower the costs of production. In terms of cost, a benefit is also achieved during the installation process given that there are less components to place and characterise, hence speeding up this process. Further on, once the parameters and different features of the respective PICs have been carefully examined and tested (research and development), they are manufactured in a highly reproducible manner. This is particularly useful for the production of the imb-MZIs, where the delay lines of Alice and Bob should be as close in length as possible. It is not a trivial task to manually fabricate delay lines of a fibre-based imbalanced interferometer that require precisely

the same length. This manual process is also highly time-consuming.

Next, points that can be improved for future generations of the setup of the presented integrated QKD setup will be examined. A general remark regarding integrated photonics is of course the difficulty to trouble-shoot a PIC when something does not work as expected. As opposed to a fibre-based component, a PIC cannot, simply, be dismantled and repaired and in general only has a few inputs and outputs. On the bright side, when it works, it is rather robust and reliable.

Exploring the improvements of the transmitter and receiver, starting with the former, an improvement would include using the available integrated filter instead of using an external one. In the developed PIC a ring filter is present, however its input was unfortunately damaged for the used PIC. In the future its usage should be considered. Also, it is possible to get rid of the external pulse generator and place its function in a common PCB including the electronics needed for the PIC and the laser [16]. Further on, the need of DCF at the transmitter side is unpractical. Not only does it take a lot of space (the size of a standard fibre spool), but also the necessary length depends on the distance chosen, thus it does not allow for a lot of flexibility once placed. An option could be to work at a lower repetition rate (1.25 GHz instead of 2.5 GHz), and so become less dependent on the chromatic dispersion thanks to the increased size of the time-bins. Lastly, of course the question of integration of the laser is a valid wondering, as it can be seen as a disadvantage that it is external in this setup. In order to integrate a laser on PIC, an active material is needed like for example InP and not Si (as mentioned in section 1.2). Si was chosen to integrate, in a cheap way (InP being much more expensive) the optics *and* the expensive electronics (DAC and amplifier). Doing this in InP would be possible, however much more expensive, thus leading to a less obvious network installment.

In terms of the receiver, a simple improvement for a future run is to include a tunable beam splitter at the entrance of the PIC of Bob. It should be made clear that this was an option for the production of this PIC, but it being the first try, it was chosen to play safe and place a passive beam splitter, in case it does not work as expected. Another improvement concerns the detectors. Here Stirling-cooled SPADs were used, which come with an unpractical packaging (dimensions of around 40 cm x 45 cm). In the future, Peltier-cooled detectors should be used in order for simple integration of the full setup in a box.

Selected implementations of integrated QKD are presented in table 4.7 and used to compare this

16. This project is ongoing and a lot of work has already been done, hence this is totally feasible.
17. The transmitter included an integrated laser and the total loss of the receiver was 9 dB. The achieved key rate was an asymptotic one.
18. Asymptotic secret key rate.
19. Asymptotic secret key rate. The detectors used were SPADs.
20. Both the transmitter and the receiver were hybrid. The detectors used were SNSPDs.
21. The receiver presented 15 dB loss.
22. Emulated fibre distance. The receiver PIC presented a total loss of 13 dB and is suited for multiple users. The detectors used were SNSPDs.
23. The distance of 100 km corresponds to an emulated fibre distance and the laser was integrated in a PIC. The detectors used were SNSPDs. Asymptotic secret key rates.
24. On the transmitter side the laser was integrated and a fibre-based phase modulator was utilised on the receiver side. The total loss of receiver PIC was 4.5 dB, however the typical loss of their PICs was 9.0 dB.
25. Finite key SKR.
26. Emulated fibre distance. The detectors used were integrated SNSPDs.
27. First line using SPADs, second line using SNSPDs.

Work	**TX** (Platform)	**RX** (Platform)	**Protocol**	**Clock Rate** [Hz]	**SKR** [kbps]	**Distance** [km]	**QBER** [%]
[50] [17]	InP	SiO_xN_y	BB84 (time-bin)	560M	345	20	1.0
			COW	0.86G	311	20	1.4
			DPS	1.72G	565	20	0.88
[128] [18]	Si	SiO_xN_y	COW	1.72G	916	20	1.0
		-	BB84 (pol.)	1G	329	20	1.1
[129] [19]	Si	-	BB84 (pol.)	9.71k	0.95	5	5.4
[130] [20]	Si	SOI	BB84 (pol.)	625M	157	43	2.8
[131] [21]	Si	Si	BB84 (time-bin)	100M	85.7	20	0.8
[132] [22]	-	SOI	BB84 (pol.)	10M	13.7	20	0.5
[58] [23]	InP	Si	DPS	1G	400	100	2.5
			BB84 (phase)		270	100	2.2
					618	75	2.0
[59] [24]	InP	Si	BB84 (phase)	1G	726	Direct	3.7
					28	50	6.2
[133] [25]	Si	-	BB84 (pol.)	312.5M	42.7	100	0.4
[49] [26]	-	Si_3N_4	BB84 (time-bin)	2.5G	20	125	3.0
This work	Si	Silica	BB84 (time-bin)	2.5G	1.3	152	3.3
[70] [27]					9.4	202	0.9

Table 4.7.: A selection of the state-of-the-art of integrated QKD. TX = transmitter, RX = receiver, SKR = secret key rate, QBER = quantum bit error rate, BB84 = Bennett-Brassard 1984 protocol, COW = coherent one-way protocol, DPS = differential-phase-shift protocol and pol. = polarisation-based.

work with previous ones. We consider this selection to contain the most pertinent systems to compare with the presented work of this chapter as they are the most similar in terms of protocol and implementation. The number and variety of them reflects the mature status of integrated photonics. The integrated QKD systems include either a fully integrated transmitter [50], a hybrid transmitter where the laser is off-chip [70, 128–131, 133], or where the laser is integrated but includes a fibre-based modulator [58, 59]. Only the work [49] presents a fully integrated receiver. In general terms it can be concluded that this integrated QKD setup performs within the state-of-the-art. Notably it has the highest clock rate and longest link among the integrated QKD implementations (to the knowledge of the author) and performs with high SKRs and low QBERs. Moreover, the loss of the integrated receiver chip of our setup is among the lowest compared to the works presented in table 4.7 [28]. Also, it is one of the few works that present a SKR with finite statistics, as opposed to an asymptotic SKR.

For the interested reader, further integrated QKD works can be found in the reviews [41, 42]. It should also be mentioned that integrated works based on *continuous variable* (CV)-QKD have been demonstrated, for example [134–138], as well as works based on *measurement-device-independent* (MDI)-QKD, for example [60, 139–141], or even integrated silicon photonics for daylight free-space QKD [142]. Additionally, the works [49] and [143] have presented integrated detectors, which would be extremely appealing as it would allow for an even more compact and

28. Only the work of [49] has lower loss, the corresponding platform is Si_3N_4.

thus practical QKD setup. However, both works made use of SNSPDs that were placed on a PIC, which had to be cooled down to cryogenic temperatures. This is not particularly practical, however the advancement of placing them in PICs is a great step forwards.

In conclusion, an integrated transmitter with characteristics of high-speed and accurate state preparation and an integrated receiver with low loss and polarisation independence were manufactured, characterised and used in an integrated QKD setup, allowing for high-quality secret key exchanges. This experimental implementation does not only encourage the use of integrated photonics for QKD purposes but is also a catalyst for further developments and improvements of this setup. The present work thus indicates clear benefits of using integrated photonics for QKD systems used for secure communications within fibre-based networks.

5. Integrated Quantum Random Number Generator

5.1. Random number generators

The usage and utility of randomness is well-established in society. Greek philosophers discussed its concept already hundreds of years BC and there is even evidence of games of chance that were played by different populations around 2100 years BC [1]. Since then, not only has the subject amused mathematicians, computer scientists, physicists and philosophers, but even become an extremely important tool in today's civilisation. Notably within the subjects of simulation, gambling and cryptography. The exact application of the randomness will define the importance of the quality of the RNG. What it exactly means for random numbers to have high quality is not straightforward to define, nor to actually verify. For now, we can start with saying that an event or number that is random is equal to it being unpredictable.

Going more into detail about the usages of RNGs. When performing a scientific simulation, for example Monte-Carlo, it is highly useful to use unpredictable data. The most important property of the randomness of the data is its uniformity and independence of the simulation algorithm. However, if this data is not generated with the highest quality of unpredictability, it is not an issue, as for such applications only a minimum amount of randomness is needed. For other applications, like a lottery, it is highly important to have high quality and secret random numbers as otherwise cheating would be simple. High quality random numbers are even more critical within the realm of cryptography as here the random numbers will define the security of the private communication. An example regards the generation of the pin of your bank card. The lower quality the random number has, the easier it is for a malicious party to guess it, which risks to threaten the security of your pin code. In this case, random numbers should be generated in the most unpredictable way as can be. Other applications of random numbers in cryptography also include its usage in QKD, where the choice of basis and state necessarily has to be random (see chapter 2).

We will now explain how such random numbers can be produced. The types of generators of random numbers can be categorised into two main groups, PRNG or TRNG [144].

1. `https://en.wikipedia.org/wiki/History_of_randomness`, visited: 09/07/2023.

5.1.1. Pseudo random number generators

PRNGs are devices whose random numbers are generated from deterministic algorithms. Such an algorithm will produce, from an input *seed*, a longer, random sequence of bits. A congruential generator is an example of such an algorithm [145]. It will produce random numbers from a recursive formula, such as

$$X_{n+1} = (aX_n + c) \textbf{ mod } m, n \geq 0, \tag{5.1}$$

where n refers to the position of the number in the random number sequence, m is the modulus, a is the multiplier and c is the increment [2]. The choice of parameters will define the period of the sequence of random numbers. It is essential that this period is as long as possible, to avoid repetition. Another example of PRNG is the function "random()" from the class "random" in the programming language Python. This function produces a random number from a deterministic algorithm. Its input seed is the time (to the nanosecond) of calling of the function.

Advantages of using PRNGs are their high generation rate and reproducibility, when used with the same seed. This is useful in the domain of scientific simulations for example, however in terms of cryptography and security, this is a huge disadvantage, as using the same seed would imply the same random number sequence. Additionally, if a malicious party gets hold of the algorithm and seed, they can produce the exact same number sequence in their laboratory and the sequence is no longer private.

One could use a generator which is based on an extremely hard problem to solve, which would make it more secure. This is the idea of the Blum-Blum-Shub generator [3] [146]. However, the security of this generator is not future proof as it could well be that someone comes up with a clever way to solve the problem in the future. Also, such problems could be solved in non-polynomial times with a quantum computer, applying Shor's algorithm [11, 12].

It is useful to apply a series of statistical tests to the generated random sequence to perform a quality check of its randomness. Here the periodicity, the autocorrelation and the frequency (proportion of 0s and 1s) for example, are tested. Examples of such tests are the NIST suites [147] or the Die-Hard tests [148]. It should be noted that there does not exist a way to fully check if a finite sequence is random because, by definition of randomness, the sequence 000000 is as random as 111111 and 101110. Implying that one is more random than another would imply that 0 is more random than 1. It is even possible, statistically, that an ideal RNG does not pass some of the tests. Thus, in order to produce *truly* random numbers, one should find a *truly* random mechanism and use it as a generator.

2. $m > 0, 0 \leq a < m$ and $0 \leq c < m$.
3. The recursive formula in question is: $X_{i+1} = X_i^2$, mod N, where $N = pq$ and p and q are two primes. Guessing X_{i-1} from X_i is computationally hard.

5.1.2. True random number generators

The other group of RNGs is the one of TRNGs. Such generators use an unpredictable (or very hard to predict) event to produce random numbers. We can further divide this group into two subgroups: classical or quantum RNGs. The former subgroup are based on events that are incredibly hard to predict or model with current day technology. For example, the motion of a computer mouse [4], thermal noise or atmospheric noise (weather linked for example). These are examples of chaotic systems, whose unpredictability is based on our ignorance of the system. Meaning that we do not have all the initial conditions to be able to model the system and perfectly predict its behaviour. Indeed classical physics is deterministic, the randomness arises from our lack of knowledge. Thus, in present-time, the generation of their random numbers is secure. But, it is possible that in the future we will manage to model such system with the use of a quantum computer, for example.

Thus, the need for an intrinsically random process is greatly desirable, ergo the interest of QRNGs. Such a RNG uses properties of quantum mechanics, that are fundamentally random, to produce a sequence of random numbers. Examples of quantum mechanical processes are the decay of a radioactive atom [21], vacuum fluctuations [25, 26] or the detection of a photon impinging on a beam splitter [22–24]. The usage of a QRNG is necessary when it is of uttermost importance to have pure and secret randomness, for example in cryptographic schemes, such as QKD.

Several QRNGs have been concretised, among the first going back almost 30 years [22–24, 149–151]. Since then many different types of QRNGs have been demonstrated. Notably, random number generation based on the detection of vacuum states in the work of [152] or random numbers originating from the interference of phase-randomised pulses in [153] and [154]. There has even been a QRNG implemented on a mobile phone by [27]. For a further information, we suggest the review of [155].

One way to describe QRNGs is through categorising them as a function of the implemented protocol. In general, this means defining the protocol as *device-dependent* (DD), *device-independent* (DI) or something in between, which is called *semi-device-independent* (SDI). In the first case, all experimental devices are assumed to be perfectly characterised and most importantly, not malicious. Examples of such implementations include all the above mentioned works. The DI case corresponds to the situation with the least amount of assumptions on the experimental setup. To be certain that the random number generation is quantum and safe, loophole-free Bell inequalities have to be violated under strict laboratory conditions [156]. Experimentally, this is complicated to achieve and when succeeded, only a low generation rate is possible [157–160]. In the DD case, we have to assume that all the manufacturers and even colleagues are honest, however a high rate of generation of random numbers is conceivable. The ideal case would be one where the level of security is high (like in the DI case), as well as the performance (like in the DD case). Their combination is often called the "sweet-spot", which is not trivial to achieve. The best compromise (in terms of security and experimental complexity) is to put ourselves in a place where few assumptions are made on the experimental setup while still being able to

4. One example website using this is: `http://www.russellcottrell.com/mousePointerRNG.htm`.

achieve high rates of random numbers. This corresponds to the SDI scenario. Figure 5.1 shows the relationship between the different regimes. Several works have established QRNG protocols in this regime and shown viable implementations, for example [161–164]. For the rest, we will consider this specific type of QRNG.

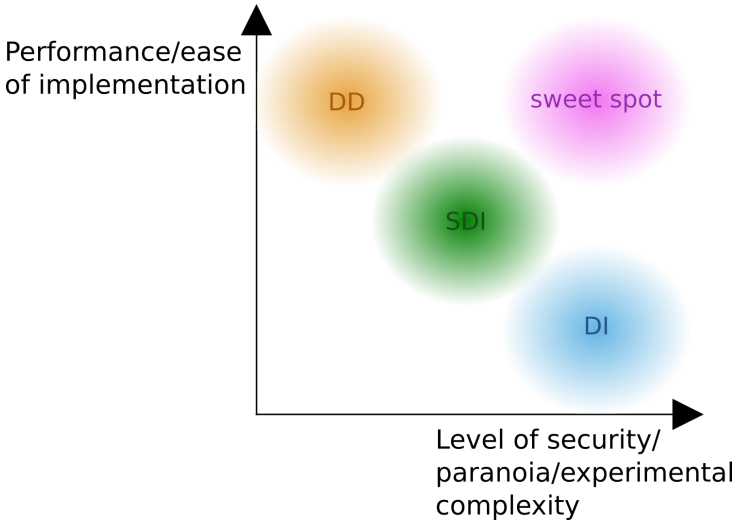


Figure 5.1.: Graph of the performance of the quantum random number generator as a function of the security level or experimental complexity showing the link between the different categories of QRNG protocols. DD = device-dependent, DI = device-independent and SDI = semi-device-independent.

5.2. Self-testing quantum random number generator

The SDI QRNG protocol presented in this chapter is based on works [71–73, 165] and theses [76, 166]. This protocol is also *self-testing*, such that the user can in real-time validate the production of the random numbers throughout the usage. Indeed, statistics generated from the experiment are used by the protocol to certify the entropy. The protocol thus allows for a reasonable rate of random number production, while keeping the level of security high.

5.2.1. Theoretical description of self-testing protocol

The protocol is set in a *prepare-and-measure* (P&M) scenario. A theoretical model of it is illustrated in the figure 5.2 below.

The input, x, of the *source* (S) or the "prepare" device, is binary, $x \in \{0, 1\}$. Depending on x, the source will prepare one of two possible quantum states, ρ_x. It is important to note that at least two different preparation choices of S and an additional assumption are needed as otherwise a classical modelling could fully describe the input and output behaviours. The *measurement* (M) device will output $b \in \{0, 1\}$.

The states, ρ_x, that are prepared are assumed to have a non-zero overlap. This means that

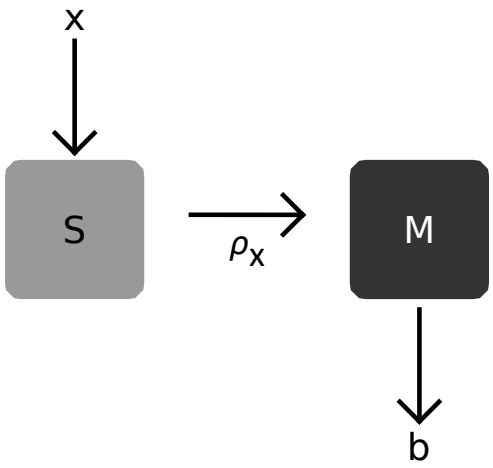


Figure 5.2.: Theoretical model of the QRNG setup. S = source, M = measurement, x = input, b = output and ρ_x = quantum state.

they are non-orthogonal, and thus cannot be perfectly distinguished, according to the laws of quantum mechanics. If we note the overlap as δ and the wave function of the states ψ_x, the overlap can be expressed as: $\delta = |\langle\psi_0|\psi_1\rangle| > 0$. The imperfect distinguishability gives rise to probabilistic results of detection, which are inherently quantum and can be used to certify the quantum randomness of our device. An intuitive representation of the states is shown in figure 5.3, where $\psi_0 = \sqrt{1-a^2}\,|+\rangle + a\,|-\rangle$ and $\psi_1 = a\,|+\rangle + \sqrt{1-a^2}\,|-\rangle$.

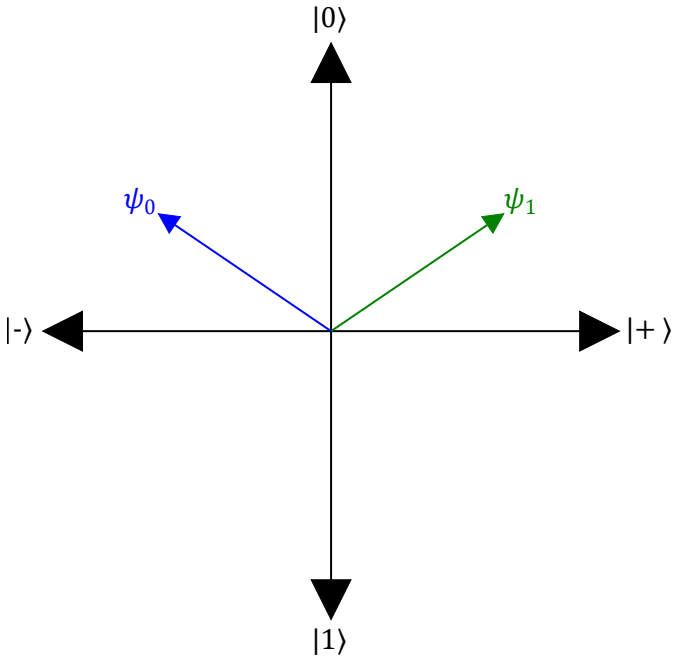


Figure 5.3.: Representation of two possible prepared states (ψ_0 and ψ_1) with an overlap δ, in the $X - Z$ plane of the Bloch sphere.

It is possible to entirely describe the joint behaviour of the devices, meaning the outcome b depending on the input x, according to the equation

$$p(b|x) = \mathrm{Tr}[M_b \rho_x], \tag{5.2}$$

where M_b corresponds to the measurement performed on the state. Therefore, in this particular scenario, the four probabilities [5] characterise completely the joint behaviour of S and M.

In a more general scenario, it is possible that the devices S and M are correlated due to classical noise. Therefore, a more generalised way of representing equation (5.2) exists. The correlation of S and M is represented as λ, an unknown parameter. This classical noise has to be correctly separated with the quantum one, in order to be sure that the produced bits are generated from quantum randomness. For each possible correlation λ, there is a given relationship between S and M. Equation (5.2) can be re-written as

$$p(b|x) = \sum_{\lambda} p_\lambda \mathrm{Tr}[M_b^\lambda \rho_x^\lambda]. \tag{5.3}$$

In order to be able to describe the behaviour of S and M with quantum mechanics, an additional assumption has to be made. According to the work of [73], an upper bound on the average energy of the two states should be set. This is called the *average energy* assumption. We can write the upper bound of the energy of each state as

$$\omega_x = \sum_{\lambda,x} p_\lambda \mathrm{Tr}[N \rho_x^\lambda] \leq \omega. \tag{5.4}$$

Here ω_x is the average mean photon number of the states, N is the photon-number operator and ω is the upper bound on the average energy. N corresponds to a measurement of the number of photons in a given mode with energy $\hbar\omega_x$. Thus, representing the total energy in that mode. The interest of making an "average"-type assumption is that the corresponding physical quantities [6] can fluctuate, as long as the mean value does not exceed the bound over the round. In terms of experimental verification of the assumption, it is enough to use a well-characterised, and thus trusted, powermeter. Hence this protocol does not need any precise knowledge of M and only partial knowledge of S, rendering the setup SDI.

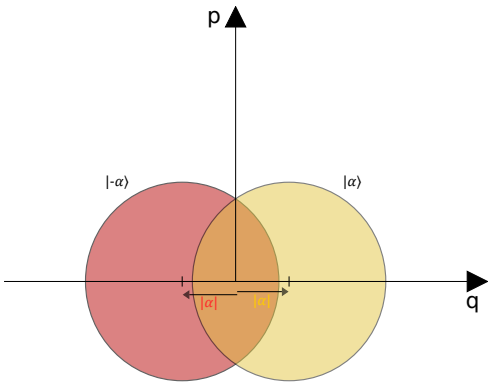
The first step of the protocol is therefore to make sure that the states have an overlap in energy. This is measured by monitoring their average energy throughout the rounds and verifying that it does not exceed the given upper bound. The next step is to make certain that the probabilities $p(b|x)$ belong to the set of quantum correlations and not deterministic correlations [7]. To do this, a *semi-definite program* (SDP) is used, which returns a lower bound on the conditional Shannon

5. $p(0|0), p(1|0), p(0|1), p(1|1)$
6. In this case the energy of a given photon.
7. The work of [72] proved that the quantum set of correlations is bigger than the classical one.

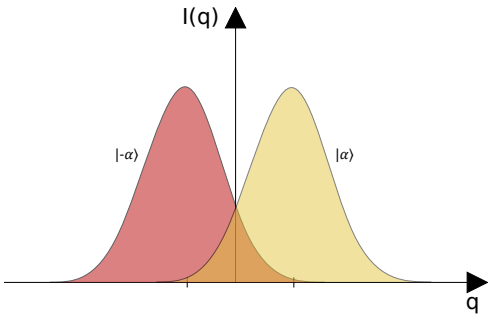
entropy, $H(B|X,\Lambda)$, where B is the set of outputs and Λ is the set of deterministic correlations. The exact working of the used SDP is beyond the scope of this thesis, we refer to the work [72]. A linear witness [8], which includes ω and the measurement statistics, $p(b|x)$, is then created and used to verify the working of the setup after a selected n number of rounds [9]. The witness is upper bounded by $H(B|X,\Lambda)$ and should be lower bounded by a certain entropy h, fixed in the beginning of the measurement. The choice of the optimal h is based on the number of extractable bits per generated state and the number of successful rounds. If the witness follows this bound throughout the n rounds, the results are certified with quantum randomness. The number of bits from the raw sequence that can be used for extraction is given by H_{min}, the worst-case conditional smooth min-entropy. H_{min} is estimated from ω and $p(b|x)$. We refer to the works [71, 73, 165] for more information. The randomness extractor is used to provide a sequence of uniformly random numbers. It will also balance any bias among the bits, for example due to noise. Different types of extractors can be used, for example the Toeplitz algorithm [167].

5.2.2. Experimental implementation of the self-testing protocol

It was found in the work of [71] that a practical way of implementing this protocol is through using the *binary phase-shift keying* (BPSK) scheme and homodyne detection. The two coherent states that are generated by the source are $|\alpha\rangle$ and $|-\alpha\rangle$, where $|\alpha|^2$ is the mean photon number. Their visualisation, including their overlap is showed in figure 5.4.



(a) Representation of the prepared states $|\alpha\rangle$ and $|-\alpha\rangle$ in the phase space.



(b) Representation of the intensity of the q-quadrature of the prepared states $|\alpha\rangle$ and $|-\alpha\rangle$.

Figure 5.4.: Graphs representing $|\alpha\rangle$ and $|-\alpha\rangle$ and their overlap.

The two states are differentiated by their phase difference, $\phi = \pi$. A phase modulator can be used to produce them. The input x, going to the source, will define the phase of the state, i.e. $x = 0 \rightarrow \phi = 0$ and $x = 1 \rightarrow \phi = \pi$. Regarding the measurement, the most optimal way (in terms of performance and practicality) of discriminating the two states (to obtain $b = 0$ or $b = 1$) is through using a homodyne detection scheme [10]. Such a scheme is based on the interference of the prepared states, called the signal, with a strong light field, called the *local oscillator* (LO), on

8. Extracted from the dual of the SDP.
9. Further information is found in [71, 72].
10. For further discussions, we refer to the thesis [76].

a perfectly balanced beam-splitter, in a bal-MZI. The interference is measured by a photodiode (linear detector) placed in each arm of the beam-splitter. These detectors are connected such that the output signal corresponds to their difference of output, which is proportional to the quadrature of the states. From the figures in 5.4, the two states are different in terms of their phase (q-axis). Their phase difference is π, thus they are centered at $-\pi/2$ and $\pi/2$, $|-\alpha\rangle$ and $|\alpha\rangle$, respectively. Photons that live in the overlap, will not be distinguished without a minimum amount of errors, which will occur truly randomly. Photons living outside the overlap will, on the other hand, be able to be distinguished perfectly.

The full experimental setup was chosen, following the work of [71], to include a continuous wave laser, connected to the input of a bal-MZI. In the signal arm, there is a phase modulator, a beam-splitter, a powermeter (to monitor the average energy of the states) and a VOA (to attenuate down the light such that they have an overlap in energy). In the LO arm, there is a phase shifter, to stabilise the phase of the interferometer. A pair of linear detectors are connected to the output of the bal-MZI, which will perform the homodyne detection. Necessary electronics to discriminate the output analog signal (b) should in this scenario also be thought of, as well as the electronics of the input signal (x) to the phase modulator. The schematics of the proposed experimental setup is presented in figure 5.5.

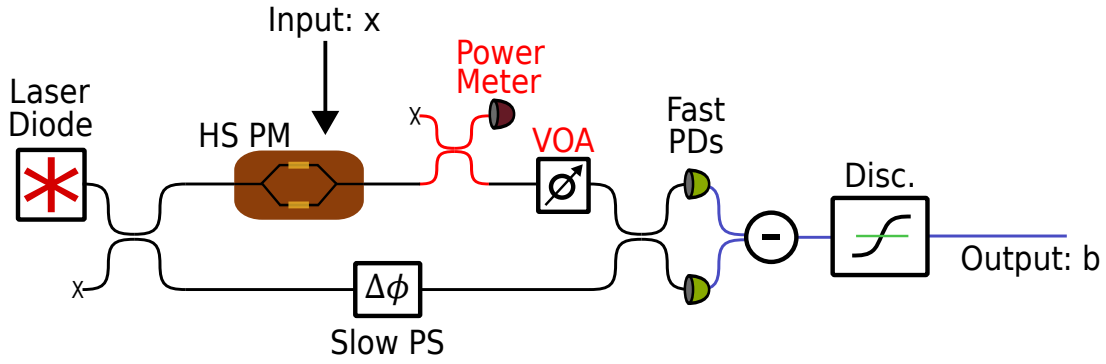


Figure 5.5.: Experimental setup of the described self-testing protocol. HS PM = high-speed phase modulator, PS = phase shifter, VOA = variable optical attenuator, PD = photodiode and Disc. = discriminator. Components and text in red correspond to parts that have to be characterised.

It is important to define what has to be characterised for the experimental setup to work with the self-testing protocol we present. Performing the experiment with the simplified, but sufficient, setup presented in figure 5.5 requires the characterisation of some elements, to verify the average energy of the states and their overlap. This includes the beam-splitter placed after the phase modulator, the powermeter and the VOA (in red in figure 5.5). The rest of the components do not have to be characterised, but of course function. If they do not, there is no problem of security of the self-testing protocol. Depending on the malfunction, the conditional probabilities will just not pass the witness tests or the bound on the energy and no random sequence will be produced, such a sequence will be discarded.

5.2.3. Example of experimental implementation of the self-testing protocol

The presented self-testing protocol has been implemented in a fibre-based setup in the work of [71], its experimental setup is represented in figure 5.6.

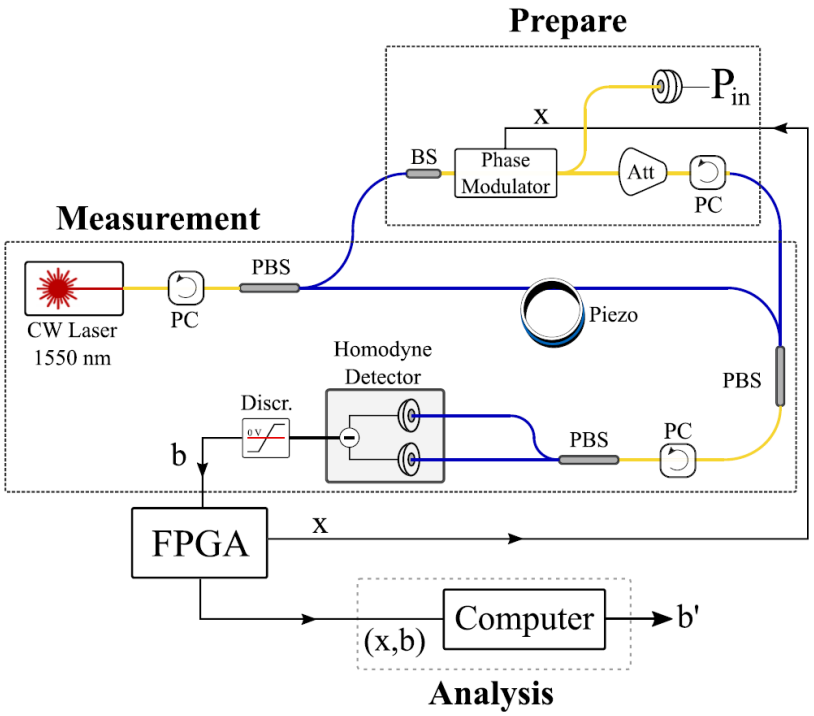


Figure 5.6.: Fibre-based implementation of the self-testing SDI protocol. Image taken from [71]. CW = continuous wave, PC = polarisation controller, PBS = polarising beam-splitter, BS = beam-splitter, Att = optical variable attenuator and Disc. = discriminator.

The phase stabilisation of the interferometer is done via a Piezo controller. The additional components of the setup in figure 5.6 that were not mentioned in the setup of figure 5.5 are the polarisation controllers and *polarising beam-splitter*s (PBSs). This experiment showed a quantum random number repetition rate of 145.5 MHz.

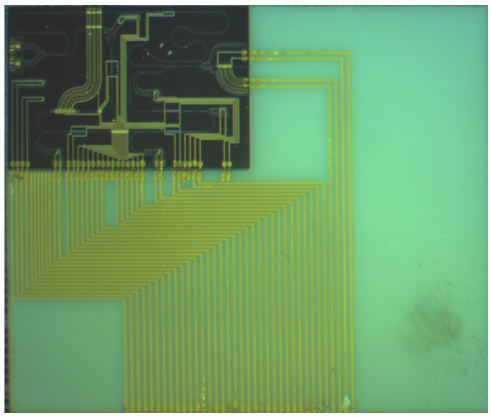
Recently, we started characterising and implementing the self-testing protocol on a PIC, which hosts all the optical components of the setup in figure 5.5. There are several advantages of doing this. One of which is that we do not need any polarisation controllers nor PBSs anymore, rendering the experimental setup simpler. In the next section we will present the integrated QRNG PIC and show a selection of the first important characterisations, necessary for the full implementation.

5.3. Integrated experimental setup for the self-testing protocol

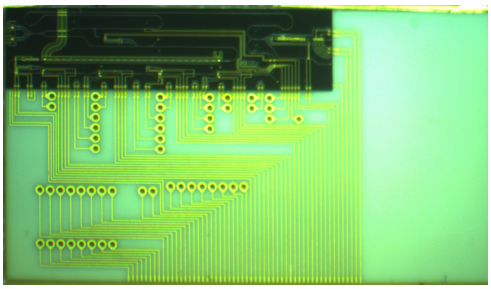
There are many reasons for integrating the QRNG setup, presented in figure 5.6. For example, it would bring about the lowering of costs, power consumption and size of the full QRNG setup. Other reasons include, improved scalability and stability, as well as an uncomplicated installation during production [11], giving rise to a smoother adoption for industrial usages (for example cryptographic services). Several works have already undertaken the challenge of integrating a QRNG setup on a PIC [168–171]. The works [169, 170] present a QRNG based on phase fluctuations of a laser diode in *silicon on insulator* (SOI). Given the material chosen, the laser in these works is not integrated. The work [168] integrated a QRNG in InP, based on two-laser interference and heterodyne detection. Finally, the work [171], implemented a SDI QRNG based on a heterodyne receiver in SOI, with the laser, VOA and polarisation controller not integrated. In the following we will present the layout of our proposed QRNG PIC which is designed to function as the fibre-based setup presented in figure 5.5, with all necessary optical components integrated in a PIC.

5.3.1. Design of the photonic integrated circuit

The QRNG PIC is based on InP and is designed and manufactured in collaboration with Fraunhofer Heinrich-Hertz-Institut (HHI). The PIC is placed on an interposer in ceramic which includes pads on the edges to bond the chip to an in-house-made PCB. Two versions of the PIC were made, one for fast modulation ($\sim$ 2.5 GHz) and one for slower modulation ($\sim$ 200 MHz). The modulation of the fast chip is two times faster than the fibre based experiment [71]. Images of the two PICs taken with a camera that is placed on a microscope can be found in the figures 5.7a and 5.7b below.



(a) Slow QRNG PIC in InP on its interposer.



(b) Fast QRNG PIC in InP on its interposer.

Figure 5.7.: Images of the fast and slow PICs. The gold lines are electrical connections from the PIC to the bonding pads.

11. Only one discrete optical component has to be assembled in a future final product.

The sizes of the slow and fast chips, including the interposer, are around 12 mm × 10 mm and 18 mm × 10 mm, respectively. The schematics featuring the optics of the fast PIC is presented in figure 5.8.

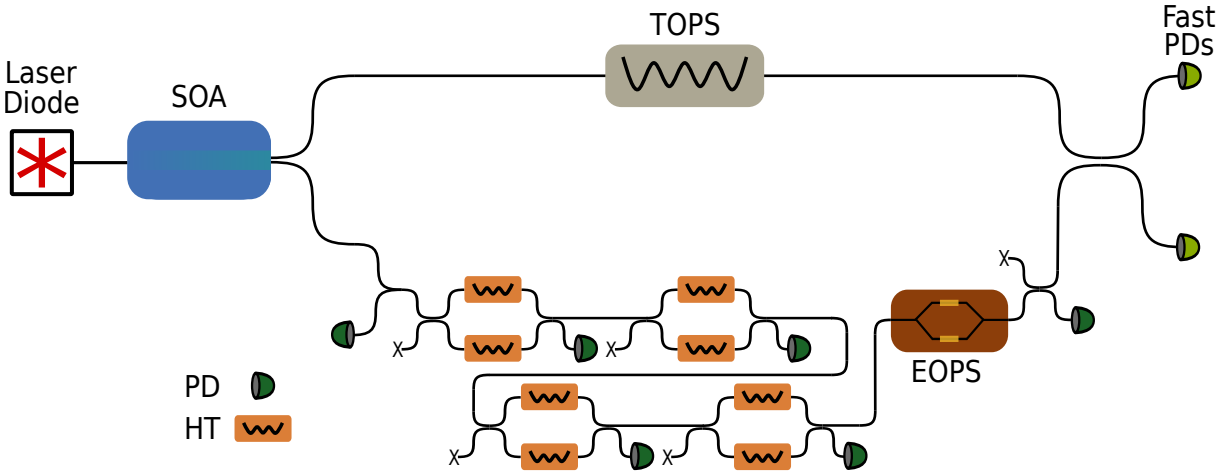


Figure 5.8.: Schematics of the fast QRNG PIC. SOA = semiconductor optical amplifier, TOPS = thermo-optic phase shifter, EOPS = electro-optic phase shifter, PD = photodiode, HT = heater.

The fast chip includes a DFB laser which is operated in continuous mode via a laser driver from Thorlabs [12]. The driver controls the injected current. At a current of 150 mA, the laser furnishes around 5 mW of power, according to manufacturer specifications. A heater connected to the laser allows to change the wavelength of the laser. According to the manufacturer, the range of wavelength change is around 3 nm, relative to the wavelength at the threshold. The intensity of the light can be amplified via the usage of a *semiconductor optical amplifier* (SOA). The SOA can provide a gain of up to around 20 dB. As it is employed, it amplifies around 10 dB according to the specifications. Light then enters a bal-MZI, as previously explained in section 5.2.2. Via a beam-splitter (50/50), light is sent either through the upper arm (the LO) or the lower arm (the signal). Light going through the upper arm will pass through a TOPS, which is placed to stabilise the phase of the interferometer. Light passing through the lower arm will pass by four VOAs consisting each of a balanced MZI, including heaters in each arm. These are used to attenuate the signal to the desired level. Before recombining with the LO, the signal light passes through an EOPS, which is modulated at 2.5 GHz. The EOPS also includes a bias section in order to improve the phase modulation. According to the manufacturer less than 8 V is needed to achieve a π phase shift. Arriving at the final beam splitter (50/50), the LO and the signal interfere and travel to the fast PDs. These detectors are connected electronically together such that the output signal corresponds to the difference in current of the two detectors. The fast PDs are bonded to an electrical amplifier circuit, specifically designed to be able to record the minuscule signals coming from the homodyne detection (order of nV). More information about the design of the amplification circuit is found in section 5.3.3. Slow PDs are placed at various locations in the PIC (coupled to the waveguide or isolated from it) to be able to monitor the flow of light as well as to characterise the components that need characterising, more information in section 5.3.4.

12. Miniature Laser Driver, MLD203CLN.

The schematics of the slow PIC are similar to that of the fast PIC, the only difference being that it does not include a bias section for the EOPS nor an SOA. The schematics of the slow chip is found in the appendix, figure D.1.

Given the many components present on the PIC, it can easily heat up when used. Hence, proper mechanics and electronics for cooling had to be thought of. We made use of a large (40 mm × 40 mm) and powerful Peltier [13] and in-house-made radiators. The combination allows for a satisfying temperature control and stabilisation when used with a TEC driver from Thorlabs [14].

5.3.2. Design of the electronics

The concept of the full integrated QRNG setup, including the electronics is presented in figure 5.9.

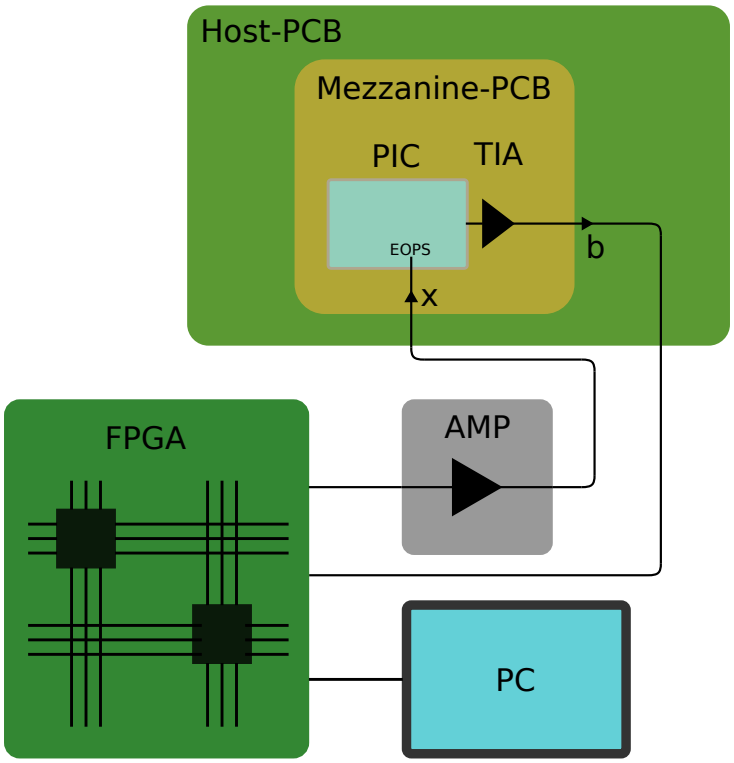


Figure 5.9.: Schematics of the electronics of the integrated QRNG experimental setup where x and b correspond to the input and output, respectively. PCB = printed circuit board, PIC = photonic integrated circuit, AMP = amplifier, TIA = transimpedence amplifier, EOPS = electro-optic phase shifter, FPGA = field-programmable gate array, PC = personal computer.

Figure 5.9 gives a visual overview (not to scale) of the full experimental setup. It can be noted that very few discrete components are actually needed, as the setup consists of only one host-PCB,

13. Wakewield-Vette TEC-40-33-127
14. MTD415T

an external amplifier [15], an FPGA [16] and a PC. The FPGA provides a binary pseudo-random sequence. The signal of the sequence is amplified by the external amplifier before arriving at the EOPS of the PIC. This corresponds to the input x. The PIC is responsible for the generation of light and the homodyne measurement. The *transimpedance amplifier* (TIA) is responsible for the production of a measurable signal. The output signal, b, is sent to the output circuit, where it is discriminated and sent to the FPGA. The FPGA is responsible for storing the relative frequencies $p_f(b|x)$ [17]. The analysis and extraction of the random numbers are done with the PC. The main PCB includes a micro controller [18] which is used with the PC to control the slow components of the PIC, meaning the heaters and the slow PDs. The host-PCB is powered with a 12 V and 1 A and supplies all components of the PCBs.

5.3.3. Design of the transimpedence amplifier

The signal coming from the homodyne detection that we are interested in measuring is extremely weak, order of the nV, as it corresponds to the difference in signal of the two PDs. In order to detect such a signal with a standard oscilloscope, it is thus necessary to properly amplify it. The amplification process is done with a TIA circuit. It will convert the weak input current to a measurable voltage. A simplified schematic drawing of the situation is depicted in figure 5.10.

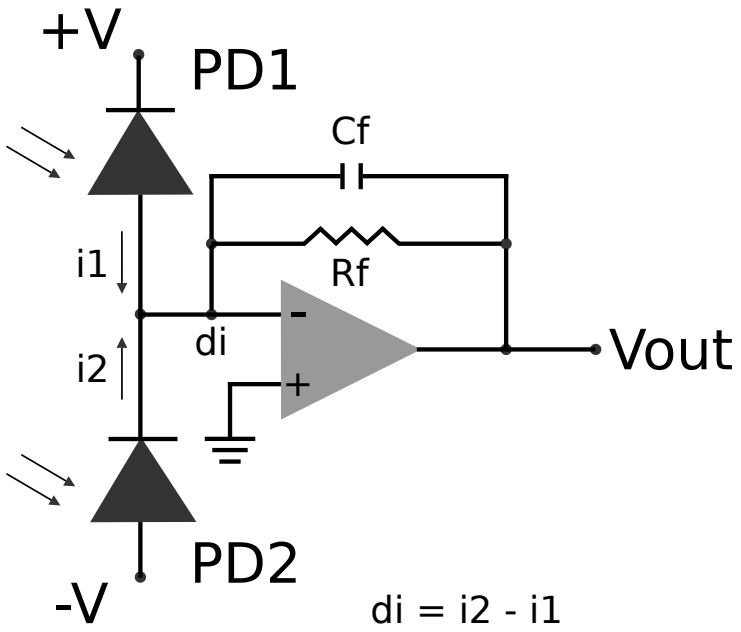


Figure 5.10.: Simplified schematic of the amplifying circuit and the homodyne detection including the subtraction of the output signals from the PDs. PD = photodiode, i represents the current flowing from either PD and di their subtracted signal. Cf and Rf are the feedback capacitance and resistance, respectively. ±V corresponds to the respective biases of the PDs and Vout represents the output voltage after the TIA.

15. iXblue DR-AN-10-HO
16. Virtex-6
17. $p_f(b|x) \cong \frac{n_{b,x}}{n_x}$, where $n_{b,x}$ is the number of counts of b when x is sent and n_x is the total number times x is sent, which corresponds to what we will experimentally record.
18. Teensy 4.1

Figure 5.10 shows how the two photodiodes (PD1 and PD2), performing the homodyne detection, are connected such that the input current to the *operational amplifier* (OP-AMP) is equal to the difference in output current of the two (noted di). Notably, PD1 is connected with the cathode to ground and PD2, anode to ground. The feedback resistance (Rf in figure 5.10) will dictate how much amplification the TIA circuit will bring about [19]. The output voltage (Vout) is sent to the output circuit where the voltage level will be discriminated before being sent to the FPGA.

Since the TIA is amplifying a weak signal, it is important to minimize any noise entering it, as this will also be amplified and therefore worsen the *signal-to-noise ratio* (SNR). The noise sources of the TIA include thermal noise, $1/f$ noise and electrical shot noise. For the interested reader, the work of [172] studied the noise effects in a homodyne detection scenario with a TIA. Additionally, maximising the bandwidth of the TIA is also an important task as it is directly proportional to the achievable detection rate of the homodyne detector and so also the maximum rate of generation of random numbers. The bandwidth is inversely proportional to the total capacitance of the circuit (C_{tot}) [172], hence the TIA circuit has to be designed to minimise C_{tot}. The total capacitance includes the individual capacitance of the PDs and that of the OP-AMP. Additionally, any parasitic noise from the PCB will increase C_{tot}, hence the placement of the components is carefully thought of. Notably, the TIA circuit is placed as close to the PIC as possible. A photo of the design of the PCB hosting the PIC and TIA is shown in figure 5.11.

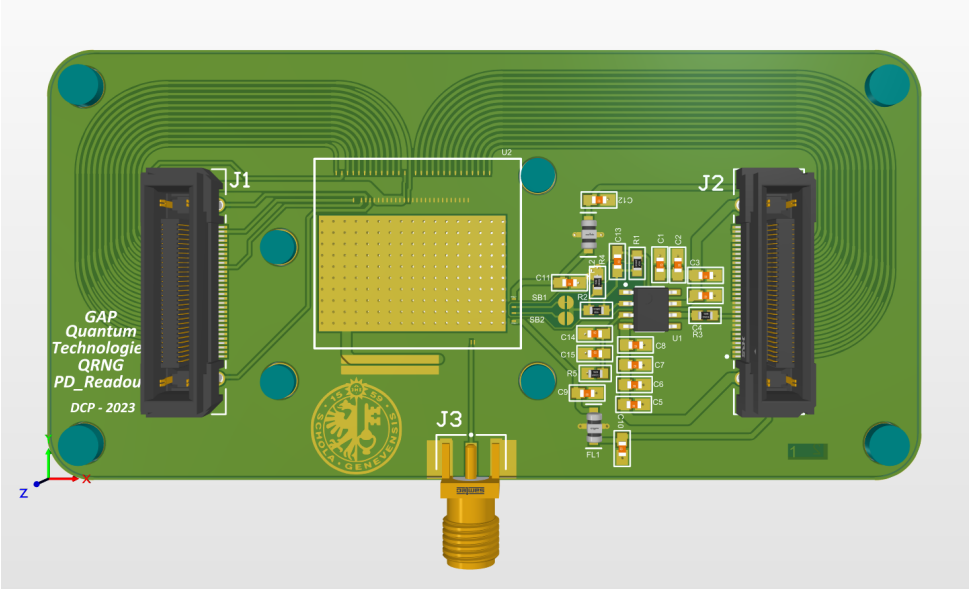


Figure 5.11.: 3D drawing of the mezzanine PCB which hosts the PIC and TIA. Its dimensions are 10 cm × 5 cm. The PIC is glued on to the gold rectangle.

We opted for a design with the PIC on a smaller PCB, which is called the mezzanine where the TIA circuit is also placed. The mezzanine also includes a *sub-miniature version A* (SMA) connector where the 2.5 GHz pulses coming from the FPGA enter and via bondings arrive at the EOPS. The mezzanine is connected to the host PCB via a set of connectors [20].

19. More precisely the gain (G) can be defined as: $G = V_{out}/V_{in} = R_f/R_{in}$, where R_{in} is the input resistance.
20. FX23-60S-0.5SV from Mouser Electronics.

The choice of the OP-AMP is therefore crucial for the correct functioning of the amplification part. Given that we aim for working at rates of 2.5 GHz for the fast PIC, a high bandwidth OP-AMP is needed. Furthermore, low noise and high gain is required. We thus went for the OPA847 from Texas Instruments that carries precisely the desired features [21].

5.3.4. Plan of integrated self-testing QRNG experiment

We will here present what components of the integrated QRNG setup need to work well or be characterised with respect to the assumptions we make, as well as how we will do it. Firstly, we focus on the TIA and its circuitry, as the first step for the experiment to work is to make sure that the readout from the homodyne measurement is done properly. The main characteristics that should be measured are the *quantum to classical noise ratio* (QCNR) and the bandwidth of the circuit. The former is equal to the clearance of the detectors. It has to be high as its performance will be proportional to the detection capability of the system. The latter characteristic should be higher than the speed of our system (2.5 GHz). Due to of lack of time, these physical quantities have not yet been measured with the PIC. However, other characterisations of the TIA circuit could be performed on a "test"-TIA PCB. These are presented in section 5.4.1.

Another important part of the setup is to be able to measure the mean photon energy, that is assumed to not exceed a certain bound. In the setup in figure 5.5, this was done by placing a characterised beam-splitter and powermeter after the phase modulator. In the case of the integrated setup, the laser, the detectors and all other components, including all waveguides are integrated. Hence there is no way of measuring whatsoever with an external instrument (like an external laser or powermeter). Fortunately, there are a handful of PDs in the PIC, which are either coupled to the waveguide, or located away from the waveguide. We will utilise these detectors as powermeters within the PIC. Since we don't even have the knowledge of the amount of optical power that comes out from the laser (despite from the specifications of the manufacturer), we must find another way of characterising the signal coming from the PDs.

Characterising the output signal of the PDs is equivalent to characterising their readout circuit, which is composed of an OP-AMP and an ADC. From the ADC we obtain a number, which we call "PD value". It is situated between 0 and 2^{15} and corresponds to a certain current that is produced by the PD. This current is linked to the impinging optical power via the sensitivity (in [A/W]), given by the manufacturer, notably 0.8 A/W. We thus decide to trust the manufacturer on this value, as well as on the splitting ratios throughout the PIC, which are all 50/50. In order to know the optical power, we have to link the output PD value with an input current, and then via the sensitivity, calculate the optical power. This is thus a crucial characterisation to make to be sure the average energy assumption is held true. The corresponding measurements and characterisation is presented in section 5.4.2. To be sure we are not underestimating the energy, and so violating the bound without realising, we will take into account a margin of security on the energy we measure [22].

Another important characterisation to make to be sure our states are at the desired mean photon

21. It's gain bandwidth product is 3.9 GHz.
22. This means lowering the bound more than necessary.

number and have an overlap in energy concerns the four MZIs with their respective heaters. The job of these components is to attenuate the signal by setting the phase of the MZIs, using the heaters. Thus, a careful characterisation of the ER of each MZI has to be done. We then have to assume that the total ER of the four MZIs is equal to the sum of their ERs [23]. The behaviour of each MZI is done by measuring the output power (using the corresponding PD connected to the waveguide) as a function of the current flowing through a given heater of the MZI. Due to time constraints, this characterisation is not yet completely finished, thus it is not presented in this chapter.

5.4. Preliminary measurements

5.4.1. TIA characterisation

Before designing the full PCB of the experimental setup, we created a separate PCB for the amplifying circuit (TIA) and performed some preliminary characterisations. This was done completely without the previously described PIC. Photodiodes from Koheron [24] were souldered on the TIA-PCB, such that their output currents are subtracted and their difference enters the OP-AMP of the TIA. The experimental setup that is necessary to perform the characterisations of the QCNR and the bandwidth is shown in figure 5.12. The laser is used in continuous mode and comes from Gap Optique [25] and the VOA is from Exfo [26].

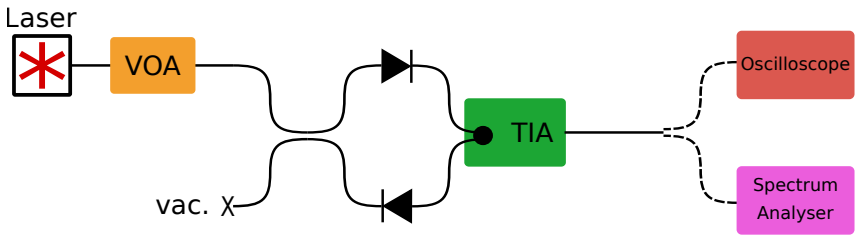


Figure 5.12.: Schematics of the experimental setup to test the working of the TIA-PCB. VOA = variable optical attenuator, TIA = transimpedence amplifier and vac. corresponds to the vacuum state (this input was blocked).

A similar experimental setup to the one in figure 5.12 was used for the characterisation performed on the test-TIA. Namely, to check that the two photodiodes have similar responsivity (0.8 A/W according to the manufacturer) and work in the linear regime [27]. This will be reflected in their graph of the output voltage as a function of optical input power, where the two detectors should have the same behaviour. This is the case if their graph is symmetric over the x-axis. Their behaviour can be quantified via the absolute value of the slope of their respective curves, which should be equal to the gain of the TIA circuit. We thus measure the output voltage at different

23. As the PDs are not sensitive enough to measure low optical powers of around -60 to -80 dBm.
24. https://www.koheron.com/photodetectors/
25. Gap Optique no longer exists is now bought by Exfo.
26. Model: FVA-3100.
27. The output voltage should be proportional to the quadrature signal.

input powers for each detector individually. This means that the detector that was not under test was shielded from any incoming light [28]. The corresponding experimental setup is therefore the same as in figure 5.12, but with only one detector connected at a time. The obtained graph is presented in figure 5.13.

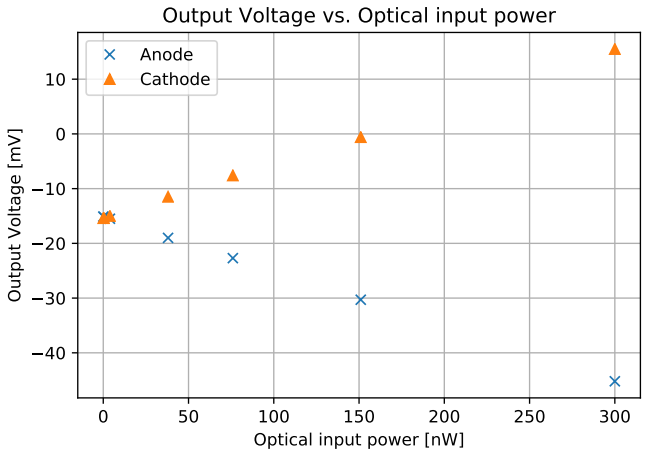


Figure 5.13.: The output voltage as a function of the optical input power of the anode and cathode photodiodes connected to the TIA circuit.

The electrical noise level is at -15.0 ± 0.1 mV. By fitting the curves, the absolute value of the slopes of the anode and cathode, respectively can be found: 0.1003 ± 0.0007 mV/nW and 0.10232 ± 0.0007 mV/nW. Indicating thus that both detectors operate in slightly disperse manners [29]. The gain of the TIA circuit is thus found to be around 100 k [30]. This corresponds well to the value of the feedback resistance that is used.

We will make a comment on the future measurement of the QCNR, linked to the clearance. The QCNR should be as high as possible, as it will improve the detection capability and so improve the generation rate of random numbers. The setup that should be used to perform this measurement is equal to the one in figure 5.12, using the oscilloscope. A range of optical powers should be sent in the LO arm and the noise variance (in $[\text{mV}]^2$) should be recorded. The total noise variance is equal to the sum of the electronic and the quantum one, where the electronic noise comprises the background noise of the oscilloscope as well as the TIA circuit, including the detectors. The maximum QCNR would be found at the highest optical input power. Examples of QCNR measurements with a similar TIA circuit and homodyne detectors to the one proposed here is found in [26, 173].

To understand the working bandwidth of the TIA circuit, we performed a measurement of the noise power as a function of frequency using a spectrum analyser [31]. However, we could unfortunately not go above 1 GHz with this device, hence we do not know the limit of the amplifying

28. In practice this means, not connecting one of the fibres of the beam-splitter to this detector and placing a cap on the input of the shielded detector.
29. If these were the ones that would be used for in the experimental circuit, more characterisations would be worth performing.
30. From the slope (m) we obtain the gain (G) from: $G = m \cdot 10^{-3}/10^{-9}$.
31. Anritsu MS9710C.

circuit. According to the OP-AMP used, we should be able to go to around 3.9 GHz. For the interested reader, the graph of noise power as a function of frequency is presented in the appendix, figure D.2.

5.4.2. Slow photodiode characterisation

As previously discussed, all the optical components of the experimental setup are integrated, it is therefore necessary to properly characterise the slow PDs. They are the sole available powermeters and will thus be used for monitoring the optical power throughout the PIC. The readout of the PDs can be visualised with the flow diagram in figure 5.14.

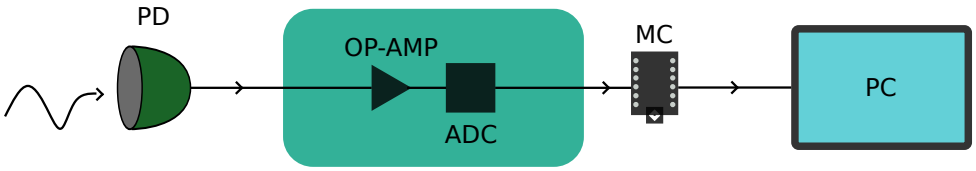


Figure 5.14.: Flow chart of slow photodiode readout scheme. PD = photodiode, OP-AMP = operational amplifier, ADC = analog-to-digital converter, MC = micro controller, PC = personal computer.

The optical signal arriving at a given PD will be converted to a current, which will be amplified with an OP-AMP [32] and converted to a digital signal via an ADC [33]. Through the usage of a microcontroller we can read a corresponding "PD value" on the PC. This value situates itself between 0 and $2^{15} = 32768$, where 0 corresponds to no optical input power and 32768 the maximum optical input power before saturation. A characterisation of the "PD value" and the optical input power is thus necessary. We performed such a characterisation by connecting a sourcemeter [34] directly to the OP-AMP (the PIC was not connected) and recording the "PD value" for a given input current. Using the responsivity of the PDs given by the manufacturers, 0.8 A/W, the "PD value" can be converted to an optical power. An example of characterisation of the first PD after the laser is shown in figure 5.15.

We noticed that the "PD value" slightly fluctuates for each measurement point, therefore values were taken during 30 s intervals to obtain an average. To understand the relevance of the fluctuations, we plotted the maximum, minimum and average values during each 30 s time period. From the graph in figure 5.15 it is thus clear that the fluctuations are minor. It can also be concluded that our photodiodes are sensitive in the regime around -25 dBm to -49 dBm. The corresponding current range, which is proportional to the x-axis, is from $0 - 2.6\ \mu$A.

32. OPA380
33. MCP3428
34. Keithley 2400

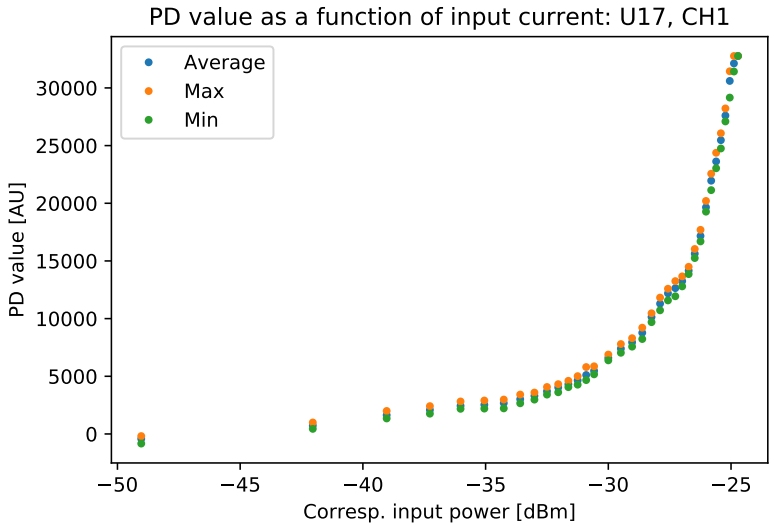


Figure 5.15.: The PD value as a function of the corresponding input power for the first photodiode after the laser.

5.5. Discussion

This project is still ongoing, thus an intermediate conclusion will me made and future measurements will be discussed. For now, the development of the necessary electronics has taken place. This includes the control of all the slow components as well as the output amplification circuit. The readout circuit of the PDs has also been characterised. The PDs can thus be used as powermeters for monitoring the flow of light in the PIC as well as for characterising other components. Future measurements include the characterisation of the MZIs, particularly their heaters and the corresponding ERs they can achieve. Later on, the EOPS in combination with the external amplifier and the fast detectors with the TIA circuit, should also be tested.

From the experimental tests that have been done, we can conclude that integrating all the optical components of the QRNG setup does render the experimental setup simple to handle. In particular, there is only the need of one host-PCB, and only one source of power. Also, there is only a single micro-controller which is connected to the computer, thus through the use of a single program we can control every component of the PIC. Not only is it practical from the point of view of a researcher that has to characterise the various components, but also from the point of view of a worker in the production of a company wanting to sell such a system. Indeed, given that all the components are integrated, much fewer components have to be placed in the designated product package. This also allows the package to be smaller, and thus more practical. In the long run a decrease in costs and so price of such a product would also take place, thanks to the decrease in assembling time, the amount of material needed for the package and most importantly, the price of the PICs, which is inversely proportional to the amount that are made [35].

35. Until the law of diminishing returns is reached.

6. Conclusion

The domain of quantum communications is getting more recognition than ever due to the imminent menace of the security of classical communication schemes. There is a risk that Shor's factoring algorithm [11, 12], let run on a quantum computer, breaks the security of the currently applied public-key encryption algorithms (for example RSA [10]). Therefore, other methods of secure communication have to be thought of. Since the first idea of a quantum communication protocol, whose security is based on the laws of physics [64] (a QKD protocol), the requests of quantum communications and technologies have considerably expanded. As a consequence, the research in this field has grown to a point where a motivation is to accommodate the technology in present-day communications networks, which is precisely the interest of the presented thesis.

The main work of the thesis involved implementing the 3-state BB84 protocol with 1-decoy state [65, 66], previously implemented in a fibre-based setup [67, 86], in an integrated photonics experimental setup. On the transmitter side, a PIC and an EIC, both in silicon photonics, were designed and manufactured in collaboration with IDQ SA and Sicoya GmbH. The integrated transmitter, including an external laser, displayed excellent performance in terms of high-speed and accurate state preparation. These are precisely the demanded requirements for this part of the setup. On the receiver side, two different platforms were examined, one in silica and the other in silica on silicon. The former was designed and manufactured in collaboration with the group of Roberto Osellame at CNR-IFN in Milano and the latter, with VLC photonics. The silica platform was employed for the secret key exchanges, thanks to its low loss and polarisation independence. Both characteristics are paramount for achieving high SKRs the QKD system. The SKRs, obtained with external SNSPDs or SPADs, that lead to the work [70], correspond to the state-of-the-art within integrated photonics (for detailed comparisons we refer to table 4.7). The integrated QKD system also presented similar performance with respect to its fibre-based analogue [67, 86]. We hope that this work [70] will stimulate future research within, and outside, the group, as well as encourage the commercial development of QKD systems based on integrated photonics.

The development of the presented integrated QKD system into a ready-to-use prototype is a natural next step of the project [1]. The integrated system of this thesis is a proof-of-concept, where a QKD system based on integrated photonics and the previously developed protocol [2] is proven to work well. However, no extra efforts were placed into rendering every discrete component of the setup more compact [3]. The motivation of the follow-up work to this project, is to prove the working of the previously presented integrated system when implemented in the most practical way possible, to be able to simply plug it in a real-world network. One of the

1. This project is ongoing within the group, lead by Maria Pereira.
2. 3-state BB84 with 1-decoy state protocol [65–67].
3. This was the case only for the components included in the PICs.

challenges is thus to fit all the components in a standard 19" chassis. Therefore, the suggested main changes of the overall integrated setup include lowering of the repetition rate [4] and reduce the footprint of the electronics. On the transmitter side, it is necessary to pulse the laser with a compact laser driving PCB to avoid using an external pulse generator. On the receiver side, the usage of Peltier cooled SPDs would ease the integration of the detectors in a compact chassis and to improve the working distance of the system, a tunable beam splitter for the basis selection in the PIC is necessary. In general, a careful design of the mechanics as well as a robust design of the packaging of the PICs has to therefore be thought of.

The integrated QRNG experiment is still ongoing within the group. The characterisations that have been performed so far have given positive results. There are still a few components that should be characterised and tested in the future before the final generation of random numbers can take place. The future characterisations include mainly the MZIs for attenuation purposes, as well as the fast detectors and the EOPS. However, even though the experiment is not terminated, it can be concluded that integrating all components on a single PIC is highly advantageous in terms of practicality, for research and development, as well as for assembling purposes, if the setup were a product. The self-testing protocol [71–73] displays a close-to-ideal compromise of achievable security, ease of implementation and rate of random number generation. Therefore it is incredibly appealing to be able to render the setup even more attractive for users by minimising its size, power consumption, cost and time of assemble via the use of integrated photonics.

In general, the usage of integrated photonics for QKD systems and QRNGs should not be missed. Several advantages come with these technologies, notably, reduction in cost, ease of mass-production, reproducibility, simpler trouble-shooting [5], reduced footprints, high reliability, and so on. However, the research around such a product might take more time compared to a fibre-based product. This is because it is complicated, if not impossible, to improve certain parameters or the working of certain components of the experimental setup that are integrated without producing a new PIC. Notably, its is hard to do anything about, for example the overall loss [6], the splitting ratios, the length of a delay line or the correct functioning of any component [7]. Thus, the debugging of a PIC can be quite cumbersome and to improve the setup, another run of fabrication has to be planned, which can take half a year. The silver lining is that when the PIC operates as it should, it is rather robust and stable. Additionally, the reproduction of the PIC is reliable. An important aspect to carefully ponder is that of the packaging of the PIC. PICs are in general relatively fragile, especially any component connected to it, like for example a grating coupler or butt-coupled fibres. It is therefore crucial that the PIC is packaged in a robust way, while still keeping its advantage of a reduced footprint. The packaging should also be constructed with a clever isolation or heat sink as most PICs have to be temperature stabilised.

Communication networks are in the need of improved security and privacy of data. In the future, this will possibly be achieved by employing quantum technologies, in particular QKD.

4. To be less affected by the chromatic fibre dispersion and ideally not having to use any DCF. Additionally, the system would also be less affected by the detector timing jitter.

5. Due to less number of discrete components.

6. In a fibre-based scenario the overall loss could be improved by enhancing eventual splices, cleaning fibre connectors, choosing beam splitters with lower loss, and so on.

7. If a component in a fibre-based setup seems to have broken it can either be repaired (by opening it and trying to trouble-shoot) or be replaced.

There are numerous applications that would potentially benefit from QKD, notably, governments and military [8], banking sector [9] or healthcare [10]. It is therefore important to continue the ongoing research at universities and within the industry to slowly and steadily raise the bar of the systems in terms of, for example, performance, ease of integration and lowering of costs. However, it is also important that governments and international organisations (for example the ITU) take the initiative to set proper and clear standards for these technologies. They are crucial in order to achieve a sustainable and reliable integration of quantum technologies in future communications networks. We recommend the work [174] for a recent review of the QKD development.

We hope that the presented works has given rise to an improvement in the status of quantum technologies and that they will be used as a stimulant for future projects. We also wish that the deepened knowledge of (integrated) QKD, and lately, QRNG systems acquired these past four years has been shared among fellow colleagues and researchers in order for the technologies to be pushed even further and understood even better. As Einstein once said: "the point is to understand, any fool can know". The point of understanding is not trivial and so if the comprehension is, if only a bit, improved, then we are satisfied. Finally, quantum technologies are, as we understand them now, incredibly powerful. We therefore request their usage in the most responsible way. This means, for example, that governments and policy makers take the responsibility to actively follow the ongoing research on quantum technologies to be prepared for when (if this day arrives) such technologies are widespread. Most importantly, they should also share the knowledge amongst them, to avoid a nation or company to have a monopoly on a certain technology, which might cause incredible damage. After all, it is of fundamental human right for each and every one "to enjoy the benefits of scientific progress and its applications" [11].

8. In terms of defense secrets, intellectual property or data of citizens.
9. For example regarding transactions or customer data in data centres.
10. For example personal health data that is stored (long-term) and transferred between hospitals.
11. Article 15 of the International Convenant on Economic, Social and Cultural Rights [175].

A. Integrated transmitter characterisations

A.1. Silicon PIC

Different values of current flowing through AA1 and the corresponding visibility is shown in table A.1.

AA1 current [mA]	$\mathbf{V}_{min}$ **[%]**
3.0	99.0
4.2	98.4
6.0	96.7

Table A.1.: AA1 current and the minimum visibility.

B. Integrated receiver characterisations

B.1. Silica on silicon PIC

Measurements of the minimum visibility for the different PICs (which are enumerated from 1 to 7) of the three systems is shown in table B.1. The maximum visibility, obtained with the most favorable input polarisation, is found to be around 99.8% for all PICs.

System #	**Chip #**	$\mathbf{V_{min}}$ **[%]**
1	5	83.1
1	6	42.5
1	3	66.3
2	4	94.5
2	7	51.9
3	1	31.1
3	2	26.3

Table B.1.: Minimum visibilities of different PICs of systems 1-3.

Given the results in table B.1 one can conclude that the visibility of the imb-MZI is rather dependent on the polarisation and that the arms of the imb-MZI induce different birefringences, leading to a worsened interference. Given the diverse results between the different systems, it is difficult to give a conclusive reason for this birefringence. It would be tempting to say that the system 3 performs the least well and system 2 the best. However, discrepancies and a small number of tested PICs forces inconclusiveness. An educated guess to why this is observed could be due to fabrication inaccuracies and differences in placement of the chips on the wafer.

B.2. Silica PIC

Temperature [kΩ]	$\mathbf{V_{min}}$ **[%]**
8.0	90.0
9.0	95.3
10.0	98.9
11.0	96.3
12.0	88.9

Table B.2.: Extract of results of minimum visibility at different temperatures.

C. Full results of secret key exchanges of integrated QKD setup

C.1. Utilising SNSPDs

Length [km]	Attenuation [dB]	RKR [kbps]	q_z [%]	ϕ_z [%]	SKR [kbps]
-	30	216	0.9	1.0	91.0*
-	36	66	0.8	1.1	28.3
-	38	42	0.8	1.4	17.2
-	40	27	0.8	2.1	10.6
202.0	39.5	25	0.9	2.2	9.4
[86]: 251.7	42.7	12	0.5	2.2	4.9

Table C.1.: Parameters and results of secret key exchanges when using SNSPDs. * signifies estimated SKR from raw data. For comparison, the last line presents data from reference [86] which used a fiber-based setup with SNSPDs.

C.2. Utilising SPADs

Length [km]	Attenuation [dB]	Dead time [μs]	Temperature [K]	Block time [s]	RKR [kbps]	QBER$_z$ [%]	ϕ_z [%]	SKR [kbps]
-	30	20	188	453	18.0	3.6	2.1	2.9
-	35	32	183	858	9.6	3.1	4.5	1.3
-	40	20	188	1590	4.0	4.4	6.0	0.2
151.5	29.7	40	188	716	11.0	3.3	2.7	1.3
[67]: 151.6	30.2	19	183	360	22.8	3.2	2.1	7.2

Table C.2.: Parameters and results of secret key exchanges when using InGaAs detectors. For comparison, the last line presents data of the fiber-based setup using also InGaAs detectors [67].

D. Integrated QRNG

D.1. Slow QRNG PIC

The schematics of the optics of the slow PIC is presented in figure D.1.

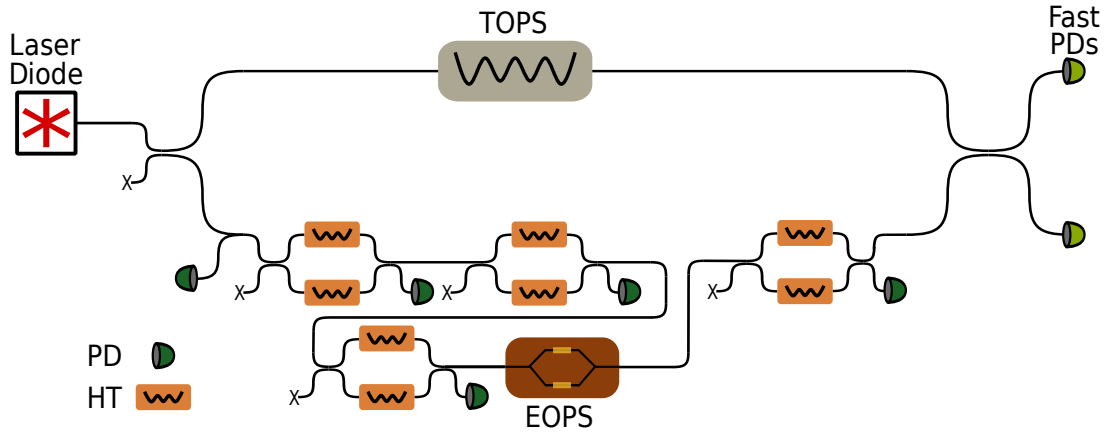


Figure D.1.: Schematics of the slow QRNG PIC. TOPS = thermo-optic phase shifter, EOPS = electro-optic phase shifter, PD = photoiode, HT = heater.

D.2. TIA characterisation

The graph of noise power as a function of frequency of the TIA-circuit with the Koheron detectors is shown in figure D.2.

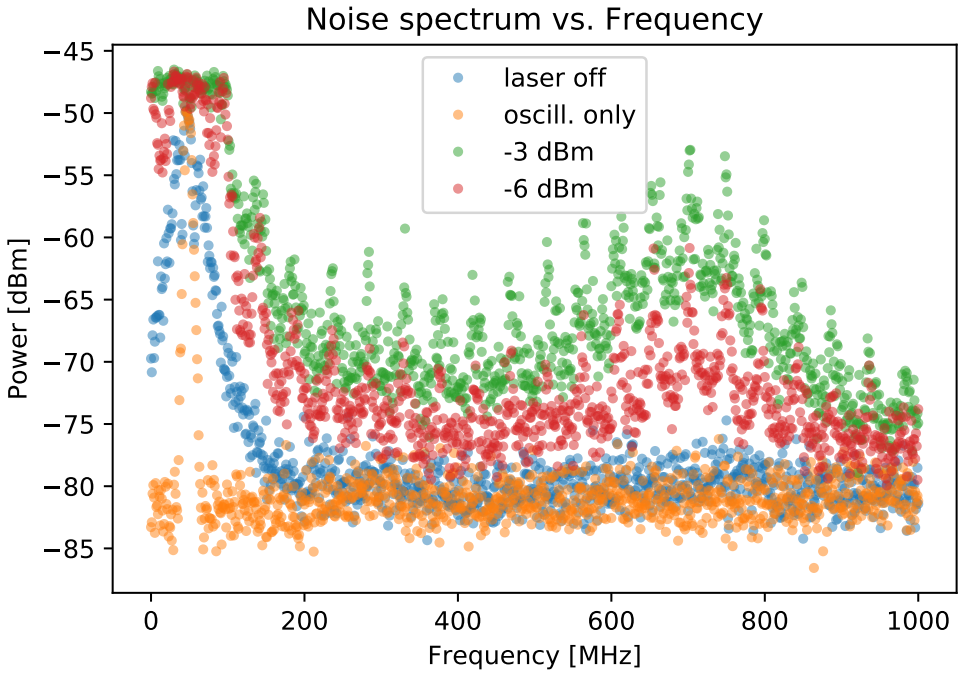


Figure D.2.: Noise power vs. frequency for different input powers.

E. Peer-Reviewed Articles

E.1. High-speed integrated QKD system

Research Article Vol. 11, No. 6 / June 2023 / Photonics Research 1007

High-speed integrated QKD system

Rebecka Sax,[1,*] Alberto Boaron,[1] Gianluca Boso,[1,2] Simone Atzeni,[3,4] Andrea Crespi,[3,4] Fadri Grünenfelder,[1] Davide Rusca,[1] Aws Al-Saadi,[5] Danilo Bronzi,[5] Sebastian Kupijai,[5] Hanjo Rhee,[5] Roberto Osellame,[3,4] and Hugo Zbinden[1]

[1]Group of Applied Physics, University of Geneva, 1205 Genève, Switzerland
[2]ID Quantique SA, 1227 Genève, Switzerland
[3]Institute for Photonics and Nanotechnologies and NO-IFN, CNR-IFN, 20133 Milano, Italy
[4]Dipartimento di Fisica, Politecnico di Milano, 20133 Milano, Italy
[5]Sicoya GmbH, 12489 Berlin, Germany
*Corresponding author: rebecka.sax@unige.ch

Received 18 November 2022; accepted 6 April 2023; posted 7 April 2023 (Doc. ID 481475); published 25 May 2023

Quantum key distribution (QKD) is nowadays a well-established method for generating secret keys at a distance in an information-theoretically secure way, as the secrecy of QKD relies on the laws of quantum physics and not on computational complexity. In order to industrialize QKD, low-cost, mass-manufactured, and practical QKD setups are required. Hence, photonic and electronic integration of the sender's and receiver's respective components is currently in the spotlight. Here we present a high-speed (2.5 GHz) integrated QKD setup featuring a transmitter chip in silicon photonics allowing for high-speed modulation and accurate state preparation, as well as a polarization-independent low-loss receiver chip in aluminum borosilicate glass fabricated by the femtosecond laser micromachining technique. Our system achieves raw bit error rates, quantum bit error rates, and secret key rates equivalent to a much more complex state-of-the-art setup based on discrete components [A. Boaron *et al.*, Phys. Rev. Lett. 121, 190502 (2018)].

https://doi.org/10.1364/PRJ.481475

1. INTRODUCTION

The security of the exchange of an encrypted message is an extremely relevant issue in today's society, as disastrous consequences can arise when it is compromised. One rising threat is the quantum computer, which would be able to efficiently crack the current most-used encrypting techniques [1] and whose technology matures as the authors are writing this article [2,3]. Hence, the natural entry of quantum key distribution (QKD), which establishes an information-theoretically secure key exchange and provides long-term security.

Since the first proposal of a QKD protocol in 1984 [4] and its first experimental realization in 1992 [5], more protocols and a multitude of experiments have been established. This global enthusiasm has resulted in enormous increase in the communication distance (using fiber [6–8], as well as free space [9]) and in the secret key rate (SKR) [10,11].

In order to industrialize QKD and to merge it with existing networks, a vision of integrated transmitters and receivers separated at metropolitan distances seems rather judicious. The miniaturization of such systems is notably important, with advantages in terms of low cost, mass production, scalability, simple stabilization in temperature, and compatibility with CMOS-production.

The first realization of a fully integrated QKD system (both the transmitter and receiver integrated) consisted of a silicon transmitter and a SiO_xN_y receiver operating at 1.72 GHz clock rate, using the COW protocol at 20 km distance separation [12]. Subsequently, several integrated implementations have been reported for various QKD schemes [13–22]. Some included an integrated laser [13–15], and others presented hybrid versions that maintain one of the components as non-integrated (either the transmitter or the receiver device, or one of their sub-components) [14–17]. Integrated detectors on-chip have also been realized [23].

Here we present a 2.5 GHz integrated QKD system, the fastest integrated system to our knowledge [24], which features a precise state preparation and a polarization-independent receiver. At a distance of 151.5 km of standard single-mode fiber (SMF), we obtain an SKR of 1.3 kb/s using InGaAs/InP negative feedback avalanche photodiodes. We further demonstrate extremely low quantum bit error rates (QBERs) ($QBER_z$ of 0.9% and ϕ_z of 2.2%) using superconducting nanowire single-photon detectors (SNSPDs) at a distance of 202.0 km, thereupon raising the bar of the state-of-the-art integrated QKD and further laying the groundwork for its use.

2. QKD PROTOCOL

We apply a three-state BB84 protocol using the one-decoy state method [25,26] with time-bin encoding. The three states, and their respective decoys, prepared by Alice are shown in Fig. 1. They belong to one of the two bases, Z and X, and they are chosen at random. The two states in the Z basis are

$$|0\rangle = |\alpha\rangle_E|0\rangle_L, \tag{1}$$

$$|1\rangle = |0\rangle_E|\alpha\rangle_L. \tag{2}$$

The subscript E stands for early, L for late, and $|\alpha\rangle$ for a weak coherent state. The state in the X basis is

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \tag{3}$$

Qubits detected in the Z basis will undergo a time-of-arrival measurement and constitute the raw key. In order to preserve security, a second basis, the X basis, is used to check for any eavesdropping attempts. Qubits detected in the X basis will pass through an imbalanced Mach–Zehnder interferometer (imb-MZI). In an intuitive way, if an eavesdropper attempts to make a measurement on one of the states in the Z basis (in order to gain information about the key), the coherence of the state $|+\rangle$ will be altered, which will generate errors in the X basis [27].

3. EXPERIMENTAL SETUP

An overview of the full QKD setup is depicted in Fig. 2. Alice, the transmitter, and Bob, the receiver, are connected via a quantum channel (QC) and a service channel (SC). The former serves for guiding the quantum encoded states and the latter for classical (public, but authenticated) communication between the parties. Each of the two apparatuses is controlled by a field-programmable gate array (FPGA), which also allows for synchronization and communication of the two parties, via the SC.

Regarding the optical elements, the transmitter encompasses a distributed feedback (DFB) laser with a filter, a photonic integrated circuit (PIC), and a dispersion compensating fiber (DCF). Phase-randomized pulses of light at a repetition rate of 2.5 GHz and a full width at half maximum of around 31 ps are generated by a gain-switched high-bandwidth DFB laser at

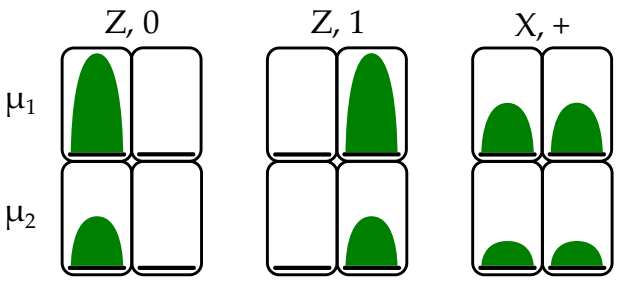


Fig. 1. Encoding of the states sent by Alice. Z and X are the bases in which the states $|0\rangle$, $|1\rangle$ and, $|+\rangle$, respectively, live. μ_1 and μ_2 correspond to the two mean photon numbers used for the one-decoy state protocol [26].

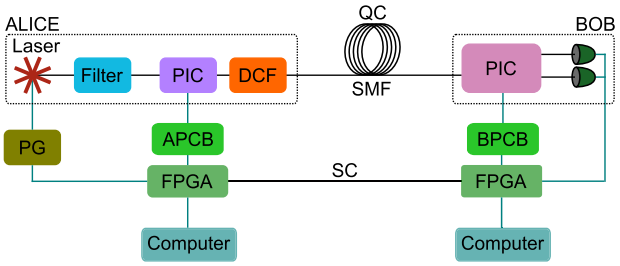


Fig. 2. Simplified schematic of the experimental setup. PIC, photonic integrated circuit; DCF, dispersion compensating fiber; QC, quantum channel; SMF, single-mode fiber; PG, pulse generator; APCB, Alice printed circuit board (PCB); BPCB, Bob PCB; FPGA, field-programmable gate array; SC, service channel. Black lines correspond to optical links, and blue lines correspond to electrical connections.

1550 nm (Gooch and Housego). The pulse train enters the integrated transmitter chip where the three states and their decoys are produced at random using the following components: imb-MZI, intensity modulator (IM), and variable optical attenuators (VOAs). The probability to select the basis Z (p_z) and X (p_x) is 0.67 and 0.33, respectively. The random numbers used to choose the states are produced by Advanced Encryption Standard (AES) cores seeded by a quantum random number generator (QRNG), Quantis from ID Quantique SA. Upon exiting the chip, light pulses travel through the DCF, which consists of specially fabricated fiber with a large negative dispersion coefficient. It will, hence, pre-compensate all the chromatic dispersion created on the trip from Alice to Bob in the QC. For example, 7 km of DCF compensates the chromatic dispersion from 50 km of SMF. The QC consists of SMF with around 0.2 dB/km losses.

On the receiver side, the integrated part consists of a passive beam splitter and an imb-MZI. The effective splitting ratio for the Z and X bases, i.e., taking into account different losses in respective optical paths, is 94/6. The imbalance of the interferometer of Bob should be ideally the same as that of Alice, i.e., 200 ps. However, due to fabrication uncertainties, a delay difference of around 1.6 ps between the two interferometers is measured using optical low-coherence interferometry. The main effect of a delay difference is on the QBER in the X basis, QBER_x, as it leads to a reduced interference of the pulses in the imb-MZI. The relative phase of their interferometers is actively adjusted by acting on the phase of Alice's interferometer in such a way that the two pulses interfere destructively in the output we monitor in the X basis. A feedback loop is locked to minimize the number of detections in this output. It should be noted that, since the occurrences are already low, the active adjustment will be more difficult with increased channel loss due to the, at that point, even lower statistics. The second output of the imb-MZI on the receiver side is not monitored.

The (off-chip) single-photon detectors (SPDs) adopted for our main experiment are InGaAs/InP negative feedback single-photon avalanche diodes (SPADs) cooled by a free-piston Stirling cooler to around −85°C [28]. The timing jitter of the SPADs is below 100 ps, the dark count rates are below 120 counts per second, and the detector efficiency is around

20%. For the characterization of our system, we also use in-house-made superconducting-nanowire single-photon detectors (SNSPDs) cooled at 0.8 K [29]. These detectors feature low timing jitter (around 40 ps), negligible after-pulsing probability, high detector efficiency (around 80 %), and low dark count rates ($d_z = 200$ Hz, $d_x = 100$ Hz). The SPADs are used for the experiment as these detectors are more mature than SNSPDs for practical real-world applications. It should be noted that the fixed 94/6 splitting ratio of the integrated beam splitter on Bob's chip is suited for intermediate distances in this proof-of-principle experiment. Indeed, for short distances, the large number of photons in the Z basis would rapidly saturate the SPADs, whereas for long distances too few detections in the X basis would give rise to non-negligible dark count contribution. However, versatility of the system could be easily increased by replacing the passive beam splitter at the receiver side with a tunable Mach–Zehnder interferometer.

4. INTEGRATED TRANSMITTER

Several challenges arise in the realization of integrated systems for QKD purposes depending on the protocol one uses. For our considerations, due to our high clock rate, we need accurate modulation of the quantum states at high frequencies on the transmitter side. Indeed, accuracy is reflected on the extinction ratio (ER) of the quantum states and consequently on the QBER. Moreover, for time-bin encoding, the platform must allow for the implementation of an MZI with high imbalance.

We developed an integrated chipset based on silicon photonics, with the formerly mentioned qualities for the transmitter, in collaboration with Sicoya GmbH. It consists of a PIC, which is as small as 4.50 mm × 1.10 mm and an adjacent electronic driver integrated circuit (EIC) 4.50 mm × 0.75 mm (see Fig. 3). It is highly advantageous to use silicon photonics for our system as now most of the expensive electronics are on-chip, hence allowing for high component density and small footprints. As can be seen in Fig. 3, the integrated circuits (ICs) are glued on and bonded to a small printed circuit board (PCB). This PCB is combined with a larger one (APCB in Fig. 2), which provides the all electronic signals necessary to control the different components of the chip. It is further connected to a computer-controlled FPGA, as shown in Fig. 2. Light is coupled to the PIC via a fiber array and a grating coupler. The chip is temperature stabilized at 45°C using a standard Peltier cooler/heater placed under the host PCB of the PIC.

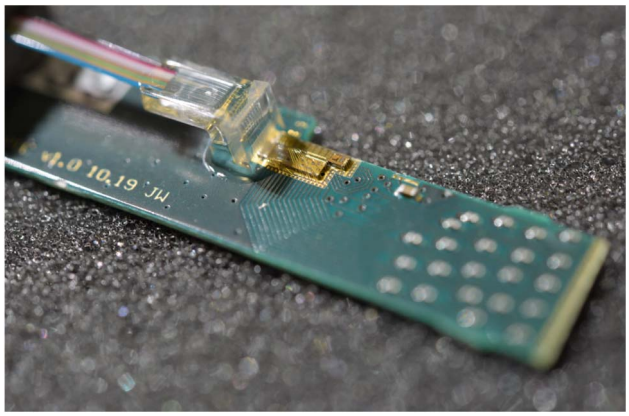


Fig. 3. Photo of the transmitter integrated circuit.

The chips were fabricated in the 0.13 μm SG25PIC SiGe bipolar-complementary metal–oxide semiconductor (BiCMOS) process at the Leibniz Institute for High Performance Microelectronics (IHP) in Frankfurt (Oder), Germany, using 200 mm silicon-on-insulator (SOI) wafers and 248 nm deep ultraviolet (DUV) lithography [30]. The nanowires are embedded within the 220 nm thick silicon device layer of the SOI substrate. The SOI rib waveguides have dimensions of 220 nm × 450 nm and are fabricated in a shallow trench process. The etching depth of the photonic structures is 170 nm, with a 50 nm high remaining slab on top of the underlying SiO_2 BOX layer with a thickness of 2 μm. The implant doping level inside the p^+- and n^+-doped regions of the electro-optic phase shifters (EOPS) is 1×10^{20} cm^{-3}. The process provides a CMOS back-end-of-line with a stack of five metal layers. For fabrication of the driver chips, the SG25H4 SiGe BiCMOS technology also from IHP was used.

Figure 4 reports a functional scheme of the transmitter device. It should be noted that the input and output are on the same side, as according to the image in Fig. 3, but drawn here on separate sides for clarity. Light entering the PIC passes first through an imb-MZI. The phase of the interferometer can be controlled via thermo-optic phase shifters (TOPSs or heaters), one in each arm, one of which is adjusted for the active phase stabilization between Alice and Bob. The shorter arm also comprises an attenuator (based on carrier absorption) to compensate for propagation loss in the longer arm. It should be highlighted that the fabrication of such a long delay line is not trivial given the size of the chip and its two-dimensional restriction, hence the specific geometry of the delay line. Light then enters an IM based on a balanced Mach–Zehnder-modulator (MZM). In the arms of the IM, there are three EOPSs based on carrier injection, which allow for a much higher electro-optic effect compared to a depletion type phase shifter, leading also to a more compact design. The bandwidth limitation is overcome by equalization schemes in the electronic driver design. Each EOPS has been fabricated with a specific size and is designed for a given amplitude of modulation. Three of them are used in order to produce our three amplitude levels independently. In addition, each EOPS is connected to the analog driver circuit on the EIC via wire-bondings. This allows us to individually actuate each EOPS and produce the full combination of quantum states. Likewise to the imb-MZI, the two arms of the IM include heaters, used to adjust its working point.

The electronic driver chip consists of several drivers digitally controlled by serial peripheral interface (SPI) with an input limiting amplifier for a high-speed and high-voltage swing application implemented in 250 nm BiCMOS technology. The amplification stage uses a cascode configuration to explore high bandwidth and output voltage swing. Differential input for limiting operation needs 50 mV, and the driver has a differential output swing of up to $3V_{pp}$ with a power consumption of 400 mW. The single driver consists of three active stages: a limiting amplifier, a buffer stage, and a current-mode logic (CML) output, plus a passive input matching network

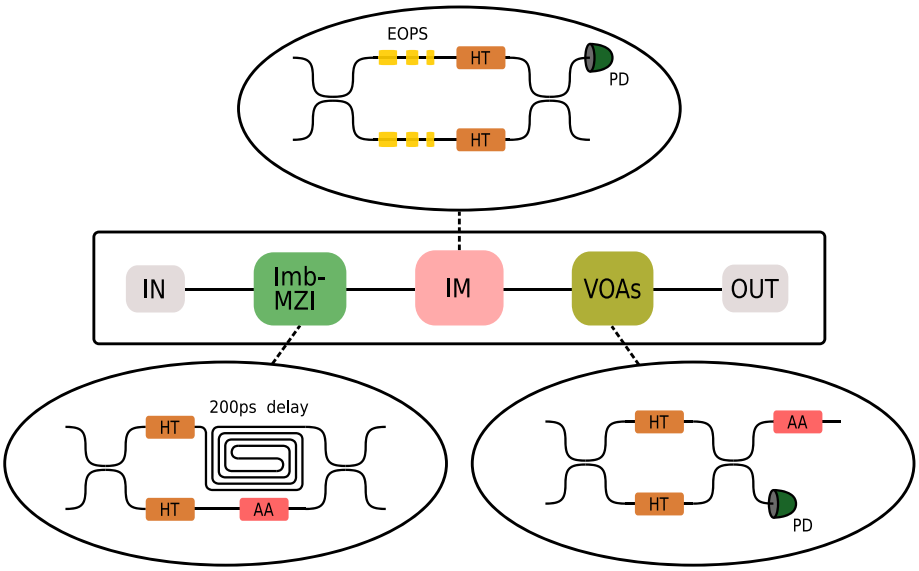


Fig. 4. Structure of the integrated transmitter circuit. Imb-MZI, imbalanced Mach–Zehnder interferometer; IM, intensity modulator; VOAs, variable optical attenuators; HT, heater; AA, absorption attenuator; EOPS, electro-optic phase shifter; PD, photodiode. The lengths of the three EOPSs are 200 μm, 400 μm, and 600 μm.

consisting of two common-base transistors. The limiting amplifier stabilizes the in-chip signal at $0.4V_{\mathrm{pp}}$ differential, which is a compromise between the gain required at the output and the bandwidth and dissipation of the limiting amplifier itself. The buffer stage (emitter follower) partially improves the signal and brings the signal to lower DC voltages, thus allowing for higher voltage swing at the output. Finally, the output stage consists of a cascoded common-emitter amplifier with a controllable capacitive and resistive source degeneration: at low frequency, the capacitor acts as an open circuit, and the presence of the resistor causes a voltage drop that diminishes the output gain. At high frequency, the capacitor acts as a short circuit, thus restoring the full gain of the amplifier. The core of the single-channel driver is very small (order of hundred of microns) and the entire layout of the cell circuitry was kept strictly, thermally and electrically, symmetric with respect to the radio-frequency (RF) inputs and outputs. With such a configuration, the current design offers a wide range of gain and frequency compensation equivalent to two-tap digital pre-emphasis output that enables a full equalization of the low bandwidth of the phase shifters [31]. The drivers have fully differential inputs and outputs and are connected to the modulators to realize a push–pull configuration.

Before exiting the integrated chip, the light pulses are attenuated through two VOAs: one consists of a balanced-MZI with heaters in both arms in order to tune the MZI transfer function closer to a point of minimal transmission, while the other one is based on carrier absorption (the same as in the imb-MZI). Monitoring photodiodes have been placed at the outputs of the IM and the VOA-MZI. The total loss of the chip is around 25 dB. For testing purposes, it is possible to use an alternative optical input path, which is directly connected to the IM, bypassing the imb-MZI. This input has around 20 dB loss. Note that, as opposed to the receiver, loss is not an issue for the transmitter.

5. INTEGRATED RECEIVER

On the receiver side, the integrated chip is completely passive. According to our protocol, we require its polarization independence, meaning that the visibility of the integrated receiver interferometer should be high (100% ideally) for any incoming polarization state. We characterize the polarization independence by measuring the maximum and minimum visibilities depending on the incoming polarization state. Additionally, the first beam splitter should also be independent of the polarization. The former requirement is difficult to achieve in PICs due to the intrinsic birefringence of the waveguides [32–34], which is hard to control in an imb-MZI. To our knowledge, only recently, a polarization-independent receiver chip of a QKD system has been demonstrated [35,36]. However, the receiver in Ref. [35] showed a low maximum visibility (<98%) and high insertion losses (excess loss up to 6 dB) and the receiver in Ref. [36] showed a maximum visibility of 98.7%. In addition, a hybrid receiver based on a Michelson imbalanced interferometer and Faraday mirrors glued to the exterior of the chip has been recently validated [37].

In the present experiment, we make use of a polarization-independent PIC produced by the femtosecond laser micromachining technique [38]. Waveguides with low propagation loss (<0.2 dB/cm) and low birefringence ($<3\times10^{-5}$, due to residual stress in the material induced by the laser writing process) were inscribed in an aluminum borosilicate glass (EAGLE XG, Corning Inc.). Polarization independency of the directional couplers was achieved by exploiting the multiscan inscription technique, followed by a thermal annealing process, as described in Ref. [39]. Furthermore, at room temperature, a careful control of the waveguides' birefringence, by fabricating compensation tracks around the waveguide of the longer arm of the imb-MZI [39,40], as well as by finely tuning the temperature of the chip, allowed for the same polarization

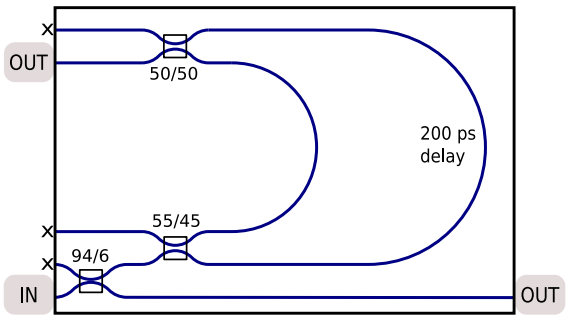


Fig. 5. Structure of the receiver integrated circuit. X means non-fiber-coupled ports. Fibers are butt-coupled to the waveguides and permanently pigtailed with UV-curing, index-matching glue. Fiber to waveguide coupling losses are better than 0.3 dB/facet.

rotation in both arms. We achieve temperature stabilization using, as on the transmitter side, a Peltier cooler/heater. At ambient temperature (around 20°C) as good as perfect birefringence compensation occurs, giving rise to a minimum visibility as high as 98.9%. It is important to note that this is the visibility corresponding to the case of the most unfavorable input polarization state; hence, the average visibility is higher. To compare our results with the values provided above in other implementations, our maximum visibility is 99.7%. The additional loss in the longer arm is compensated by adjusting the coupling ratio of the first coupler of the imb-MZI (around 55/45). The relationship of the visibility and QBER_x is given by $\mathrm{QBER}_x = (1 - V)/2$, and so, at the optimum temperature, its contribution to the QBER_x is minor.

Figure 5 shows a scheme of the receiver device. When entering the PIC, the light passes first through a 94/6 beam splitter. The majority of the light passes straight through the chip and out to an SPD. The lesser amount of light goes to the imb-MZI where another SPD at one of the outputs of the interferometer detects the exiting light. The footprint of Bob is around 6 cm × 8 cm. The total loss of the chip is notably low, something that is much desired on the receiver side. In fact, we measure the excess loss for the Z and X bases, using a low-coherence light source, to be around 2.75 dB and 3.50 dB, respectively. This is excluding the splitting ratios of the first and last beam splitters but including input/output coupling.

6. RESULTS

We performed complete secret key exchanges for different emulated distances and also employed standard SMF, using first the SNSPDs and then the InGaAs SPADs. We applied real-time error correction using a cascade algorithm with a block size of 8192 bits [41]. After 1000 error correction blocks, privacy amplification was executed. Thus, the total privacy amplification block size is 8.192×10^6 bits. In order to calculate the obtained SKR, we followed the security analysis of the one-decoy state protocol [26], where the SKR per privacy amplification block is given by

$$\mathrm{SKR} = \frac{1}{t}\{s_0 + s_1[1 - h(\phi_z)] - \lambda - 6\log_2(19/\epsilon_{\mathrm{sec}}) - \log_2(2/\epsilon_{\mathrm{corr}})\},$$

where t is the block acquisition time, s_0 is the lower bound on the number of vacuum events in the Z basis, s_1 is that of the single-photon events, $h(\cdot)$ is the binary entropy, ϕ_z is the upper bound on the phase error rate, λ is the leakage of the bits during the error correction process, and $\epsilon_{\mathrm{sec}} = 10^{-9}$ and $\epsilon_{\mathrm{corr}} = 10^{-9}$ are the secrecy and correctness parameters, respectively.

The first set of measurements was done with the main aim to understand the maximum performance of the integrated QKD system; hence, we employed the SNSPDs (see Section 3). In Table 1, we present the results obtained using different emulated fiber distances and using a 202.0 km long SMF. The emulated fiber distances were realized using an external VOA.

At 30 dB attenuation, the number of raw detections was too large for the real-time cascade error correction to be performed (this problem could be overcome by implementing a low-density parity check error correction on the FPGA [11]). Extremely low QBER_z values for all measurements with the SNSPDs were recorded. The main contribution to the QBER_z is estimated to come from the timing jitter of the SNSPD (see Section 3). A small contribution to the QBER_z could also come from the ER of the IM. In a static mode, it is above 40 dB, and it is estimated to be slightly lower in an active mode. Regarding the phase error rate, ϕ_z, it will depend on the visibilities of the interferometers at Alice's and Bob's sides and the active phase stabilization between them. Thanks to the high visibilities, ϕ_z is noticeably low. This is the case especially for the 30 dB attenuation due to the large number of counts, giving rise to a high raw key rate (RKR) and, therefore, a significant SKR. At higher attenuations, ϕ_z increases due to the smaller number of counts in the X basis detector, making it harder to stabilize the phase (for further discussion, see Section 3). For the measurement using 202.0 km of standard SMF placed in between the transmitter and the receiver, active time-tracking was performed in order to compensate for length fluctuations in the fiber.

Table 1. Parameters and Results of Secret Key Exchanges When Using SNSPDs[a]

Length [km]	Attenuation [dB]	Block Time [s]	RKR [kb/s]	QBER_z [%]	ϕ_z [%]	SKR [kb/s]
-	30	37	216	0.9	1.0	91.0*
-	36	124	66	0.8	1.1	28.3
-	38	168	42	0.8	1.4	17.2
-	40	306	27	0.8	2.1	10.6
202.0	39.5	351	25	0.9	2.2	9.4
251.7	42.7	720	12	0.5	2.2	4.9

[a]The asterisk * signifies estimated SKR from raw data. For comparison, the last line presents data from Ref. [1], which used a fiber-based setup with SNSPDs.

Table 2. Parameters and Results of Secret Key Exchanges When Using InGaAs Detectors[a]

Length [km]	Attenuation [dB]	Dead Time [μs]	Temperature [K]	Block Time [s]	RKR [kb/s]	$QBER_z$ [%]	ϕ_z [%]	SKR [kb/s]
-	30	20	188	453	18.0	3.6	2.1	2.9
-	35	32	183	858	9.6	3.1	4.5	1.3
-	40	20	188	1590	4.0	4.4	6.0	0.2
151.5	29.7	40	188	716	11.0	3.3	2.7	1.3
151.6	30.2	19	183	360	22.8	3.2	2.1	7.2

[a]For comparison, the last line presents data of the fiber-based setup using also InGaAs detectors [25].

It is interesting to note how the integrated version of the three-state BB84 protocol compares with a similar fiber-based setup employing SNSPDs, described in Ref. [1]. Its performance with 251.7 km of ultra low-loss SMF is shown in the last line of Table 1. It can be concluded that, with similar mean photon numbers, the same block size, and around 3 dB less attenuation than the measurement performed in the fiber-based setup, the integrated setup is practically as good as its fiber-based counterpart in terms of performance. However, in terms of practicality and cost, the integrated setup is more attractive.

In the following, we present measurements using the practical SPADs. On one hand, these detectors are considered more qualified than the SNSPDs for industrial implementations as they are uncomplicated to cool down. On the other hand, they present higher dark count rates, after-pulsing probabilities, and timing jitters, as well as lower efficiencies. The results obtained using the InGaAs SPADs are shown in Table 2.

Similar conclusions as for the results of Table 1 can be drawn. Compared to the results with the SNSPDs, a lower RKR is observed, which is reasonable as the detector efficiency is around 20% (a fourth of the efficiency of the SNSPDs). The increased values of $QBER_z$ are due to the higher timing jitters and after-pulsing probabilities of the InGaAs SPADs. The non-optimal 94/6 splitting ratio generates a faster saturation of the detector in the Z basis, hence a high $QBER_z$ at 30 dB attenuation, as well as non-negligible dark count rates for higher attenuations in the X basis. 151.5 km standard SMF was also placed in between the transmitter and the receiver. Due to the lower number of counts and, therefore, increased difficulty to perform perfect time-tracking and active phase tracking (see Section 3), ϕ_z is slightly higher than its attenuated analogue. The $QBER_z$ and ϕ_z at 40 dB attenuation are higher than at lower attenuations due to a smaller amount of counts, and so there is a worse signal-to-noise ratio.

Again we compare these results with those obtained using the same detectors and protocol in a fiber-based setup, more precisely, the one in Ref. [25]. At a distance of 151.6 km, with half of the mean photon numbers and the same block size, the fiber-based setup seems to perform better in terms of RKR and SKR than the integrated one with these detectors; however, this difference can be attributed mainly to the fact that the detectors were operated with different parameters. In fact, the fixed, yet non-optimal, splitting ratio at the receiver side of the integrated QKD setup forced a lower bias voltage and higher dead time in the X basis to minimize the dark counts (while lowering the detector efficiency) and maximize the number of counts, respectively. However, the comparable values of $QBER_z$ and ϕ_z

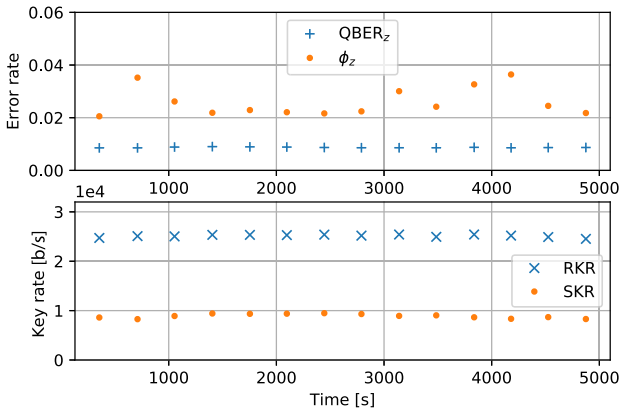


Fig. 6. $QBER_z$, ϕ_z, RKR, and SKR during several secret key exchanges over 80 min using SNSPDs at a distance of 202.0 km SMF.

make the employment of the integrated devices still attractive. In particular, the replacement of the first beam splitter with a tunable MZI, a device already well-optimized on the same platform [42], will allow for an optimal splitting ratio at the receiver side with a negligible cost in terms of loss and device complexity.

Lastly, we present the complete results of the integrated QKD setup with 202.0 km of standard SMF and SNSPDs as detectors with a secret key exchange run for around 80 min. In Fig. 6, the RKR, SKR, $QBER_z$, and ϕ_z are shown as a function of time. We observe stable RKR and SKR, around 25 kb/s and 9 kb/s, respectively. The same goes for the $QBER_z$, around 0.9 %, thanks to the large number of detections in the Z basis, and so there is excellent time-tracking. Concerning ϕ_z, as previously mentioned, more fluctuations are observed due to a lower detection rate in the X basis, and so there is a more complicated time-tracking and active phase adjustment (refer to Section 3).

7. CONCLUSION

An integrated QKD system has been presented and shown to perform as well as its fiber-based analogue and, most importantly, as the state-of-the-art of integrated QKD systems [24]. Its transmitter is practical and with low cost thanks to the integration of the imb-MZI and, especially, the IM and corresponding electronics. Additionally, its receiver features low loss and is polarization-independent, which is typically complicated to achieve in integrated platforms.

Even though polarization fluctuations of QKD systems are nowadays very well controlled and compensated in laboratory

conditions [43,44], it might still be demanding to compensate for particularly rapid fluctuations in polarization that could occur in real-world fiber-optic lines, e.g., because of trains passing or lightning strikes [45]. Thus, the integrated QKD system here suggested, based on time-bin encoding and polarization insensitivity, testifies for effortless integration in present-day fiber-optic networks.

We believe that the integrated high-speed QKD system gives an important contribution to the advancement of integrated quantum technologies and simultaneously reflects their maturity. Future investigations could cover how to integrate all components on-chip (meaning the laser on the transmitter side and the SPDs on the receiver side), which has the risk of being costly due to the active materials required, such as InP, and further complicated due to the need of interfacing different active and non-active materials via gluing or bonding. Several works have already examined the merge of InP platforms with silicon platforms [46,47]. On the transmitter side of the present integrated platform, the PIC, the driver EIC, and all DC control loops could be monolithically integrated in a single electronic and photonic IC (EPIC) chip. The EPIC technology [48] for this approach is mature and already in use for data center applications. An adaptation to QKD applications is only a matter of chip design rather than process development. Furthermore, EPIC and even PIC/EIC solutions can be scaled to significantly higher modulation rates, however limited by the achievable ER. Thanks to the small dimensions of the introduced integrated platforms, it is rather straightforward to integrate the current QKD system in two rack-mountable enclosures, ready for usage in a real-work network.

Funding. Eurostars Projects (E!11493); European Quantum Flagship project openQKD (857156); Italian Ministry for University and Research (PRIN2017-SRNBRK, PNRR-NQSTI); European Research Council (742745).

Acknowledgment. We thank Claudio Barreiro for providing the electronic cards and Federico Bassi for his preliminary work on the fabrication and characterization of the receiver. We thank the Eurostars project E!11493 QuPIC for financial support. SA and AC acknowledge funding by the PRIN2017 program, QUSHIP project. RO acknowledges funding by the European Union through the ERC Advanced Grant CAPABLE, and the Italian Ministry for University and Research through the PNRR project PE0000023-NQSTI.

Disclosures. The authors declare no conflicts of interest.

Data Availability. Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

REFERENCES

1. P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM J. Comput. **26**, 1484–1509 (1997).
2. M. Amico, Z. H. Saleem, and M. Kumph, "Experimental study of Shor's factoring algorithm using the IBM Q experience," Phys. Rev. A **100**, 012305 (2019).
3. K. Wright, K. M. Beck, S. Debnath, J. M. Amini, Y. Nam, N. Grzesiak, J.-S. Chen, N. C. Pisenti, M. Chmielewski, C. Collins, K. M. Hudek, J. Mizrahi, J. D. Wong-Campos, S. Allen, J. Apisdorf, P. Solomon, M. Williams, A. M. Ducore, A. Blinov, S. M. Kreikemeier, V. Chaplin, M. Keesan, C. Monroe, and J. Kim, "Benchmarking an 11-qubit quantum computer," Nat. Commun. **10**, 5464 (2019).
4. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *International Conference on Computers, Systems & Signal Processing* (1984), pp. 175–179.
5. C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," J. Cryptol. **5**, 3–28 (1992).
6. A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Secure quantum key distribution over 421 km of optical fiber," Phys. Rev. Lett. **121**, 190502 (2018).
7. M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," Nature **557**, 400–403 (2018).
8. S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, W. Chen, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, "Twin-field quantum key distribution over 830-km fibre," Nature **16**, 154–161 (2022).
9. S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-ground quantum key distribution," Nature **549**, 43–47 (2017).
10. Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. W. Sharpe, A. R. Dixon, E. Lavelle, J. F. Dynes, A. Murakami, M. Kujiraoka, M. Lucamarini, Y. Tanizawa, H. Sato, and A. J. Shields, "10-Mb/s quantum key distribution," J. Lightwave Technol. **36**, 3427–3433 (2018).
11. F. Grünenfelder, A. Boaron, M. Perrenoud, G. V. Resta, D. Rusca, C. Barreiro, R. Houlmann, R. Sax, L. Stasi, S. El-Khoury, E. Hänggi, N. Bosshard, F. Bussières, and H. Zbinden, "Fast single photon detectors and real-time key distillation: enabling high secret key rate QKD systems," arXiv, arXiv:2210.16126 (2022).
12. P. Sibson, J. E. Kennard, S. Stanisic, C. Erven, J. L. O'Brien, and M. G. Thompson, "Integrated silicon photonics for high-speed quantum key distribution," Optica **4**, 172–177 (2017).
13. P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. L. O'Brien, and M. G. Thompson, "Chip-based quantum key distribution," Nat. Commun. **8**, 13984 (2017).
14. T. K. Paraïso, T. Roger, D. G. Marangon, I. De Marco, M. Sanzaro, R. I. Woodward, J. F. Dynes, Z. Yuan, and A. J. Shields, "A photonic integrated quantum secure communication system," Nat. Photonics **15**, 850–856 (2021).
15. T. K. Paraïso, I. D. Marco, T. Roger, D. G. Marangon, J. F. Dynes, M. Lucamarini, Z. Yuan, and A. J. Shields, "A modulator-free quantum key distribution transmitter chip," npj Quantum Inf. **5**, 1 (2019).
16. C. Ma, W. D. Sacher, Z. Tang, J. C. Mikkelsen, Y. Yang, F. Xu, T. Thiessen, H.-K. Lo, and J. K. S. Poon, "Silicon photonic transmitter for polarization-encoded quantum key distribution," Optica **3**, 1274–1278 (2016).
17. D. Bunandar, A. Lentine, C. Lee, H. Cai, C. M. Long, N. Boynton, N. Martinez, C. DeRose, C. Chen, M. Grein, D. Trotter, A. Starbuck, A. Pomerene, S. Hamilton, F. N. C. Wong, R. Camacho, P. Davids, J. Urayama, and D. Englund, "Metropolitan quantum key distribution with silicon photonics," Phys. Rev. X **8**, 021009 (2018).
18. L. Kong, Z. Li, C. Li, L. Cao, Z. Xing, J. Cao, Y. Wang, X. Cai, and X. Zhou, "Photonic integrated quantum key distribution receiver for multiple users," Opt. Express **28**, 18449–18455 (2020).
19. W. Geng, C. Zhang, Y. Zheng, J. He, C. Zhou, and Y. Kong, "Stable quantum key distribution using a silicon photonic transceiver," Opt. Express **27**, 29045–29054 (2019).
20. H. Semenenko, P. Sibson, A. Hart, M. G. Thompson, J. G. Rarity, and C. Erven, "Chip-based measurement-device-independent quantum key distribution," Optica **7**, 238–242 (2020).

21. K. Wei, W. Li, H. Tan, Y. Li, H. Min, W.-J. Zhang, H. Li, L. You, Z. Wang, X. Jiang, T.-Y. Chen, S.-K. Liao, C.-Z. Peng, F. Xu, and J.-W. Pan, "High-speed measurement-device-independent quantum key distribution with integrated silicon photonics," Phys. Rev. X **10**, 031030 (2020).
22. G. Vest, P. Freiwang, J. Luhn, T. Vogl, M. Rau, L. Knips, W. Rosenfeld, and H. Weinfurter, "Quantum key distribution with a hand-held sender unit," Phys. Rev. Appl. **18**, 024067 (2022).
23. F. Beutel, H. Gehring, M. A. Wolff, C. Schuck, and W. Pernice, "Detector-integrated on-chip QKD receiver for GHz clock rates," npj Quantum Inf. **7**, 40 (2021).
24. Q. Liu, Y. Huang, Y. Du, Z. Zhao, M. Geng, Z. Zhang, and K. Wei, "Advances in chip-based quantum key distribution," Entropy **24**, 1334 (2022).
25. A. Boaron, B. Korzh, R. Houlmann, G. Boso, D. Rusca, S. Gray, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Simple 2.5 GHz time-bin quantum key distribution," Appl. Phys. Lett. **112**, 171108 (2018).
26. D. Rusca, A. Boaron, F. Grünenfelder, A. Martin, and H. Zbinden, "Finite-key analysis for the 1-decoy state QKD protocol," Appl. Phys. Lett. **112**, 171104 (2018).
27. D. Rusca, A. Boaron, M. Curty, A. Martin, and H. Zbinden, "Security proof for a simplified Bennett-Brassard 1984 quantum-key-distribution protocol," Phys. Rev. A **98**, 052336 (2018).
28. B. Korzh, N. Walenta, T. Lunghi, N. Gisin, and H. Zbinden, "Free-running InGaAs single photon detector with 1 dark count per second at 10% efficiency," Appl. Phys. Lett. **104**, 081108 (2014).
29. M. Caloz, M. Perrenoud, C. Autebert, B. Korzh, M. Weiss, C. Schönenberger, R. J. Warburton, H. Zbinden, and F. Bussières, "High-detection efficiency and low-timing jitter with amorphous superconducting nanowire single-photon detectors," Appl. Phys. Lett. **112**, 061103 (2018).
30. "SiGe BiCMOS and silicon photonics technologies," 2022, http://www.ihp-microelectronics.com/services/research-and-prototyping-service/mpw-prototyping-service/sigec-bicmos-technologies.
31. Q. Xu, S. Manipatruni, B. Schmidt, J. Shakya, and M. Lipson, "12.5 Gbit/s carrier-injection-based silicon micro-ring silicon modulators," Opt. Express **15**, 430–436 (2007).
32. D. Dai and S. He, "Analysis of the birefringence of a silicon-on-insulator rib waveguide," Appl. Opt. **43**, 1156–1161 (2004).
33. D. Dai, L. Liu, S. Gao, D.-X. Xu, and S. He, "Polarization management for silicon photonic integrated circuits," Laser Photon. Rev. **7**, 303–328 (2013).
34. L.-M. Chang, L. Liu, Y.-H. Gong, M.-Q. Tan, Y.-D. Yu, and Z.-Y. Li, "Polarization-independent directional coupler and polarization beam splitter based on asymmetric cross-slot waveguides," Appl. Opt. **57**, 678–683 (2018).
35. D. Wu, X. Li, L.-L. Wang, J.-S. Zhang, W. Chen, Y. Wang, H.-J. Wang, J.-G. Li, X.-J. Yin, Y.-D. Wu, and J.-M. An, "Temperature characterizations of silica asymmetric Mach-Zehnder interferometer chip for quantum key distribution," Chin. Phys. B **32**, 010305 (2022).
36. X. Li, M. Ren, J. Zhang, L. Wang, W. Chen, Y. Wang, X. Yin, Y. Wu, and J. An, "Interference at the single-photon level based on silica photonics robust against channel disturbance," Photon. Res. **9**, 222–228 (2021).
37. G.-W. Zhang, Y.-Y. Ding, W. Chen, F.-X. Wang, P. Ye, G.-Z. Huang, S. Wang, Z.-Q. Yin, J.-M. An, G.-C. Guo, and Z.-F. Han, "Polarization-insensitive interferometer based on a hybrid integrated planar lightwave circuit," Photon. Res. **9**, 2176–2181 (2021).
38. G. Corrielli, A. Crespi, and R. Osellame, "Femtosecond laser micromachining for integrated quantum photonics," Nanophotonics **10**, 3789–3812 (2021).
39. G. Corrielli, S. Atzeni, S. Piacentini, I. Pitsios, A. Crespi, and R. Osellame, "Symmetric polarization-insensitive directional couplers fabricated by femtosecond laser writing," Opt. Express **26**, 15101–15109 (2018).
40. L. A. Fernandes, J. R. Grenier, P. R. Herman, J. S. Aitchison, and P. V. S. Marques, "Stress induced birefringence tuning in femtosecond laser fabricated waveguides in fused silica," Opt. Express **20**, 24103–24114 (2012).
41. J. Martinez-Mateo, C. Pacher, M. Peev, A. Ciurana, and V. Martin, "Demystifying the information reconciliation protocol Cascade," arxiv, arXiv:1407.3257 (2014).
42. R. Albiero, C. Pentangelo, M. Gardina, S. Atzeni, F. Ceccarelli, and R. Osellame, "Toward higher integration density in femtosecond-laser-written programmable photonic circuits," Micromachines **13**, 1145 (2022).
43. C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, "Experimental long-distance decoy-state quantum key distribution based on polarization encoding," Phys. Rev. Lett. **98**, 010505 (2007).
44. G. B. Xavier, G. V. de Faria, G. P. Tao, and J. P. von der Weid, "Full polarization control for fiber optical quantum communication systems using polarization encoding," Opt. Express **16**, 1867–1873 (2008).
45. E. I. J.-S. Tassé and G. P. C. W. Daab, "White paper: why coherent detection systems may fail at compensating for polarization mode dispersion," 2015 https://lunainc.com/sites/default/files/assets/files/resource-library/White-Paper-Coherent-Detection-Systems-PMD-Compensation.pdf.
46. G. Roelkens, L. Liu, D. Liang, R. Jones, A. Fang, B. Koch, and J. Bowers, "III-V/silicon photonics for on-chip and intra-chip optical interconnects," Laser Photon. Rev. **4**, 751–779 (2010).
47. D. Liang and J. E. Bowers, "Recent progress in heterogeneous III-V-on-silicon photonic integration," Light Adv. Manuf. **2**, 59–83 (2021).
48. D. Knoll, S. Lischke, R. Barth, L. Zimmermann, B. Heinemann, H. Rucker, C. Mai, M. Kroh, A. Peczek, A. Awny, C. Ulusoy, A. Trusch, A. Kruger, J. Drews, M. Fraschke, D. Schmidt, M. Lisker, K. Voigt, E. Krune, and A. Mai, "High-performance photonic BiCMOS process for the fabrication of high-bandwidth electronic-photonic integrated circuits," in *IEEE International Electron Devices Meeting (IEDM)* (2015), pp. 15.6.1–15.6.4.

E.2. The limits of multiplexing quantum and classical channels: Case study of a 2.5 GHz discrete variable quantum key distribution system

Applied Physics Letters ARTICLE scitation.org/journal/apl

The limits of multiplexing quantum and classical channels: Case study of a 2.5 GHz discrete variable quantum key distribution system

Cite as: Appl. Phys. Lett. **119**, 124001 (2021); doi: 10.1063/5.0060232
Submitted: 16 June 2021 · Accepted: 1 September 2021 ·
Published Online: 20 September 2021

Fadri Grünenfelder,[a] Rebecka Sax, Alberto Boaron, and Hugo Zbinden

AFFILIATIONS

Group of Applied Physics, University of Geneva, Chemin de Pinchat 22, CH-1211 Geneva 4, Switzerland

[a]Author to whom correspondence should be addressed: fadri.gruenenfelder@unige.ch

ABSTRACT

Network integration of quantum key distribution is crucial for its future widespread deployment due to the high cost of using optical fibers dedicated for the quantum channel only. We studied the performance of a system running a simplified BB84 protocol at 2.5 GHz repetition rate, operating in the original wavelength band, the short O-band, when multiplexed with communication channels in the conventional wavelength band, and the short C-band. Our system could successfully generate secret keys over a single-mode fiber with a length of 95.5 km and with co-propagating classical signals at a launch power of 8.9 dBm. Furthermore, we discuss the performance of an ideal system under the same conditions, showing the limits of what is possible with a discrete variable system in the O-band. We also considered a short and lossy link with 51 km optical fiber resembling a real link in a metropolitan area network. In this scenario, we could exchange a secret key with a launch power up to 16.7 dBm in the classical channels.

Quantum key distribution (QKD) allows for distribution of secret keys between distant parties. As of today, a variety of QKD experiments have shown the feasibility of exchanging keys through a dedicated optical fiber over hundreds of kilometers.[1–3] However, the deployment and maintenance of optical fibers reserved for QKD only is rather costly and would, hence, limit the use cases of QKD. Therefore, a pressing issue is the seamless integration of QKD into the already existing optical fiber network infrastructure. Using wavelength division multiplexing (WDM), it is possible to couple both QKD and classical communication signals to the same fiber.[4] The challenge of this approach lies in the fact that QKD protocols typically require a launch power of less than 1 nW, whereas classical signals are launched with a power on the order of 1 mW per channel. A small fraction of the classical signal arriving at the QKD receiver is enough to increase the quantum bit error rate (QBER) to a value, where key extraction is impossible.

In many network environments, the classical signals populate the conventional wavelength band (C-band) from 1530 to 1565 nm separated by 0.8 nm in a dense WDM (DWDM) grid. Upon coexisting with a quantum channel, a classical signal generates noise at the quantum receiver due to imperfect isolation between the DWDM channels or via non-linear processes. Raman scattering and, depending on the choice of the DWDM channels and the quantum channel wavelength, four-wave mixing are the dominant non-linear processes.[5–7] While the channel isolation can be easily increased by adding suitable filters, non-linear processes can create photons at the same wavelength as the quantum signal, which cannot be spectrally filtered. Four-wave mixing is restricted to narrow spectral regions and can, therefore, be avoided by choosing the quantum wavelength carefully. Raman noise, on the other hand, exhibits a broad spectrum. For example, classical signals in the one C-band channel create a Raman noise spectrum covering the whole C-band with only two narrow local minima close to the pump wavelength.[5] In a densely populated WDM environment, the local minima are covered by the Raman noise of other channels.

One can make use of temporal filtering to help reduce the impact of noise photons at the quantum channel wavelength.[8,9] The propagation direction of the classical signals also has an influence on the amount of introduced noise. A signal counter-propagating to the quantum signal introduces more Raman noise than a co-propagating one due to the isotropic nature of Raman scattering and the higher power in vicinity to the receiver.[5]

Regarding the quantum channel wavelength, there are two frequent choices. It is placed either in the C-band or in the original wavelength band (O-band) from 1260 to 1360 nm. The advantage of

placing it in the C-band is the high fiber transmission. However, in a network, the quantum channel is then spectrally close to the classical channels and, therefore, strongly affected by Raman noise. Placing the quantum channel in the O-band reduces not only the amount of Raman noise but also the fiber transmission.[4,6,10] Generally speaking, it is advantageous to put the quantum signal in the O-band above a certain power threshold for the classical channels in the C-band.[10] In present-day networks, the total loss of a link is often dominated by the excess loss due to fiber connections, routing devices, or other components. In such an environment, a quantum channel in the O-band is advantageous since the transmission approaches the one of the C-bands, but the noise is reduced. For both choices of the quantum channel wavelength, the performance of QKD systems in the presence of classical communication has been studied.[4,9,11–14] One study also considered a quantum channel in the long wavelength band (L-band) from 1565 to 1625 nm and the short wavelength band (S-band) from 1460 to 1530 nm.[15]

The performance of a QKD system in a network depends heavily on the quality of the noise filtering on the receiver side. First, high isolation of the quantum channel from the classical channel is needed. This can be easily achieved by cascading WDM modules. Second, high Raman noise rejection is desired. The quality of noise rejection depends on the time-bandwidth product of the quantum signal and on how tight the temporal and spectral filtering can be implemented. In the case of continuous variable (CV-)QKD systems, the homodyne detection acts as a spectral filter.[16] For discrete variable (DV-)QKD systems, like the one presented in this study, filters have to be added at a cost of decreasing the transmission.

In this work, we demonstrate the operation of a QKD system with a quantum channel in the O-band with a wavelength of 1310 nm. We consider a scenario, where all the classical signals are co-propagating in the same fiber. This configuration is often found in metropolitan networks.[6,17] The quantum channel is launched in the same direction as the classical channels to minimize the degradation of the quantum signal. We consider a channel, where the loss is only given by the fiber attenuation, and another channel, where a substantial amount of loss is given by imperfections, which is a more realistic model for a network environment. Finally, we compare our setup to an ideal system in terms of temporal and spectral filtering.

We utilize a simple time-bin protocol with one decoy state, operating at a qubit repetition rate of 2.5 GHz.[18] The QKD implementation and the configuration of the classical channels are depicted in Fig. 1. Alice encodes the qubits in two time-bins. The bits in the Z basis, which are used to generate the key, are encoded in either the early or late time bin. Only one state in the X basis is used, namely, the superposition of the early and late bin with a fixed relative phase. The laser source is a gain-switched distributed feedback laser emitting pulses with a full width at half maximum (FWHM) of 26 ps. Due to the gain-switching, the pulses are chirped.

Bob uses free-running InGaAs/InP negative-feedback avalanche diodes (NFADs).[19] Both NFADs are cooled to −85 °C, show a detection efficiency of 25% at 1310 nm, and a jitter of 50 ps. The detector in the X basis (Z basis) shows a dark count rate of 108 Hz (91 Hz).

The dead time was set to 40 μs for the detector in the X basis and to 32 μs for the one in the Z basis. The detection window per time bin has a duration of 100 ps. Detections outside this window are ignored by the acquisition system. The error correction was performed with a Cascade algorithm[20] with an efficiency of 1.05. The compression factor was calculated over a privacy amplification block of 8×10^6 bits and taking into account finite-key effects.[21]

The classical communication runs over 13 C-band channels. They are multiplexed with a DWDM module and then amplified using an erbium-doped fiber amplifier. The quantum channel is added to the fiber with a coarse WDM (CWDM) module. On the receiver end, the quantum and classical signals are separated by a CWDM module. Another CWDM module is used to increase isolation between quantum and classical channels. To prevent classical signals to travel multiple times between the CWDM modules and to further improve the isolation, we added a fiber spool with a winding radius of 16 mm and 36 windings. This spool has an insertion loss of 1.0 at 1310 and

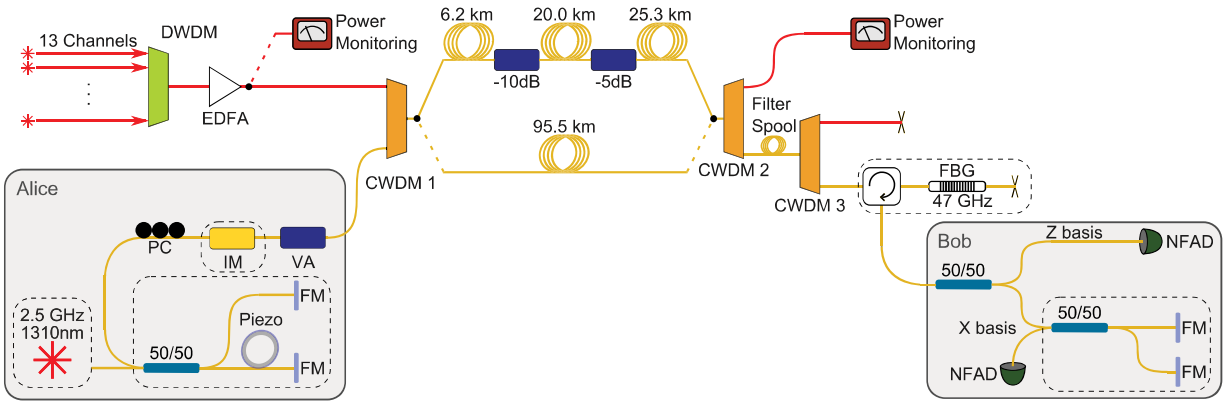


FIG. 1. Schematic of the setup. The dashed boxes are temperature stabilized. Fibers carrying the classical and quantum signals are shown in red and yellow, respectively. The transmission line is either a 95.5 km or a 51.5 km long fiber, and the latter is intercepted by attenuators. The classical launch power was measured after the amplifier and the receiver power at the 1550 nm port of the CWDM2. EDFA: erbium doped fiber amplifier; CWDM: coarse wavelength division multiplexer; DWDM: dense wavelength division multiplexer; FBG: fiber Bragg grating; FM: Faraday mirror; IM: intensity modulator; NFAD: negative-feedback avalanche photodiode; PC: polarization controller; VA: variable attenuator.

TABLE I. Loss introduced by the filters. The filters are named the same as in Fig. 1.

Description	Insertion loss at 1310 nm (dB)	Isolation from 1550 nm (dB)	Remarks
CWDM 1	0.8	>45	
CWDM 2	0.6	>45	
CWDM 3	0.8	>45	
Filter spool	1.0	32.9	
Fiber Bragg grating (FBG) and circulator	4.0	>30	The insertion loss is partially caused by spectral mismatch of laser pulse and filter. A loss of 1.8 dB was measured at peak transmission.
Loss due to detector jitter and pulse broadening by FBG	1.9	···	The loss was obtained by observing the ratio between detection events outside and inside the detection time window.

32.9 dB at 1550 nm. The remaining signal and noise are filtered by a fiber Bragg grating (FBG) with a transmission window of 47 GHz FWHM and more than 30 dB of extinction outside the window.

The excess loss experienced by the quantum signal due to the filters is summarized in Table I. The spectral width of the laser is close to the spectral width of the FBG, leading to increased insertion loss. Furthermore, the FBG is slightly chirped, and therefore, the already chirped laser pulse gets temporally broadened by the FBG. The broadening due to the FBG together with the detector jitter increases the chance to detect the pulse outside the predefined time window and, therefore, effectively introduces loss.

We performed secret key exchanges in two different regimes. First, we considered a case similar to a real network, where we used a standard single mode fiber (Corning® SMF-28e+®) with a length of 51.5 km together with 15 dB of excess loss in the channel (see Fig. 1 for details). This configuration acts as a model for a realistic link. In a metropolitan network, this loss could be due to connectors and routing equipment. Second, we exchanged a key over 95.5 km of the standard single-mode fiber (Corning® SMF-28e+®). This measurement was done for ease of comparison with previous studies. In both cases, we are interested in the secret key rate as a function of the launch power in the classical channels.

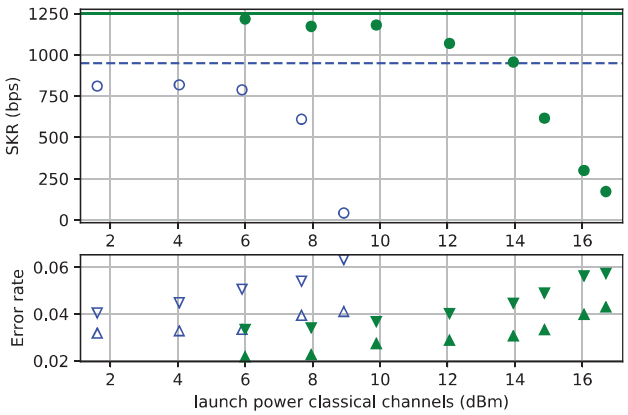


FIG. 2. Measured secret key rate, phase error rate (triangles pointing up), and QBER Z (triangles pointing down) as a function of the total launch power in the classical channels. The filled green points were measured with the 51.5 km link, and the empty blue points were measured with the 95.5 km link. The green solid line and the blue dashed line show the corresponding secret key rates without any classical signal.

In Fig. 2, we show the secret key rate, the QBER in the Z basis, and the phase error rate as a function of the classical launch power for the two different channel configurations. We obtained a secret key rate of 42 bps with a launch power of 8.9 dBm, which corresponds to a total received power of −12.1 dBm. In the case of the 51.5 km long and high loss link, a secret key rate of 172.2 bps could be obtained at a total launch power of 16.7 dBm, corresponding to a total received power of −11.8 dBm.

We were also interested in finding the limits of what would be possible with an ideal setup using the same protocol, quantum channel wavelength, and repetition rate as our experiment. For this, we assume that the filter block on Bob's side (CWDM 3, filter spool, circulator, and FBG in Fig. 1) has negligible insertion loss that the detectors have no jitter and no dark counts, and Alice is sending Fourier-limited

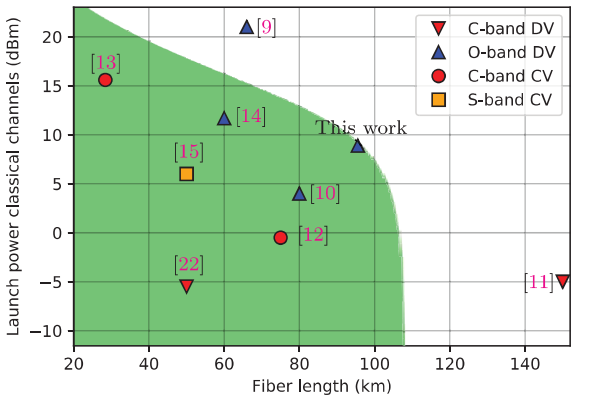


FIG. 3. Comparison to previous studies. The marker shape indicates if a continuous (CV) or discrete variable (DV) system was used and in which Telecom band the quantum channel was situated. The green surface indicates the region, where our experiment yields a positive secret key rate and was obtained by simulation with the same repetition rate, filter insertion loss, detector efficiency, pulse broadening, detector jitter, and dark counts as in our setup. For all studies, the data point with the highest launch power in the classical channels at the highest fiber length is included in this figure.

sech^2-pulses and that the filter spectrum of the FBG would be optimized both in bandwidth and in shape for these pulses. Our simulation shows that in this case, the maximum tolerable launch power would increase by 17.7 dB, where 14.1 dB could be gained due to the absence of jitter, the optimized shape, and bandwidth of the FBG and of the laser pulse and 3.6 dB could be gained if we had an ideal filter block with negligible insertion loss. We also estimated that the maximum tolerable launch power would increase by 1.5 dB if we used superconducting nanowire single-photon detectors (SNSPDs) with a jitter of 30 ps instead of NFADs with a jitter of 50 ps as in our experimental setup.

In Fig. 3 and Table II, we compare our work to previous studies. In summary, CV-QKD systems show the best performance both in the tolerated launch power and in the secret key rate at short and low loss links. At longer distances, DV-QKD systems, both in the C- and O-bands, outperform the CV-QKD systems. We can conclude that, as of today, DV-QKD systems operating in the O-band are best suited for networks with distances between 50 and 95 km and high launch power. Furthermore, our results in Fig. 2 with the short and high loss links show that in a real network, O-band DV-QKD systems can tolerate more power than suggested by measurements with links, where the loss is mainly given by the fiber. Another advantage of O-band QKD systems is that separating a signal from the C-band is possible with rather low loss and high isolation by using CWDM modules. In our case, one CWDM module has an insertion loss of 0.8 dB and a channel isolation of more than 45 dB. If we wanted to isolate one C-band channel from other C-band channels, we would need DWDM modules, which typically exhibit an insertion loss of 2.5 dB while having a channel isolation of only 25 dB. Therefore, it is best to use O-band QKD systems in metropolitan area networks.

In conclusion, we showed that with a simple and practical QKD system, it is possible to exchange a secret key in the presence of classical channels. We demonstrated the feasibility of key generation for a short distance and a high loss link and also for a medium range link, where the loss is predominantly given by the fiber attenuation. An ideal DV-QKD system at a repetition rate of 2.5 GHz in the O-band could tolerate a total launch power of 27 dBm of co-propagating classical signals over 95 km of single-mode fibers. This would be even enough to operate the QKD system in a backbone fiber network.[9] Finding ways to prepare almost ideal pulses and manufacturing optimized filters could increase noise tolerance of DV-QKD systems by more than an order of magnitude according to our simulation.

TABLE II. Comparison to previous studies. For each study, at least the points with the maximum fiber length and maximum launch power are mentioned. The classical channels are co-propagating with the quantum channel for all points shown here. The C-band spans from 1530 to 1565 nm, the O-band from 1260 to 1360 nm, and the S-band from 1460 to 1530 nm.

Continuous/discrete variable QKD	Wavelength band	Fiber length (km)	Att. quantum channel (dB)	Launch power (dBm)	Secret key rate (bps)	Finite-key statistics	Reference
Discrete	O	51.5	34.1	16.7	1.7×10^2	Yes	This work
		51.5	34.1	13.9	9.6×10^2		
		95.5	34.8	5.9	7.9×10^2		
		95.5	34.8	8.9	4.2×10^1		
		66.0	22.3	21.0	3.0×10^3	Yes	9
		66.0	22.3	16.0	3.9×10^3		
		66.0	22.3	11.0	4.8×10^3		
		40.0	12.8[a]	17.6	5.0×10^2	No	14
		50.0	16.0[a]	14.7	2.6×10^2		
		60.0	19.2[a]	11.7	1.8×10^2		
		60.0	19.2[a]	4.0	4.2×10^3	Yes	10
		80.0	25.6[a]	4.0	1.2×10^3		
	C	50.0	9.6	−18.5	1.1×10^6	Yes	22
		50.0	9.6	−12.5	8.6×10^5		
		50.0	9.6	−5.5	1.3×10^5		
		100.0	18.0[a]	−3.1	1.0×10^4	Yes	11
		150.0	27.0[a]	−8.1	2.0×10^3		
		150.0	27.0[a]	−5.0	1.2×10^3		
Continuous	C	25.0	5.0[a]	11.5	1.2×10^1	Yes	12
		75.0	15.0[a]	−0.5	9.0		
		75.0	15.0[a]	−3.0	4.9×10^2		
		13.2	3.0[a]	15.6	7.2×10^7	No	13
		28.4	6.4[a]	15.6	2.8×10^6		
	S	25.0	5.0[a]	14.0	4.0×10^5	No	15
		50.0	10.0[a]	6.0	1.7×10^6		

[a]The attenuation of the quantum channel was estimated from the fiber length.

We thank Romain Alléaume and Eleni Diamanti for the useful discussions and the Swiss NCCR QSIT (Grant No. 51NF40-185902) for financial support.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

[1]A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, Phys. Rev. Lett. **121**, 190502 (2018).
[2]J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin, M.-J. Li, H. Chen, H. Li, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **124**, 070501 (2020).
[3]M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R. I. Woodward, M.-J. Li, Z. Yuan, and A. J. Shields, arXiv:2012.15099 (2020).
[4]P. Townsend, Electron. Lett. **33**, 188 (1997).
[5]P. Eraerds, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, New J. Phys. **12**, 063027 (2010).
[6]S. Aleksic, F. Hipp, D. Winkler, A. Poppe, B. Schrenk, and G. Franzl, Opt. Express **23**, 10359 (2015).
[7]R. Tkach, A. Chraplyvy, F. Forghieri, A. Gnauck, and R. Derosier, J. Lightwave Technol. **13**, 841 (1995).
[8]K. A. Patel, J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, Phys. Rev. X **2**, 041010 (2012).
[9]Y. Mao, B.-X. Wang, C. Zhao, G. Wang, R. Wang, H. Wang, F. Zhou, J. Nie, Q. Chen, Y. Zhao, Q. Zhang, J. Zhang, T.-Y. Chen, and J.-W. Pan, Opt. Express **26**, 6010 (2018).
[10]L.-J. Wang, K.-H. Zou, W. Sun, Y. Mao, Y.-X. Zhu, H.-L. Yin, Q. Chen, Y. Zhao, F. Zhang, T.-Y. Chen, and J.-W. Pan, Phys. Rev. A **95**, 012301 (2017).
[11]B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plews, A. W. Sharpe, Z. Yuan, and A. J. Shields, Optica **4**, 163 (2017).
[12]R. Kumar, H. Qin, and R. Alléaume, New J. Phys. **17**, 043027 (2015).
[13]D. Milovancev, N. Vokic, F. Laudenbach, C. Pacher, H. Hubel, and B. Schrenk, J. Lightwave Technol. **39**, 3445 (2021).
[14]J.-Q. Geng, G.-J. Fan-Yuan, S. Wang, Q.-F. Zhang, Y.-Y. Hu, W. Chen, Z.-Q. Yin, D.-Y. He, G.-C. Guo, and Z.-F. Han, Opt. Lett. **46**, 2573 (2021).
[15]S. Kleis, J. Steinmayer, R. H. Derksen, and C. G. Schaeffer, Opt. Express **27**, 16540 (2019).
[16]B. Qi, W. Zhu, L. Qian, and H.-K. Lo, New J. Phys. **12**, 103042 (2010).
[17]A. Ciurana, J. Martínez-Mateo, M. Peev, A. Poppe, N. Walenta, H. Zbinden, and V. Martín, Opt. Express **22**, 1576 (2014).
[18]A. Boaron, B. Korzh, R. Houlmann, G. Boso, C. C. W. Lim, A. Martin, and H. Zbinden, J. Appl. Phys. **120**, 063101 (2016).
[19]E. Amri, G. Boso, B. Korzh, and H. Zbinden, Opt. Lett. **41**, 5728 (2016).
[20]J. Martinez-Mateo, C. Pacher, M. Peev, A. Ciurana, and V. Martin, Quantum Inf. Comput. **15**, 453 (2015).
[21]D. Rusca, A. Boaron, M. Curty, A. Martin, and H. Zbinden, Phys. Rev. A **98**, 052336 (2018).
[22]J. F. Dynes, W. W.-S. Tam, A. Plews, B. Fröhlich, A. W. Sharpe, M. Lucamarini, Z. Yuan, C. Radig, A. Straw, T. Edwards, and A. J. Shields, Sci. Rep. **6**, 35149 (2016).

E.3. Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems

nature photonics

Article

https://doi.org/10.1038/s41566-023-01168-2

Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems

Received: 31 August 2022

Accepted: 30 January 2023

Published online: 9 March 2023

Check for updates

Fadri Grünenfelder[1,4] ✉, Alberto Boaron[1], Giovanni V. Resta[1,2], Matthieu Perrenoud[1], Davide Rusca[1], Claudio Barreiro[1], Raphaël Houlmann[1], Rebecka Sax[1], Lorenzo Stasi[1,2], Sylvain El-Khoury[2], Esther Hänggi[3], Nico Bosshard[3], Félix Bussières[2] & Hugo Zbinden[1]

Quantum key distribution has emerged as the most viable scheme to guarantee information security in the presence of large-scale quantum computers and, thanks to the continuous progress made in the past 20 years, it is now commercially available. However, the secret key rates remain limited to just over 10 Mbps due to several bottlenecks on the receiver side. Here we present a custom multipixel superconducting nanowire single-photon detector that is designed to guarantee high count rates and precise timing discrimination. Leveraging the performance of the detector and coupling it to fast acquisition and real-time key distillation electronics, we remove two major roadblocks and achieve a considerable increase of the secret key rates with respect to the state of the art. In combination with a simple 2.5-GHz clocked time-bin quantum key distribution system, we can generate secret keys at a rate of 64 Mbps over a distance of 10.0 km and at a rate of 3.0 Mbps over a distance of 102.4 km with real-time key distillation.

Quantum key distribution (QKD) allows the exchange of cryptographic keys at a distance without assumptions on the technological limits of a possible eavesdropper, in particular their computational power[1,2]. In contrast, currently used public key systems rely on computationally demanding tasks[3,4]. Although, nowadays, an eavesdropper is bound to use classical computers, this could change in the near future with the advent of large-scale quantum computers, which would render an eavesdropper able to use powerful attacks that today's public key systems cannot withstand[5]. The security of QKD, however, is solely based on the laws of quantum mechanics, so, together with the one-time pad[6], private communication can be ensured even in a future where quantum computers are widely available.

Since the advent of the QKD era with the BB84 protocol[1], a variety of other protocols have been developed[2,7–9]. Although the complexity and level of device independence differ among protocols, the main goals remain the same, namely to increase the distance over which a secret key can be generated or, conversely, to maximize the secret key rate (SKR) over a certain distance. To give some context, we consider the use-case of encrypted video conferencing. The United States Federal Communications Commission recommends a download rate of 6 Mbps for this application[10], so, with one-time-pad encryption, one needs an SKR equal to this rate per user. For more demanding applications, such as data centres, much higher SKRs can be required. Recently, it was demonstrated that a single QKD link can achieve a sustainable SKR up to 13.72 Mbps over a channel equivalent to 10 km of single-mode fibre[11]. A proof-of-principle experiment using space division multiplexing showed that it would be possible to achieve an SKR of 105.7 Mbps over a distance of 7.9 km by using 37 QKD transmitters and receivers with a multicore fibre as the quantum channel[12].

[1]Group of Applied Physics, Genève, Switzerland. [2]ID Quantique SA, Acacias, Genève, Switzerland. [3]Lucerne School of Computer Science and Information Technology, Lucerne University of Applied Sciences and Arts, Rotkreuz, Switzerland. [4]Present address: University of Vigo, Vigo, Spain. ✉e-mail: fagrue@com.uvigo.es

https://doi.org/10.1038/s41566-023-01168-2

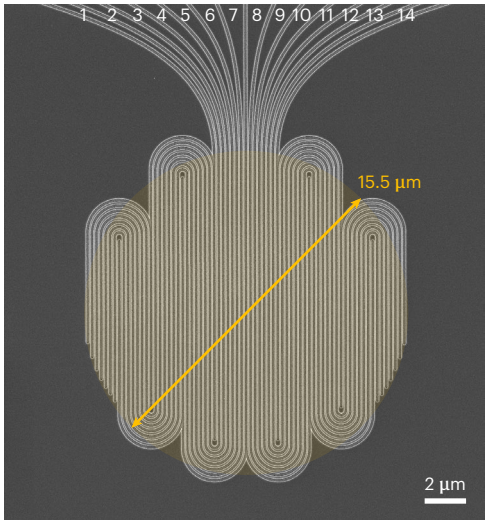


Fig. 1 | The SNSPD with 14 interleaved pixels. Image taken with a scanning electron microscope (SEM). The detector covers an area with a diameter of ~15.5 µm, which corresponds to an overlap of 99.7% (6σ) with the mode of the SMF-28 fibre. The width of the nanowires is 100 nm with a fill factor of 50%, and the interleaved design ensures uniform illumination of the pixels.

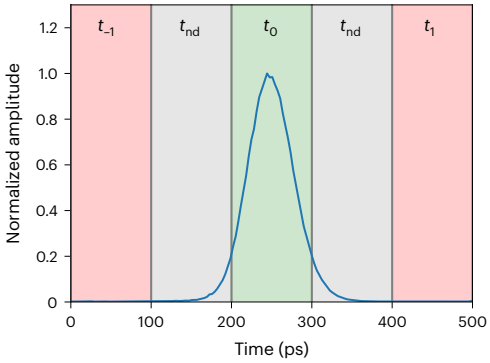


Fig. 2 | Timing resolution of detections. Histogram of the arrival times measured with one pixel (for a total count rate of 15.3 Mcps), which is the result of a convolution of the laser pulse shape and the jitter of the detector including readout electronics. Detections falling in the central green time bin t_0 are correct, detections falling in the red time bins t_{-1} and t_1 lead to errors, whereas events in the grey time bins t_{nd} are discarded to lower the QBER. In other words, jitter leads both to loss (t_{nd} bins) or errors (t_{-1} and t_1 bins).

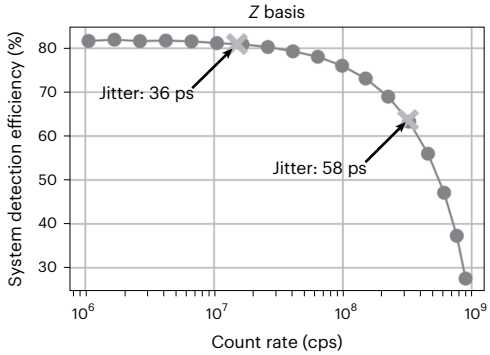


Fig. 3 | SDE of the multipixel detector versus count rate. At low count rates (below 10 Mcps) we measure a maximum SDE of 82%. As the count rate increases, the SDE begins to drop as more photons are reaching the detector within the dead time of each pixel. The crosses show the operating points for the performed key exchanges. At a distance of 10 km, the detector operates at 320 Mcps with SDE of 64% and temporal jitter of 58 ps, and at a distance of 100 km it operates at 15.0 Mcps with SDE of 81% and temporal jitter of 36 ps. The contributions to the jitter come both from the detector and the readout electronics.

To increase the SKRs even further, without multiplexing, a QKD system needs to fulfil a few key requirements. In the first place, the transmitter must emit qubits at a high repetition rate. However, a high repetition rate is only useful, in particular at shorter distances, if (1) the single-photon detectors are able to count at high rates with high efficiency and low timing jitter, (2) the readout and sifting electronics are able to process these rates and (3) the post-processing unit is capable of correcting the key (with low leakage) and performing privacy amplification in real time.

In this Article we report on our efforts to improve these three factors. In particular, we present a custom superconducting nanowire single-photon detector (SNSPD) featuring high count rates and high efficiency. We discuss how to optimize the parameters of a QKD system for high SKR and demonstrate an implementation generating an SKR of more than 60 Mbps over 10 km and 3 Mbps over 100 km. We use a simplified BB84 with time-bin encoding and one decoy state clocked at 2.5 GHz (time bins of 100 ps separated by 100 ps)[13–15], but the presented principles are valid also for polarization-based schemes[16].

Results

Multi-pixel SNSPD

We designed the multipixel SNSPD[17,18] such that high efficiency, low jitter and a high maximum count rate can be achieved simultaneously. We use niobium-titanium nitride (NbTiN), sputtered from a NbTi target in a nitrogen-rich atmosphere, as the superconducting material. The superconducting film has a thickness of ~9 nm and exhibits a critical temperature (T_c) of 8.8 K. The detector is composed of 14 independent pixels arranged in an interleaved geometry (Fig. 1). The number of pixels was chosen to comply with the requirements of Bob, and the generated signals are amplified at 40 K with a custom-made amplifier board. Thanks to the large number of pixels and the interleaved design (which guarantees uniform illumination of the pixels), the probability that two detections occur during the recovery time on the same pixel is minimized[18]. The detector is integrated into an optical cavity designed to maximize photon absorption at 1,550 nm, and exhibits a maximum system detection efficiency (SDE) of 82% (Fig. 3). The detector covers the same area as a conventional single-pixel SNSPD (~200 µm^2), so the length of each nanowire is greatly reduced, allowing for a much faster recovery time (on average <8 ns to be back at full efficiency). The fast recovery time of each pixel directly translates into the capability to reach ultrahigh detection rates when reading all 14 pixels simultaneously.

We also characterized the jitter of each pixel at different bias currents (I_b) and at a low count rate (100 kcps for each pixel), using a commercially available time-correlated single-photon-counting module. We obtained an average full-width at half-maximum (FWHM) jitter of 22 ps for bias currents (I_b) close to the critical current (I_c) and an average jitter of 26 ps for $I_b = 0.9I_c$, which represents an excellent starting point for when the detector will be operated at high count rates. In fact, during the key exchange, Bob must measure the arrival time of the pulses and be sure to assign them to the correct time bin, which has a 100-ps duration (Fig. 2). At the high rates of the QKD system, more and more photon detections occur when the bias current in the SNSPD has not yet reached its maximum value, that is, before the current and efficiency have fully recovered, thus causing an increase of the jitter. One contribution to the jitter at high detection rates is the variation in the amplitude of the detection signal, and this contribution can be minimized by using constant fraction discriminators (CFDs) instead of threshold discriminators on Bob's side. We designed and built CFDs optimized to

https://doi.org/10.1038/s41566-023-01168-2

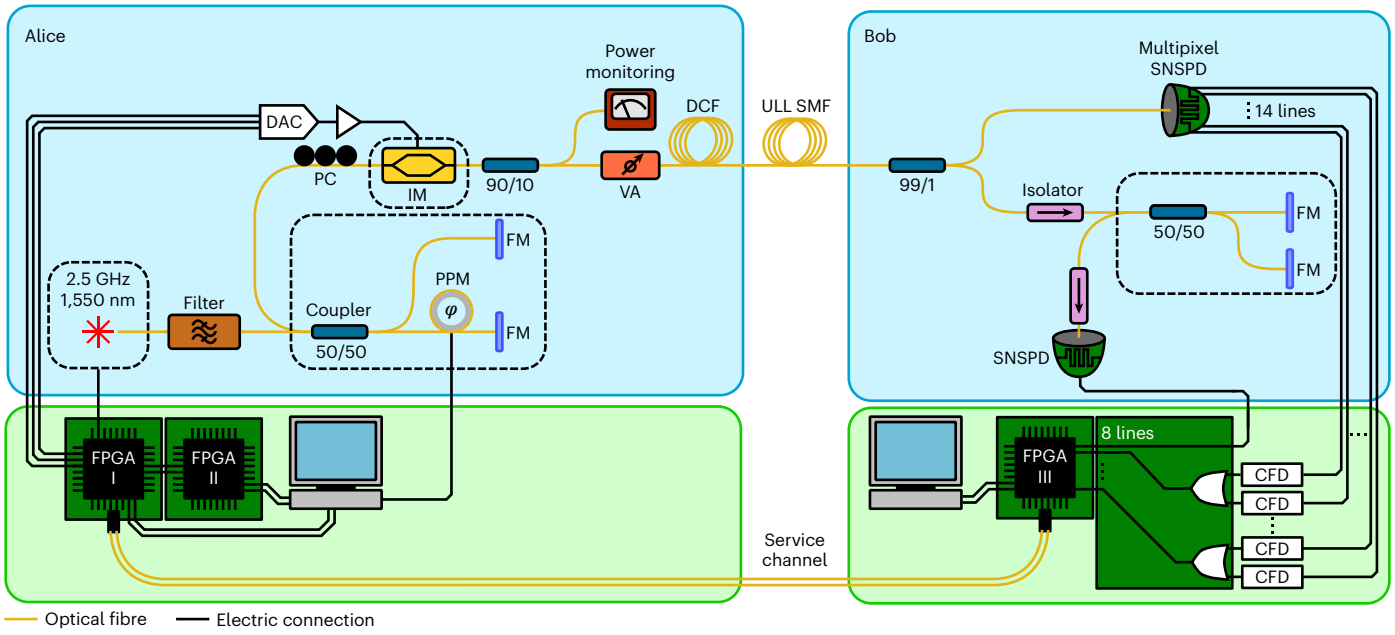


Fig. 4 | QKD set-up. Schematic representation of the QKD set-up with all the key components. CFD, constant fraction discriminator; DAC, digital-to-analogue converter; DCF, dispersion-compensating fibre; FM, Faraday mirror; FPGA, field-programmable gate array; IM, intensity modulator; PC, polarization controller; PPM, piezo-electric phase modulator; SNSPD, superconducting nanowire single-photon detector; ULL SMF, ultra-low-loss single-mode fibre; VA, variable attenuator. The dashed boxes are temperature-stabilized. FPGA I controls the state preparation, FPGA II is used for error correction, and FPGA III acquires the detection events. The sifting is done between FPGAs I and III. Both Michelson interferometers exhibit an imbalance of 200 ps.

be used with our multipixel detector, and with this readout electronics we simultaneously obtained a jitter below 60 ps and an efficiency of 64% at a count rate of 320 Mcps, which represents the operating point of the detector for our short-distance key exchange (Fig. 3).

It should be noted that, in the past, SPDs used in QKD experiments, such as avalanche photodiodes (APDs) and SNSPDs, have been shown to be vulnerable to hacking[19]. However, free-running multipixel SNSPDs with specifically designed readout electronics (including a shunt resistor to prevent latching) are particularly robust against such attacks[20], and monitoring coincidence clicks between the pixels can be a powerful countermeasure[21].

Error correction and privacy amplification

The ultrafast SNSPD and post-processing error correction are implemented in our QKD system as shown in Fig. 4. For error correction, we use a quasi-cyclic low-density parity check code (LDPC) with a syndrome size of 1/6, which is implemented in field-programmable gate arrays (FPGAs)[22]. Bob calculates the syndrome and sends it to Alice. The resource-intensive error correction core runs on FPGA II (Xilinx Virtex-6 LXT; Fig. 4) on Alice's side. One core can correct up to 110 Mcps and, by simply running two cores in parallel on the same FPGA, we achieve a throughput of 220 Mcps, which is high enough for our experiment. The privacy amplification is implemented on a consumer-type computer that receives the sifted key via a Generation 2 PCIe x4 connector (maximum throughput of 4 GB) from the FPGA. It runs on a consumer-type graphics processing unit (RTX 2070 Super Ventus OC) and has a maximum throughput of 3.4 Gbps. The block size of the algorithm is 2^{27} bit ≈ 134 Mbit, and the secrecy parameter we used is 10^{-9} (more details on the extraction are provided in ref. [23]).

Protocol description

We use the simplified BB84 with time-bin encoding and one decoy state[13–15]. Alice prepares the states as shown in Fig. 5. In the Z basis, we have a pulse either in the early (state $|0\rangle$) or in the late time bin (state $|1\rangle$). State $|+\rangle$ of the X basis carries pulses in both time bins, but with half the intensity compared to the pulses in the Z basis. These two pulses have a fixed phase relation, whereas, between the states, the phase has to be random. Alice chooses the basis at random with probabilities $p_{Z,\mathrm{A}}$ for the Z basis and $1-p_{Z,\mathrm{A}}$ for the X basis. In the case where she chooses the Z basis, she picks either $|0\rangle$ or $|1\rangle$ with equal probability. Additionally, she chooses at random between two mean photon numbers μ_0 and μ_1 with probabilities p_{μ_0} and p_{μ_1}. Bob picks a measurement basis at random with probabilities $p_{Z,\mathrm{B}}$ for the Z basis and $1-p_{Z,\mathrm{B}}$ for the X basis. The secret key is generated from the correlations in the Z basis, while the X basis is used to find an upper bound on the phase error rate via the decoy method[14].

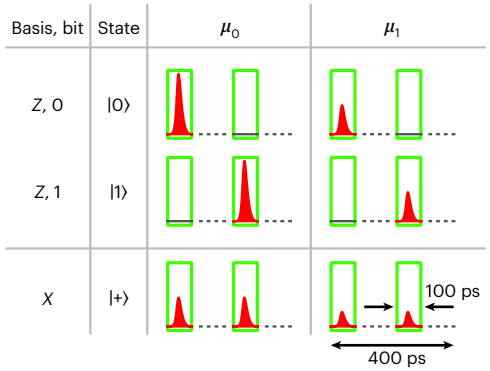


Fig. 5 | States prepared by Alice. Each state consists of two time bins. The two pulses of one state have a fixed phase relation, but pulses of different states have a random phase relation. Alice chooses the mean photon number μ_0 or μ_1 for each state at random. The green boxes are the detection time windows of Bob, each with a duration of 100 ps.

Implementation

A distributed feedback InGaAsP/InP multi-quantum-well laser diode is used to create a train of phase-randomized pulses with FWHM of 45 ps and at a rate of 2.5 GHz. The pulses then pass an imbalanced Michelson

https://doi.org/10.1038/s41566-023-01168-2

Table 1 | Measured SKR and corresponding experimental parameters

Fibre length (km)	Att. (dB)	μ_0	μ_1	p_{μ_0}	$p_{Z,A}$	$p_{Z,B}$	R_{sift} (Mbps)	ϕ_Z (%)	Q_Z (%)	SKR (Mbps)
10.0	1.58	0.49	0.22	0.74	0.65	0.99	159.4	0.8	0.4	64
102.4	16.34	0.46	0.20	0.79	0.66	0.99	7.8	1.0	0.3	3.0

Variables μ_0 and μ_1 are the mean photon number of the signal and decoy states, p_{μ_0} and $p_{\mu_1} = 1 - p_{\mu_0}$ are the corresponding probabilities to choose these values, $p_{Z,A}$ and $p_{Z,B}$ are the probabilities of Alice and Bob to choose the Z basis, R_{sift} is the sifted key rate, ϕ_Z is the phase error rate and Q_Z is the QBER Z. Att., attenuation.

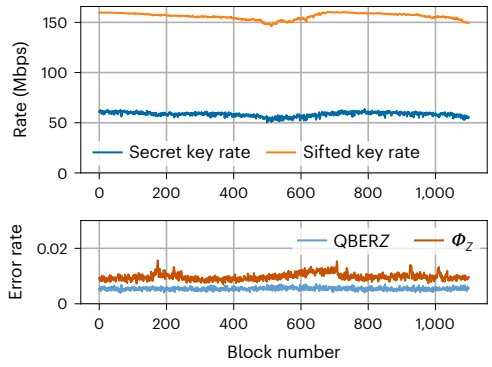


Fig. 6 | Stability of the key exchange. Measured secret and sifted key rate, QBER in the Z basis (QBER Z) and phase error rate (ϕ_Z) over consecutive privacy amplification blocks of 134 Mbits over 10 km of ULL fibre. The average acquisition time per block was 0.84 s.

interferometer with a time difference of 200 ps between the two arms. The states, as shown in Fig. 5, are encoded using an intensity modulator. The random numbers used to choose the states are produced by AES (Advanced Encryption Standard) cores seeded by a Quantis quantum random number generator (QRNG) from ID Quantique SA. The optimum value of $p_{Z,A}$ depends on the distance and, in any case, is well above 0.5. As a quantum channel there is an ultra-low-loss (ULL) single-mode fibre. Its dispersion is pre-compensated by dispersion-compensating fibre.

At the other end of the channel, at Bob, the basis is selected passively with the help of a fibre coupler. The optimal probability $p_{Z,B}$ is close to unity. This means that the sifting efficiency is significantly higher than in the standard BB84. In the Z basis, Bob measures the time of arrival of the signal with the multipixel detector described above. In the X basis, the pulses pass through a Michelson interferometer with the same delay as that of Alice. Here, the requirement on the detector is less stringent due to the high bias of the basis choice towards the Z basis. We chose a MoSi SNSPD with a parallel design (P-SNSPD)[24,25], which exhibits a timing jitter below 55 ps and a system detection efficiency of 85% at a count rate of 2 Mcps.

Alice uses the FPGA I to control the state preparation. The detections received by Bob are registered by FPGA III. The outputs of the detectors are interfaced to the FPGA III with an in-house-made card. This card can delay the 14 channels of the multipixel detector and the channel of the X basis detector individually, allowing us to synchronize them. Furthermore, the card combines the 14 channels of the multipixel detectors into seven channels with OR gates. At very high count rates, the combining of channels will mask some detections. By comparing the count rate of the QKD system with the count rate measured with time-to-digital converters, we found that, due to OR-gate masking, we lose 2.8% of the counts at 320 Mcps.

FPGAs I and III communicate directly via a fibre-optical service channel with a bandwidth of 10 Gbps to synchronize their clocks, for sifting and to perform error correction in real time. During sifting, Bob's FPGA III sends a short announcement after each detection to Alice's FGPA I. This contains the time elapsed since the previous detection, the basis and, if the event is the X basis, also the bit value of the detected states. No absolute time information is sent by Bob, only the relative time between detections. Alice uses this timing information to identify the corresponding state she sent. She replies by sending Bob the basis used in the state preparation. FPGA I forwards the sifted key to FPGA II, which performs the error correction.

Key exchange

We performed secret key exchanges through optical fibres with lengths of 10.0 km and 102.4 km for typically half an hour. In Fig. 6 we see the evolution of the sifted key rate, the SKR, the quantum bit error rate (QBER) Z and the phase error rate (ϕ_Z) for consecutive privacy amplification blocks. The slight variations of the key rates are due to slow polarization fluctuations and the polarization dependence of the SNSPD quantum efficiency. Note the very low error rates, which suggest that their fluctuations do not impact the SKR significantly. The mean photon number of the signal and decoy states and the probabilities to choose the Z basis at Alice and Bob were obtained by numerical optimization for each distance. We managed to exchange secret keys at a rate of 64 Mbps over a distance of 10.0 km and at a rate of 3.0 Mbps over a distance of 102.4 km. Table 1 shows the values of the SKR and the relevant parameters over one privacy amplification block of 134 Mbit (for the two distances).

Discussion

Although these are best-of-class results, there are still areas in which the QKD set-up could be optimized. Indeed, our QKD scheme was designed to be simple and suitable for a commercial device, and some adaptations could be made to increase even further the maximum SKR.

Due to our high repetition rate and consequently small time bins, we lose the detections that fall outside the time bins (Fig. 2). Whereas further reducing the timing jitter is not simple, we could just double the multipixel detectors at Bob. The advantage would be twofold: the detection rate will be halved on each detector, leading to an almost 10% increase in detection efficiency (Fig. 3), and there will be a decrease in jitter.

Our protocols allow for only one detector in the monitoring basis (projection in only one eigenstate of the X basis). To guarantee the security in this configuration we also need to monitor events where Alice used the Z basis and Bob measures in the X basis, and vice versa. Moreover, we also record events depending on which state was sent previously (some detection depends on two subsequent pulses, see ref. [14] for details). This forces us to choose, in the finite key scenario, a lower $p_{Z,A}$, which lowers the possible achievable sifted key rate.

Finally, the error correction is still not optimal. The used LDPC implementation has a leakage of 17% of the sifted key rate at a QBER of 0.5%. This is much higher than the Shannon limit of 5% of leakage. Rate-adaptive LDPC codes could help minimizing the leakage[26,27], but corresponding studies do not give information about the leakage at very low QBER. Another solution would be to implement the cascade error correction algorithm[28], which would allow approaching the Shannon limit, and in fact the state of the art allows for an efficiency of 1.038 and more than 500 MHz of throughput.

Implementing these improvements would allow us to achieve ~140 Mbps at 10 km (under the condition that the other parameters stay the same).

In conclusion, we have demonstrated SKRs up to 64 Mbps over a distance of 10.0 km. This achievement was possible thanks to a QKD system working at a high repetition rate of 2.5 GHz, coupled with our custom SNSPDs and readout electronics, which allow us to detect with low jitter and high efficiency at a high count rate. This result paves the way for secret key-demanding applications like real-time one-time-pad secured video encryption in a metropolitan area.

Online content

Any methods, additional references, Nature Portfolio reporting summaries, source data, extended data, supplementary information, acknowledgements, peer review information; details of author contributions and competing interests; and statements of data and code availability are available at https://doi.org/10.1038/s41566-023-01168-2.

References

1. Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. *Theor. Comput. Sci.* **560**, 7–11 (2014).
2. Ekert, A. K. Quantum cryptography based on Bell's Theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).
3. Rivest, R. L., Shamir, A. & Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **21**, 120–126 (1978).
4. Koblitz, N. Elliptic curve cryptosystems. *Math. Comput.* **48**, 203–209 (1987).
5. Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **26**, 1484–1509 (1997).
6. Shannon, C. E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **28**, 656–715 (1949).
7. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
8. Lucamarini, M., Yuan, Z. L., Dynes, J. F. & Shields, A. J. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400–403 (2018).
9. Ralph, T. C. Continuous variable quantum cryptography. *Phys. Rev. A* **61**, 010303(R) (1999).
10. *US Federal Communications Commission, Broadband Speed Guide* (USFCCC); https://www.fcc.gov/consumers/guides/broadband-speed-guide
11. Yuan, Z. et al. 10-mb/s quantum key distribution. *J. Light. Technol.* **36**, 3427–3433 (2018).
12. Bacco, D. et al. Boosting the secret key rate in a shared quantum and classical fibre communication system. *Commun. Phys.* **2**, 140 (2019).
13. Rusca, D., Boaron, A., Grünenfelder, F., Martin, A. & Zbinden, H. Finite-key analysis for the 1-decoy state QKD protocol. *Appl. Phys. Lett.* **112**, 171104 (2018).
14. Rusca, D., Boaron, A., Curty, M., Martin, A. & Zbinden, H. Security proof for a simplified Bennett-Brassard 1984 quantum-key-distribution protocol. *Phys. Rev. A* **98**, 052336 (2018).
15. Boaron, A. et al. Simple 2.5-GHz time-bin quantum key distribution. *Appl. Phys. Lett.* **112**, 171108 (2018).
16. Li, W. et al. High-rate quantum key distribution (in the press).
17. Dauler, E. A. et al. Multi-element superconducting nanowire single-photon detector. *IEEE Trans. Appl. Supercond.* **17**, 279–284 (2007).
18. Zhang, W. et al. A 16-pixel interleaved superconducting nanowire single-photon detector array with a maximum count rate exceeding 1.5 GHz. *IEEE Trans. Appl. Supercond.* **29**, 1–4 (2019).
19. Sun, S. & Huang, A. A review of security evaluation of practical quantum key distribution system. *Entropy* **24**, 260 (2022).
20. Lydersen, L., Akhlaghi, M. K., Majedi, A. H., Skaar, J. & Makarov, V. Controlling a superconducting nanowire single-photon detector using tailored bright illumination. *New J. Phys.* **13**, 113042 (2011).
21. Gras, G., Rusca, D., Zbinden, H. & Bussières, F. Countermeasure against quantum hacking using detection statistics. *Phys. Rev. Appl.* **15**, 034052 (2021).
22. Constantin, J. et al. An FPGA-based 4-Mbps secret key distillation engine for quantum key distribution systems. *J. Signal Process. Syst.* **86**, 1–15 (2017).
23. Bosshard, N., Christen, R. Hänggi, E. & Hofstetter, J. Fast privacy amplification on GPUs. Poster. In *Proc. 24th Annual Conference on Quantum Information Processing* (2021); https://doi.org/10.5281/zenodo.4551775
24. Perrenoud, M. et al. Operation of parallel SNSPDS at high detection rates. *Supercond. Sci. Technol.* **34**, 024002 (2021).
25. Stasi, L. et al. High-efficiency and fast photon-number resolving parallel superconducting nanowire single-photon detector. Preprint at *arXiv* https://doi.org/10.48550/arXiv.2207.14538 (2022).
26. Elkouss, D., Martinez-Mateo, J. & Martin, V. Information reconciliation for quantum key distribution. *Quantum Info. Comput.* **11**, 226–238 (2011).
27. Kiktenko, E. O., Trushechkin, A. S., Lim, C. C. W., Kurochkin, Y. V. & Fedorov, A. K. Symmetric blind information reconciliation for quantum key distribution. *Phys. Rev. Appl.* **8**, 044017 (2017).
28. Mao, H.-K., Li, Q., Hao, P.-L., Abd-El-Atty, B. & Iliyasu, A. M. High performance reconciliation for practical quantum key distribution systems. *Opt. Quantum Electron.* **54**, 1631 (2022).

Data availability
The data that support the findings of this study are available from the corresponding author upon reasonable request.

Code availability
The computer code that supports the findings of this study is available from the corresponding author upon reasonable request.

Acknowledgements
We acknowledge financial support from the European Quantum Flagship project openQKD (no. 857156 to A.B. and H.Z.), the Swiss NCCR QSIT (no. 51NF40-185902 to F.G. and H.Z.) and the SNSF Practice-to-Science (grant no. 199084 to E.H.) and EU Horizon 2020 research and innovation programme under a Marie Skłodowska-Curie grant agreement (no. 956071 AppQInfo MSCA ITN to L.S.).

Author contributions
F.G., A.B., H.Z., D.R. and R.S. conceived, designed and performed the experiment. G.V.R., M.P., L.S., S.E.-K. and F.B. designed, fabricated and characterized the detectors. C.B. designed the in-house made electronics. R.H. implemented the FPGA design. E.H. and N.B. worked on the privacy amplification. H.Z. and F.B. initiated and managed the project. All authors contributed to the writing of the Article.

Funding
Open access funding provided by University of Geneva.

Competing interests
The authors declare no competing interests.

Additional information
Correspondence and requests for materials should be addressed to Fadri Grünenfelder.

Peer review information *Nature Photonics* thanks Zhiliang Yuan and the other, anonymous, reviewer(s) for their contribution to the peer review of this work.

Bibliography

[1] Statista. Number of smartphone mobile network subscriptions worldwide from 2016 to 2022, with forecasts from 2023 to 2028, 2022. URL https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/. Accessed: 2023-06-15.

[2] The International Telecommunication Union. ITU connectivity infrastructure maps, 2023. URL https://www.itu.int/en/ITU-D/Technology/Pages/InteractiveTransmissionMaps.aspx. Accessed: 2023-06-15.

[3] Submarine Cable Networks. Trans-Atlantic, 2023. URL https://www.submarinenetworks.com/trans-atlantic. Accessed: 2023-06-15.

[4] Olga Khazan The Atlantic. The creepy, long-standing practice of undersea cable tapping, 2013. URL https://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/. Accessed: 2023-06-15.

[5] RTS. Enquête ouverte en France après des actes de malveillance contre le réseau de fibre optique, 2022. URL https://www.rts.ch/info/monde/13051063-enquete-ouverte-en-france-apres-des-actes-de-malveillance-contre-le-reseau-de-
html. Accessed: 2023-06-15.

[6] The Guardian. UK military chief warns of russian threat to vital undersea cables, 2022. URL https://www.theguardian.com/uk-news/2022/jan/08/uk-military-chief-warns-of-russian-threat-to-vital-undersea-cables. Accessed: 2023-06-15.

[7] RTS. Les câbles sous-marins, champ de tension des grandes puissances, 2023. URL https://www.rts.ch/info/monde/13685939-les-cables-sousmarins-champ-de-tension-des-grandes-puissances.html. Accessed: 2023-06-15.

[8] Tink Tank of the European Parlament. Security threats to undersea communications cables and infrastructure:consequences for the eu, 2022. URL https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2022)702557. Accessed: 2023-06-15.

[9] National Institute of Standards and US Department of Commerce Technology (NIST). Specification for the advanced encryption standard (AES). 2001. URL https://csrc.nist.gov/publications/detail/fips/197/final.

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

[11] Peter W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994. doi: 10.1109/SFCS.1994.365700.

[12] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, oct 1997. doi: 10.1137/s0097539795293172. URL `https://doi.org/10.1137%2Fs0097539795293172`.

[13] Kenneth Wright, Kristin M Beck, Sea Debnath, JM Amini, Y Nam, N Grzesiak, J-S Chen, NC Pisenti, M Chmielewski, C Collins, et al. Benchmarking an 11-qubit quantum computer. *Nature communications*, 10(1):1–6, 2019.

[14] Mirko Amico, Zain H. Saleem, and Muir Kumph. Experimental study of Shor's factoring algorithm using the IBM Q experience. *Phys. Rev. A*, 100:012305, Jul 2019. doi: 10.1103/PhysRevA.100.012305. URL `https://link.aps.org/doi/10.1103/PhysRevA.100.012305`.

[15] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando GSL Brandao, David A Buell, et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.

[16] F. Miller. *Telegraphic Code to Insure Privacy and Secrecy in the Transmission of Telegrams*. C.M. Cornwell, 1882. URL `https://books.google.se/books?id=tT9WAAAAYAAJ`.

[17] Gilbert Vernam. Secret signaling system, 1919. U.S. Patent no. 1,310,719.

[18] G. S. Vernam. Cipher printing telegraph systems: For secret wire and radio telegraphic communications. *Journal of the A.I.E.E.*, 45(2):109–115, 1926. doi: 10.1109/JAIEE.1926.6534724.

[19] C. E. Shannon. Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656–715, 1949. doi: 10.1002/j.1538-7305.1949.tb00928.x.

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

[21] Rajesh Duggirala, Amit Lal, Shankar Radhakrishnan, Rajesh Duggirala, Amit Lal, and Shankar Radhakrishnan. Radioisotope decay rate based counting clock. *Radioisotope Thin-Film Powered Microsystems*, pages 127–170, 2010.

[22] John G Rarity, PCM Owens, and PR Tapster. Quantum random-number generation and key sharing. *Journal of Modern Optics*, 41(12):2435–2444, 1994.

[23] André Stefanov, Nicolas Gisin, Olivier Guinnard, Laurent Guinnard, and Hugo Zbinden. Optical quantum random number generator. *Journal of Modern Optics*, 47(4):595–598, 2000.

[24] Thomas Jennewein, Ulrich Achleitner, Gregor Weihs, Harald Weinfurter, and Anton Zeilinger. A fast and compact quantum random number generator. *Review of Scientific Instruments*, 71(4):1675–1680, 2000.

[25] A E Ivanova, S A Chivilikhin, and A V Gleim. Quantum random number generator based on quantum nature of vacuum fluctuations. *Journal of Physics: Conference Series*, 917(6): 062008, nov 2017. doi: 10.1088/1742-6596/917/6/062008. URL `https://dx.doi.org/10.1088/1742-6596/917/6/062008`.

[26] Cédric Bruynsteen, Michael Vanhoecke, Johan Bauwelinck, and Xin Yin. Integrated balanced homodyne photonic–electronic detector for beyond 20 GHz shot-noise-limited measurements. *Optica*, 8(9):1146–1152, 2021.

[27] Bruno Sanguinetti, Anthony Martin, Hugo Zbinden, and Nicolas Gisin. Quantum random number generation on a mobile phone. *Phys. Rev. X*, 4:031056, Sep 2014. doi: 10.1103/PhysRevX.4.031056. URL `https://link.aps.org/doi/10.1103/PhysRevX.4.031056`.

[28] G.E. Moore. Cramming more components onto integrated circuits. *Proceedings of the IEEE*, 86(1):82–85, 1998. doi: 10.1109/JPROC.1998.658762.

[29] Stewart E Miller. Integrated optics: An introduction. *The Bell system technical journal*, 48(7):2059–2069, 1969.

[30] M. Suzuki, Y. Noda, H. Tanaka, S. Akiba, Y. Kushiro, and H. Isshiki. Monolithic integration of InGaAsP/InP distributed feedback laser and electroabsorption modulator by vapor phase epitaxy. *Journal of Lightwave Technology*, 5(9):1277–1285, 1987. doi: 10.1109/JLT.1987.1075650.

[31] Davide Bacco, Ilaria Vagniluca, Beatrice Da Lio, Nicola Biagi, Adriano Della Frera, Davide Calonico, Costanza Toninelli, Francesco S Cataliotti, Marco Bellini, Leif K Oxenløwe, et al. Field trial of a three-state quantum key distribution scheme in the Florence metropolitan area. *EPJ Quantum Technology*, 6(1):5, 2019.

[32] Marco Avesani, Luca Calderaro, Giulio Foletto, Costantino Agnesi, Francesco Picciariello, Francesco BL Santagiustina, Alessia Scriminich, Andrea Stanco, Francesco Vedovato, Mujtaba Zahidy, et al. Resource-effective quantum key distribution: a field trial in Padua city center. *Optics letters*, 46(12):2848–2851, 2021.

[33] A. R. Dixon, J. F. Dynes, M. Lucamarini, B. Fröhlich, A. W. Sharpe, A. Plews, S. Tam, Z. L. Yuan, Y. Tanizawa, H. Sato, S. Kawamura, M. Fujiwara, M. Sasaki, and A. J. Shields. High speed prototype quantum key distribution system and long term field trial. *Opt. Express*, 23(6):7583–7592, Mar 2015. doi: 10.1364/OE.23.007583. URL `https://opg.optica.org/oe/abstract.cfm?URI=oe-23-6-7583`.

[34] Yu-Ao Chen, Qiang Zhang, Teng-Yun Chen, Wen-Qi Cai, Sheng-Kai Liao, Jun Zhang, Kai Chen, Juan Yin, Ji-Gang Ren, Zhu Chen, et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature*, 589(7841):214–219, 2021.

[35] Sheng-Kai Liao, Wen-Qi Cai, Johannes Handsteiner, Bo Liu, Juan Yin, Liang Zhang, Dominik Rauch, Matthias Fink, Ji-Gang Ren, Wei-Yue Liu, Yang Li, Qi Shen, Yuan Cao, Feng-Zhi Li, Jian-Feng Wang, Yong-Mei Huang, Lei Deng, Tao Xi, Lu Ma, Tai Hu, Li Li, Nai-Le Liu, Franz Koidl, Peiyuan Wang, Yu-Ao Chen, Xiang-Bin Wang, Michael Steindorfer, Georg Kirchner, Chao-Yang Lu, Rong Shu, Rupert Ursin, Thomas Scheidl, Cheng-Zhi Peng, Jian-Yu Wang, Anton Zeilinger, and Jian-Wei Pan. Satellite-relayed intercontinental quantum network. *Phys. Rev. Lett.*, 120:030501, Jan 2018. doi: 10.1103/

PhysRevLett.120.030501. URL https://link.aps.org/doi/10.1103/PhysRevLett.120.030501.

[36] Iris Choi, Yu Rong Zhou, James F. Dynes, Zhiliang Yuan, Andreas Klar, Andrew Sharpe, Alan Plews, Marco Lucamarini, Christian Radig, Jörg Neubert, Helmut Griesser, Michael Eiselt, Christopher Chunnilall, Guillaume Lepert, Alastair Sinclair, Jörg-Peter Elbers, Andrew Lord, and Andrew Shields. Field trial of a quantum secured 10Gb/s DWDM transmission system over a single installed fiber. *Opt. Express*, 22(19):23121–23128, Sep 2014. doi: 10.1364/OE.22.023121. URL https://opg.optica.org/oe/abstract.cfm?URI=oe-22-19-23121.

[37] Rodrigo S Tessinari, Anderson Bravalheri, Emilio Hugues-Salas, Richard Collins, Djeylan Aktas, Rafael S Guimaraes, Obada Alia, John Rarity, George T Kanellos, Reza Nejabati, et al. Field trial of dynamic DV-QKD networking in the SDN-controlled fully-meshed optical metro network of the bristol city 5G UK test network. In *45th European Conference on Optical Communication (ECOC 2019)*, pages 1–4. IET, 2019.

[38] M Stanley, Y Gui, D Unnikrishnan, S.R.G Hall, and I Fatadin. Recent progress in quantum key distribution network deployments and standards. *Journal of Physics: Conference Series*, 2416(1):012001, dec 2022. doi: 10.1088/1742-6596/2416/1/012001. URL https://dx.doi.org/10.1088/1742-6596/2416/1/012001.

[39] Paramjeet Kaur, Andreas Boes, Guanghui Ren, Thach G. Nguyen, Gunther Roelkens, and Arnan Mitchell. Hybrid and heterogeneous photonic integration. *APL Photonics*, 6(6): 061102, 06 2021. ISSN 2378-0967. doi: 10.1063/5.0052700. URL https://doi.org/10.1063/5.0052700.

[40] T. Honjo, K. Inoue, and H. Takahashi. Differential-phase-shift quantum key distribution experiment with a planar light-wave circuit Mach-Zehnder interferometer. *Opt. Lett.*, 29 (23):2797–2799, Dec 2004. doi: 10.1364/OL.29.002797. URL https://opg.optica.org/ol/abstract.cfm?URI=ol-29-23-2797.

[41] Jennifer Aldama, Samael Sarmiento, Ignacio H. López Grande, Stefano Signorini, Luis Trigo Vidarte, and Valerio Pruneri. Integrated QKD and QRNG Photonic Technologies. *Journal of Lightwave Technology*, 40(23):7498–7517, 2022. doi: 10.1109/JLT.2022.3218075.

[42] Qiang Liu, Yinming Huang, Yongqiang Du, Zhengeng Zhao, Minming Geng, Zhenrong Zhang, and Kejin Wei. Advances in chip-based quantum key distribution. *Entropy*, 24(10), 2022. ISSN 1099-4300. doi: 10.3390/e24101334. URL https://www.mdpi.com/1099-4300/24/10/1334.

[43] S. Bogdanov, M. Y. Shalaginov, A. Boltasseva, and V. M. Shalaev. Material platforms for integrated quantum photonics. *Opt. Mater. Express*, 7(1):111–132, Jan 2017. doi: 10.1364/OME.7.000111. URL https://opg.optica.org/ome/abstract.cfm?URI=ome-7-1-111.

[44] Long Zhang, Shihan Hong, Yiwei Xie, and Daoxin Dai. New-generation ultra-low loss silicon photonic waveguide and devices. In *Asia Communications and Photonics Conference 2021*, page T1I.6. Optica Publishing Group, 2021. doi: 10.1364/ACPC.2021.T1I.6. URL https://opg.optica.org/abstract.cfm?URI=ACPC-2021-T1I.6.

[45] S. Y. Siew, B. Li, F. Gao, H. Y. Zheng, W. Zhang, P. Guo, S. W. Xie, A. Song, B. Dong, L. W. Luo, C. Li, X. Luo, and G.-Q. Lo. Review of silicon photonics technology and platform development. *Journal of Lightwave Technology*, 39(13):4374–4389, 2021. doi: 10.1109/JLT.2021.3066203.

[46] Giacomo Corrielli, Andrea Crespi, and Roberto Osellame. Femtosecond laser micromachining for integrated quantum photonics. *Nanophotonics*, 10(15):3789–3812, oct 2021. doi: 10.1515/nanoph-2021-0419. URL `https://doi.org/10.1515%2Fnanoph-2021-0419`.

[47] Chao Xiang, Joel Guo, Warren Jin, Lue Wu, Jonathan Peters, Weiqiang Xie, Lin Chang, Boqiang Shen, Heming Wang, Qi-Fan Yang, et al. High-performance lasers for fully integrated silicon nitride photonics. *Nature communications*, 12(1):6650, 2021.

[48] Yisu Yang, Hao Zhao, Xiaomin Ren, and Yongqing Huang. Monolithic integration of laser onto multilayer silicon nitride photonic integrated circuits with high efficiency at telecom wavelength. *Opt. Express*, 29(18):28912–28923, Aug 2021. doi: 10.1364/OE.434913. URL `https://opg.optica.org/oe/abstract.cfm?URI=oe-29-18-28912`.

[49] Fabian Beutel, Helge Gehring, Martin A Wolff, Carsten Schuck, and Wolfram Pernice. Detector-integrated on-chip QKD receiver for GHz clock rates. *npj Quantum Information*, 7(1):1–8, 2021.

[50] P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. L. O'Brien, and M. G. Thompson. Chip-based quantum key distribution. *Nature Communications*, 8(1), February 2017. doi: 10.1038/ncomms13984. URL `https://doi.org/10.1038/ncomms13984`.

[51] Innocenzo De Marco, Robert I. Woodward, George L. Roberts, Taofiq K. Paraïso, Thomas Roger, Mirko Sanzaro, Marco Lucamarini, Zhiliang Yuan, and Andrew J. Shields. Real-time operation of a multi-rate, multi-protocol quantum key distribution transmitter. *Optica*, 8 (6):911–915, Jun 2021. doi: 10.1364/OPTICA.423517. URL `https://opg.optica.org/optica/abstract.cfm?URI=optica-8-6-911`.

[52] Claire Autebert, Julien Trapateau, Adeline Orieux, Aristide Lemaître, Carmen Gomez-Carbonell, Eleni Diamanti, Isabelle Zaquine, and Sara Ducci. Multi-user quantum key distribution with entangled photons from an AlGaAs chip. *Quantum Science and Technology*, 1(1):01LT02, 2016.

[53] Weiqiang Xie, Lin Chang, Haowen Shu, Justin C. Norman, Jon D. Peters, Xingjun Wang, and John E. Bowers. Ultrahigh-Q AlGaAs-on-insulator microresonators for integrated nonlinear photonics. *Opt. Express*, 28(22):32894–32906, Oct 2020. doi: 10.1364/OE.405343. URL `https://opg.optica.org/oe/abstract.cfm?URI=oe-28-22-32894`.

[54] Ehsan Mobini, Daniel H. G. Espinosa, Kaustubh Vyas, and Ksenia Dolgaleva. AlGaAs nonlinear integrated photonics. *Micromachines*, 13(7), 2022. ISSN 2072-666X. doi: 10.3390/mi13070991. URL `https://www.mdpi.com/2072-666X/13/7/991`.

[55] Christof P Dietrich, Andrea Fiore, Mark G Thompson, Martin Kamp, and Sven Höfling. GaAs integrated quantum photonics: Towards compact and multi-functional quantum photonic integrated circuits. *Laser & Photonics Reviews*, 10(6):870–894, 2016.

[56] Francisco M. Soares, Moritz Baier, Tom Gaertner, Norbert Grote, Martin Moehrle, Tobias Beckerwerth, Patrick Runge, and Martin Schell. InP-based foundry PICs for optical interconnects. *Applied Sciences*, 9(8), 2019. ISSN 2076-3417. doi: 10.3390/app9081588. URL `https://www.mdpi.com/2076-3417/9/8/1588`.

[57] Meint Smit, Kevin Williams, and Jos Van Der Tol. Past, present, and future of InP-based photonic integration. *APL Photonics*, 4(5), 2019.

[58] Taofiq K. Paraïso, Innocenzo De Marco, Thomas Roger, Davide Giacomo Marangon, James F. Dynes, Marco Lucamarini, Zhiliang Yuan, and Andrew J. Shields. A modulator-free quantum key distribution transmitter chip. *npj Quantum Information*, 5:1–6, 2019.

[59] Taofiq K. Paraïso, Thomas Roger, Davide G. Marangon, Innocenzo De Marco, Mirko Sanzaro, Robert I. Woodward, James F. Dynes, Zhiliang Yuan, and Andrew J. Shields. A photonic integrated quantum secure communication system. *Nature Photonics*, 15(11): 850–856, October 2021. doi: 10.1038/s41566-021-00873-0.

[60] Henry Semenenko, Philip Sibson, Andy Hart, Mark G. Thompson, John G. Rarity, and Chris Erven. Chip-based measurement-device-independent quantum key distribution. *Optica*, 7(3):238–242, Mar 2020. doi: 10.1364/OPTICA.379679. URL `http://opg.optica.org/optica/abstract.cfm?URI=optica-7-3-238`.

[61] Thomas Roger, Taofiq Paraiso, Innocenzo De Marco, Davide G. Marangon, Zhiliang Yuan, and Andrew J. Shields. Real-time interferometric quantum random number generation on chip. *J. Opt. Soc. Am. B*, 36(3):B137–B142, Mar 2019. doi: 10.1364/JOSAB.36.00B137. URL `https://opg.optica.org/josab/abstract.cfm?URI=josab-36-3-B137`.

[62] Ben Haylock, Daniel Peace, Francesco Lenzini, Christian Weedbrook, and Mirko Lobino. Multiplexed quantum random number generation. *Quantum*, 3:141, 2019.

[63] Sina Saravi, Thomas Pertsch, and Frank Setzpfandt. Lithium niobate on insulator: An emerging platform for integrated quantum photonics. *Advanced Optical Materials*, 9(22):2100789, 2021. doi: https://doi.org/10.1002/adom.202100789. URL `https://onlinelibrary.wiley.com/doi/abs/10.1002/adom.202100789`.

[64] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *International Conference on Computers, Systems & Signal Processing, Bangalore, India, Dec 9-12, 1984*, pages 175–179, 1984.

[65] Davide Rusca, Alberto Boaron, Marcos Curty, Anthony Martin, and Hugo Zbinden. Security proof for a simplified Bennett-Brassard 1984 quantum-key-distribution protocol. *Phys. Rev. A*, 98:052336, Nov 2018. doi: 10.1103/PhysRevA.98.052336. URL `https://link.aps.org/doi/10.1103/PhysRevA.98.052336`.

[66] Davide Rusca, Alberto Boaron, Fadri Grünenfelder, Anthony Martin, and Hugo Zbinden. Finite-key analysis for the 1-decoy state QKD protocol. *Applied Physics Letters*, 112(17): 171104, apr 2018. doi: 10.1063/1.5023340. URL `https://doi.org/10.1063/1.5023340`.

[67] Alberto Boaron, Boris Korzh, Raphael Houlmann, Gianluca Boso, Davide Rusca, Stuart Gray, Ming-Jun Li, Daniel Nolan, Anthony Martin, and Hugo Zbinden. Simple 2.5 GHz time-bin quantum key distribution. *Applied Physics Letters*, 112(17):171108, apr 2018. doi:

10.1063/1.5027030. URL https://doi.org/10.1063/1.5027030.

[68] Fadri Grünenfelder, Rebecka Sax, Alberto Boaron, and Hugo Zbinden. The limits of multiplexing quantum and classical channels: Case study of a 2.5 GHz discrete variable quantum key distribution system. *Applied Physics Letters*, 119(12):124001, sep 2021. doi: 10.1063/5.0060232. URL https://doi.org/10.1063%2F5.0060232.

[69] Fadri Grünenfelder, Alberto Boaron, Matthieu Perrenoud, Giovanni V Resta, Davide Rusca, Claudio Barreiro, Raphaël Houlmann, Rebecka Sax, Lorenzo Stasi, Sylvain El-Khoury, et al. Fast single photon detectors and real-time key distillation: Enabling high secret key rate QKD systems. *arXiv preprint arXiv:2210.16126*, 2022.

[70] Rebecka Sax, Alberto Boaron, Gianluca Boso, Simone Atzeni, Andrea Crespi, Fadri Grünenfelder, Davide Rusca, Aws Al-Saadi, Danilo Bronzi, Sebastian Kupijai, Hanjo Rhee, Roberto Osellame, and Hugo Zbinden. High-speed integrated QKD system. *Photon. Res.*, 11(6):1007–1014, Jun 2023. doi: 10.1364/PRJ.481475. URL https://opg.optica.org/prj/abstract.cfm?URI=prj-11-6-1007.

[71] Davide Rusca, Hamid Tebyanian, Anthony Martin, and Hugo Zbinden. Fast self-testing quantum random number generator based on homodyne detection. *Applied Physics Letters*, 116(26), 07 2020.

[72] Thomas Van Himbeeck, Erik Woodhead, Nicolas J Cerf, Raúl García-Patrón, and Stefano Pironio. Semi-device-independent framework based on natural physical assumptions. *Quantum*, 1:33, 2017.

[73] Thomas Van Himbeeck and Stefano Pironio. Correlations and randomness generation based on energy constraints. *arXiv preprint arXiv:1905.09117*, 2019.

[74] Jesus Martinez-Mateo, Christoph Pacher, Momtchil Peev, Alex Ciurana, and Vicente Martin. Demystifying the information reconciliation protocol Cascade. *Quantum Information and Computation*, 2014. doi: 10.48550/ARXIV.1407.3257. URL https://arxiv.org/abs/1407.3257.

[75] Alberto Boaron. *Long-distance and high-speed quantum key distribution.* PhD thesis, Université de Genève, Université de Genève, 2020.

[76] Davide Rusca. *Security of quantum cryptography: from quantum random key generation to quantum key distribution.* PhD thesis, Université de Genève, Université de Genève, 2020.

[77] Fadri Grunenfelder. *Performance, Security and Network Integration of Simplified BB84 Quantum Key Distribution.* PhD thesis, Université de Genève, Université de Genève, 2022.

[78] Kiyoshi Tamaki, Marcos Curty, Go Kato, Hoi-Kwong Lo, and Koji Azuma. Loss-tolerant quantum cryptography with imperfect sources. *Phys. Rev. A*, 90:052314, Nov 2014. doi: 10.1103/PhysRevA.90.052314. URL https://link.aps.org/doi/10.1103/PhysRevA.90.052314.

[79] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C. Sanders. Limitations on practical quantum cryptography. *Phys. Rev. Lett.*, 85:1330–1333, Aug 2000. doi: 10.1103/PhysRevLett.85.1330. URL https://link.aps.org/doi/10.1103/PhysRevLett.85.1330.

[80] Won-Young Hwang. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.*, 91:057901, Aug 2003. doi: 10.1103/PhysRevLett.91.057901. URL https://link.aps.org/doi/10.1103/PhysRevLett.91.057901.

[81] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94:230504, Jun 2005. doi: 10.1103/PhysRevLett.94.230504. URL https://link.aps.org/doi/10.1103/PhysRevLett.94.230504.

[82] Masahito Hayashi and Ryota Nakayama. Security analysis of the decoy method with the Bennett–Brassard 1984 protocol for finite key lengths. *New Journal of Physics*, 16(6): 063009, jun 2014. doi: 10.1088/1367-2630/16/6/063009. URL https://dx.doi.org/10.1088/1367-2630/16/6/063009.

[83] Charles Ci Wen Lim, Marcos Curty, Nino Walenta, Feihu Xu, and Hugo Zbinden. Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A*, 89: 022307, Feb 2014. doi: 10.1103/PhysRevA.89.022307. URL https://link.aps.org/doi/10.1103/PhysRevA.89.022307.

[84] Xiang-Bin Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.*, 94:230503, Jun 2005. doi: 10.1103/PhysRevLett.94.230503. URL https://link.aps.org/doi/10.1103/PhysRevLett.94.230503.

[85] Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo. Practical decoy state for quantum key distribution. *Phys. Rev. A*, 72:012326, Jul 2005. doi: 10.1103/PhysRevA.72.012326. URL https://link.aps.org/doi/10.1103/PhysRevA.72.012326.

[86] Alberto Boaron, Gianluca Boso, Davide Rusca, Cédric Vulliez, Claire Autebert, Misael Caloz, Matthieu Perrenoud, Gaëtan Gras, Félix Bussières, Ming Jun Li, Daniel Nolan, Anthony Martin, and Hugo Zbinden. Secure Quantum Key Distribution over 421 km of Optical Fiber. *Physical Review Letters*, 121(19):1–4, 2018. doi: 10.1103/PhysRevLett.121.190502.

[87] Emna Amri. *Single photon detection for quantum technologies.* PhD thesis, Université de Genève, Université de Genève, 2020.

[88] Misael Caloz. *Superconducting nanowire single-photon detectors for quantum communication applications.* PhD thesis, Université de Genève, Université de Genève, 2019.

[89] Boris Korzh. *High-performance single-photon detectors and applications in quantum communication.* PhD thesis, Université de Genève, Université de Genève, 2016.

[90] Emna Amri, Gianluca Boso, Boris Korzh, and Hugo Zbinden. Temporal jitter in free-running InGaAs/InP single-photon avalanche detectors. *Opt. Lett.*, 41(24):5728–5731, Dec 2016. doi: 10.1364/OL.41.005728. URL https://opg.optica.org/ol/abstract.cfm?URI=ol-41-24-5728.

[91] B. Korzh, N. Walenta, T. Lunghi, N. Gisin, and H. Zbinden. Free-running InGaAs single photon detector with 1 dark count per second at 10% efficiency. *Applied Physics Letters*, 104(8):081108, feb 2014. doi: 10.1063/1.4866582. URL https://doi.org/10.1063%2F1.4866582.

[92] Misael Caloz, Matthieu Perrenoud, Claire Autebert, Boris Korzh, Markus Weiss, Christian

Schönenberger, Richard J. Warburton, Hugo Zbinden, and Fé lix Bussières. High-detection efficiency and low-timing jitter with amorphous superconducting nanowire single-photon detectors. *Applied Physics Letters*, 112(6):061103, feb 2018. doi: 10.1063/1.5010102. URL https://doi.org/10.1063%2F1.5010102.

[93] D Stucki, M Legré, F Buntschu, B Clausen, N Felber, N Gisin, L Henzen, P Junod, G Litzistorf, P Monbaron, L Monat, J-B Page, D Perroud, G Ribordy, A Rochas, S Robyr, J Tavares, R Thew, P Trinkler, S Ventura, R Voirol, N Walenta, and H Zbinden. Long-term performance of the SwissQuantum quantum key distribution network in a field environment. *New Journal of Physics*, 13(12):123001, dec 2011. doi: 10.1088/1367-2630/13/12/123001. URL https://dx.doi.org/10.1088/1367-2630/13/12/123001.

[94] James F Dynes, Winci WS Tam, Alan Plews, Bernd Fröhlich, Andrew W Sharpe, Marco Lucamarini, Zhiliang Yuan, Christian Radig, Andrew Straw, Tim Edwards, et al. Ultra-high bandwidth quantum secured data transmission. *Scientific reports*, 6(1):35149, 2016.

[95] Bernd Fröhlich, Marco Lucamarini, James F. Dynes, Lucian C. Comandar, Winci W.-S. Tam, Alan Plews, Andrew W. Sharpe, Zhiliang Yuan, and Andrew J. Shields. Long-distance quantum key distribution secure against coherent attacks. *Optica*, 4(1):163–167, Jan 2017. doi: 10.1364/OPTICA.4.000163. URL https://opg.optica.org/optica/abstract.cfm?URI=optica-4-1-163.

[96] Yingqiu Mao, Bi-Xiao Wang, Chunxu Zhao, Guangquan Wang, Ruichun Wang, Honghai Wang, Fei Zhou, Jimin Nie, Qing Chen, Yong Zhao, Qiang Zhang, Jun Zhang, Teng-Yun Chen, and Jian-Wei Pan. Integrating quantum key distribution with classical communications in backbone fiber network. *Opt. Express*, 26(5):6010–6020, Mar 2018. doi: 10.1364/OE.26.006010. URL https://opg.optica.org/oe/abstract.cfm?URI=oe-26-5-6010.

[97] Jia-Qi Geng, Guan-Jie Fan-Yuan, Shuang Wang, Qi-Fa Zhang, Ying-Ying Hu, Wei Chen, Zhen-Qiang Yin, De-Yong He, Guang-Can Guo, and Zheng-Fu Han. Coexistence of quantum key distribution and optical transport network based on standard single-mode fiber at high launch power. *Opt. Lett.*, 46(11):2573–2576, Jun 2021. doi: 10.1364/OL.426175. URL https://opg.optica.org/ol/abstract.cfm?URI=ol-46-11-2573.

[98] Liu-Jun Wang, Kai-Heng Zou, Wei Sun, Yingqiu Mao, Yi-Xiao Zhu, Hua-Lei Yin, Qing Chen, Yong Zhao, Fan Zhang, Teng-Yun Chen, and Jian-Wei Pan. Long-distance copropagation of quantum key distribution and terabit classical optical data channels. *Phys. Rev. A*, 95:012301, Jan 2017. doi: 10.1103/PhysRevA.95.012301. URL https://link.aps.org/doi/10.1103/PhysRevA.95.012301.

[99] Fabian Beutel, Frank Brückerhoff-Plückelmann, Helge Gehring, Vadim Kovalyuk, Philipp Zolotov, Gregory Goltsman, and Wolfram H. P. Pernice. Fully integrated four-channel wavelength-division multiplexed QKD receiver. *Optica*, 9(10):1121–1130, Oct 2022. doi: 10.1364/OPTICA.468982. URL https://opg.optica.org/optica/abstract.cfm?URI=optica-9-10-1121.

[100] Alasdair B. Price, Philip Sibson, Chris Erven, John G. Rarity, and Mark G. Thompson. High-speed quantum key distribution with wavelength-division multiplexing on integrated photonic devices. In *Conference on Lasers and Electro-Optics*, page JTh2A.24. Optica Publishing Group, 2018. doi: 10.1364/CLEO_AT.2018.JTh2A.24. URL https://opg.optica.org/abstract.cfm?URI=CLEO_AT-2018-JTh2A.24.

[101] Jingyuan Chen. A broadband wavelength demultiplexer assisted by SWG-based directional couplers. *Optik*, 202:163602, 2020. ISSN 0030-4026. doi: https://doi.org/10.1016/j.ijleo.2019.163602. URL https://www.sciencedirect.com/science/article/pii/S0030402619315001.

[102] Fuling Wang, Xiao Xu, Chen Zhang, Chonglei Sun, and Jia Zhao. Design and demonstration of compact and broadband wavelength demultiplexer based on subwavelength grating (swg). *IEEE Photonics Journal*, 14(2):1–6, 2022. doi: 10.1109/JPHOT.2022.3160180.

[103] Tianyi Hao, Alejandro Sánchez-Postigo, Pavel Cheben, Alejandro Ortega-Moñux, and Winnie N. Ye. Dual-band polarization-independent subwavelength grating coupler for wavelength demultiplexing. *IEEE Photonics Technology Letters*, 32(18):1163–1166, 2020. doi: 10.1109/LPT.2020.3014640.

[104] Zhiliang Yuan, Alan Plews, Ririka Takahashi, Kazuaki Doi, Winci Tam, Andrew Sharpe, Alexander Dixon, Evan Lavelle, James Dynes, Akira Murakami, Mamko Kujiraoka, Marco Lucamarini, Yoshimichi Tanizawa, Hideaki Sato, and Andrew J. Shields. 10-Mb/s Quantum Key Distribution. *J. Lightwave Technol.*, 36(16):3427–3433, Aug 2018. URL https://opg.optica.org/jlt/abstract.cfm?URI=jlt-36-16-3427.

[105] Giovanni V Resta, Lorenzo Stasi, Matthieu Perrenoud, Sylvain El-Khoury, Tiff Brydges, Rob Thew, Hugo Zbinden, and Félix Bussières. Gigahertz detection rates and dynamic photon-number resolution with superconducting nanowire arrays. *Nano Letters*, 2023.

[106] Wei Li, Likang Zhang, Hao Tan, Yichen Lu, Sheng-Kai Liao, Jia Huang, Hao Li, Zhen Wang, Hao-Kun Mao, Bingze Yan, et al. High-rate quantum key distribution exceeding 110 Mbps. *Nature Photonics*, 17(5):416–421, 2023.

[107] Xin Mu, Sailong Wu, Lirong Cheng, and H.Y. Fu. Edge couplers in silicon photonic integrated circuits: A review. *Applied Sciences*, 10(4), 2020. ISSN 2076-3417. doi: 10.3390/app10041538. URL https://www.mdpi.com/2076-3417/10/4/1538.

[108] Siddharth Nambiar, Purnima Sethi, and Shankar Kumar Selvaraja. Grating-assisted fiber to chip coupling for SOI photonic circuits. *Applied Sciences*, 8(7), 2018. ISSN 2076-3417. doi: 10.3390/app8071142. URL https://www.mdpi.com/2076-3417/8/7/1142.

[109] Riccardo Marchetti, Cosimo Lacava, Lee Carroll, Kamil Gradkowski, and Paolo Minzioni. Coupling strategies for silicon photonics integrated chips *Invited*. *Photon. Res.*, 7(2):201–239, Feb 2019. doi: 10.1364/PRJ.7.000201. URL https://opg.optica.org/prj/abstract.cfm?URI=prj-7-2-201.

[110] Lirong Cheng, Simei Mao, Zhi Li, Yaqi Han, and H. Y. Fu. Grating couplers on silicon photonics: Design principles, emerging trends and practical issues. *Micromachines*, 11 (7), 2020. ISSN 2072-666X. doi: 10.3390/mi11070666. URL https://www.mdpi.com/2072-666X/11/7/666.

[111] Maxime Jacques, Alireza Samani, Eslam El-Fiky, David Patel, Zhenping Xing, and David V. Plant. Optimization of thermo-optic phase-shifter design and mitigation of thermal crosstalk on the SOI platform. *Opt. Express*, 27(8):10456–10471, Apr 2019. doi: 10.1364/OE.27.010456. URL https://opg.optica.org/oe/abstract.cfm?URI=oe-27-8-10456.

[112] Shengping Liu, Junbo Feng, Ye Tian, Heng Zhao, Li Jin, Boling Ouyang, Jiguang Zhu, and Jin Guo. Thermo-optic phase shifters based on silicon-on-insulator platform: State-of-the-art and a review. *Frontiers of Optoelectronics*, 15(1):9, 2022.

[113] Georgios Sinatkas, Thomas Christopoulos, Odysseas Tsilipakos, and Emmanouil E. Kriezis. Electro-optic modulation in integrated photonics. *Journal of Applied Physics*, 130(1), 07 2021. ISSN 0021-8979. doi: 10.1063/5.0048712. URL `https://doi.org/10.1063/5.0048712`. 010901.

[114] Stefan Meister, Hanjo Rhee, Aws Al-Saadi, Bülent A. Franke, Sebastian Kupijai, Christoph Theiss, Lars Zimmermann, Bernd Tillack, Harald H. Richter, Hui Tian, David Stolarek, Thomas Schneider, Ulrike Woggon, and Hans J. Eichler. Matching p-i-n-junctions and optical modes enables fast and ultra-small silicon modulators. *Opt. Express*, 21(13): 16210–16221, Jul 2013. doi: 10.1364/OE.21.016210. URL `https://opg.optica.org/oe/abstract.cfm?URI=oe-21-13-16210`.

[115] Lucas B Soldano and Erik CM Pennings. Optical multi-mode interference devices based on self-imaging: principles and applications. *Journal of lightwave technology*, 13(4):615–627, 1995.

[116] Molly Piels and John E. Bowers. 1 - photodetectors for silicon photonic integrated circuits. In Bahram Nabet, editor, *Photodetectors*, pages 3–20. Woodhead Publishing, 2016. ISBN 978-1-78242-445-1. doi: https://doi.org/10.1016/B978-1-78242-445-1.00001-4. URL `https://www.sciencedirect.com/science/article/pii/B9781782424451000014`.

[117] S. Lischke, D. Knoll, D. Wolansky, M. Kroh, A. Peczek, and L. Zimmermann. High-speed, high-responsivity Ge photodiode with NiSi contacts for an advanced photonic BiCMOS technology. pages 61–62, 2017. doi: 10.1109/GROUP4.2017.8082196.

[118] Stefan Lischke, Dieter Knoll, Christian Mai, Lars Zimmermann, Anna Peczek, Marcel Kroh, Andreas Trusch, Edgar Krune, Karsten Voigt, and A. Mai. High bandwidth, high responsivity waveguide-coupled germanium p-i-n photodiode. *Opt. Express*, 23(21): 27213–27220, Oct 2015. doi: 10.1364/OE.23.027213. URL `https://opg.optica.org/oe/abstract.cfm?URI=oe-23-21-27213`.

[119] Daoxin Dai and Sailing He. Analysis of the birefringence of a silicon-on-insulator rib waveguide. *Appl. Opt.*, 43(5):1156–1161, Feb 2004. doi: 10.1364/AO.43.001156. URL `https://opg.optica.org/ao/abstract.cfm?URI=ao-43-5-1156`.

[120] Daoxin Dai, Liu Liu, Shiming Gao, Dan-Xia Xu, and Sailing He. Polarization management for silicon photonic integrated circuits. *Laser & Photonics Reviews*, 7(3):303–328, 2013.

[121] Li-Min Chang, Lei Liu, Yuan-Hao Gong, Man-Qing Tan, Yu-De Yu, and Zhi-Yong Li. Polarization-independent directional coupler and polarization beam splitter based on asymmetric cross-slot waveguides. *Applied Optics*, 57(4):678–683, 2018.

[122] Dan Wu, Xiao Li, Liang-Liang Wang, Jia-Shun Zhang, Wei Chen, Yue Wang, Hong-Jie Wang, Jian-Guang Li, Xiao-Jie Yin, Yuan-Da Wu, and Jun-Ming An. Temperature characterizations of silica asymmetric Mach-Zehnder interferometer chip for quantum key distribution. *Chinese Physics B*, 2022. URL `http://iopscience.iop.org/article/10.1088/1674-1056/ac9224`.

[123] Xiao Li, Meizhen Ren, Jiashun Zhang, Liangliang Wang, Wei Chen, Yue Wang, Xiaojie Yin, Yuanda Wu, and Junming An. Interference at the single-photon level based on silica photonics robust against channel disturbance. *Photon. Res.*, 9(2):222–228, Feb 2021. doi: 10.1364/PRJ.406123. URL `https://opg.optica.org/prj/abstract.cfm?URI=prj-9-2-222`.

[124] Guo-Wei Zhang, Yu-Yang Ding, Wei Chen, Fang-Xiang Wang, Peng Ye, Guan-Zhong Huang, Shuang Wang, Zhen-Qiang Yin, Jun-Ming An, Guang-Can Guo, and Zheng-Fu Han. Polarization-insensitive interferometer based on a hybrid integrated planar lightwave circuit. *Photon. Res.*, 9(11):2176–2181, Nov 2021. doi: 10.1364/PRJ.432327. URL `https://opg.optica.org/prj/abstract.cfm?URI=prj-9-11-2176`.

[125] Giacomo Corrielli, Simone Atzeni, Simone Piacentini, Ioannis Pitsios, Andrea Crespi, and Roberto Osellame. Symmetric polarization-insensitive directional couplers fabricated by femtosecond laser writing. *Opt. Express*, 26(12):15101–15109, Jun 2018. doi: 10.1364/OE.26.015101. URL `https://opg.optica.org/oe/abstract.cfm?URI=oe-26-12-15101`.

[126] Luís A. Fernandes, Jason R. Grenier, Peter R. Herman, J. Stewart Aitchison, and Paulo V. S. Marques. Stress induced birefringence tuning in femtosecond laser fabricated waveguides in fused silica. *Opt. Express*, 20(22):24103–24114, Oct 2012. doi: 10.1364/OE.20.024103. URL `https://opg.optica.org/oe/abstract.cfm?URI=oe-20-22-24103`.

[127] Riccardo Albiero, Ciro Pentangelo, Marco Gardina, Simone Atzeni, Francesco Ceccarelli, and Roberto Osellame. Toward higher integration density in femtosecond-laser-written programmable photonic circuits. *Micromachines*, 13(7), 2022. ISSN 2072-666X. doi: 10.3390/mi13071145. URL `https://www.mdpi.com/2072-666X/13/7/1145`.

[128] Philip Sibson, Jake E. Kennard, Stasja Stanisic, Chris Erven, Jeremy L. O'Brien, and Mark G. Thompson. Integrated silicon photonics for high-speed quantum key distribution. *Optica*, 4(2):172, January 2017. doi: 10.1364/optica.4.000172. URL `https://doi.org/10.1364/optica.4.000172`.

[129] Chaoxuan Ma, Wesley D. Sacher, Zhiyuan Tang, Jared C. Mikkelsen, Yisu Yang, Feihu Xu, Torrey Thiessen, Hoi-Kwong Lo, and Joyce K. S. Poon. Silicon photonic transmitter for polarization-encoded quantum key distribution. *Optica*, 3(11):1274–1278, Nov 2016. doi: 10.1364/OPTICA.3.001274. URL `http://opg.optica.org/optica/abstract.cfm?URI=optica-3-11-1274`.

[130] Darius Bunandar, Anthony Lentine, Catherine Lee, Hong Cai, Christopher M. Long, Nicholas Boynton, Nicholas Martinez, Christopher DeRose, Changchen Chen, Matthew Grein, Douglas Trotter, Andrew Starbuck, Andrew Pomerene, Scott Hamilton, Franco N. C. Wong, Ryan Camacho, Paul Davids, Junji Urayama, and Dirk Englund. Metropolitan quantum key distribution with silicon photonics. *Phys. Rev. X*, 8:021009, Apr 2018. doi: 10.1103/PhysRevX.8.021009. URL `https://link.aps.org/doi/10.1103/PhysRevX.8.021009`.

[131] Wei Geng, Chao Zhang, Yu Zheng, Jiankun He, Cheng Zhou, and Yunchuan Kong. Stable quantum key distribution using a silicon photonic transceiver. *Optics express*, 27 20:29045–29054, 2019.

[132] Lingwen Kong, Zhihao Li, Congxiu Li, Lin Cao, Zeyu Xing, Junqin Cao, Yaxin Wang,

Xinlun Cai, and Xiaoqi Zhou. Photonic integrated quantum key distribution receiver for multiple users. *Opt. Express*, 28(12):18449–18455, Jun 2020. doi: 10.1364/OE.394050. URL `http://opg.optica.org/oe/abstract.cfm?URI=oe-28-12-18449`.

[133] Chen-Xi Zhu, Zhao-Yuan Chen, Yang Li, Xin-Zhe Wang, Chao-Ze Wang, Yu-Long Zhu, Fu-Tian Liang, Wen-Qi Cai, Ge Jin, Sheng-Kai Liao, and Cheng-Zhi Peng. Experimental quantum key distribution with integrated silicon photonics and electronics. *Phys. Rev. Appl.*, 17:064034, Jun 2022. doi: 10.1103/PhysRevApplied.17.064034. URL `https://link.aps.org/doi/10.1103/PhysRevApplied.17.064034`.

[134] Gong Zhang, Jing Yan Haw, Hong Cai, Feng Xu, SM Assad, Joseph F Fitzsimons, Xianzhong Zhou, Y Zhang, S Yu, J Wu, et al. An integrated silicon photonic chip platform for continuous-variable quantum key distribution. *Nature Photonics*, 13(12):839–842, 2019.

[135] Lang Li, Tao Wang, Xinhang Li, Peng Huang, Yuyao Guo, Liangjun Lu, Linjie Zhou, and Guihua Zeng. Continuous-variable quantum key distribution with on-chip light sources. *Photon. Res.*, 11(4):504–516, Apr 2023. doi: 10.1364/PRJ.473328. URL `https://opg.optica.org/prj/abstract.cfm?URI=prj-11-4-504`.

[136] J. Aldama, S. Sarmiento, S. Etcheverry, I. López Grande, L. Trigo Vidarte, L. Castelvero, A. Hinojosa, T. Beckerwerth, Y. Piétri, A. Rhouni, E. Diamanti, and V. Pruneri. InP-based CV-QKD PIC transmitter. In *Optical Fiber Communication Conference (OFC) 2023*, page M1I.3. Optica Publishing Group, 2023. doi: 10.1364/OFC.2023.M1I.3. URL `https://opg.optica.org/abstract.cfm?URI=OFC-2023-M1I.3`.

[137] Yoann Piétri, Luis Trigo Vidarte, Matteo Schiavon, Philippe Grangier, Amine Rhouni, and Eleni Diamanti. CV-QKD receiver platform based on a silicon photonic integrated circuit. In *2023 Optical Fiber Communications Conference and Exhibition (OFC)*, pages 1–3, 2023. doi: 10.1364/OFC.2023.M1I.2.

[138] Y. Shen, L. Cao, X. Y. Wang, J. Zou, W. Luo, Y. X. Wang, H. Cai, B. Dong, X. S. Luo, W. J. Fan, L. C. Kwek, and A. Q. Liu. On-chip continuous-variable quantum key distribution (CV-QKD) and homodyne detection. In *2020 Optical Fiber Communications Conference and Exhibition (OFC)*, pages 1–3, 2020.

[139] Kejin Wei, Wei Li, Hao Tan, Yang Li, Hao Min, Wei-Jun Zhang, Hao Li, Lixing You, Zhen Wang, Xiao Jiang, Teng-Yun Chen, Sheng-Kai Liao, Cheng-Zhi Peng, Feihu Xu, and Jian-Wei Pan. High-speed measurement-device-independent quantum key distribution with integrated silicon photonics. *Phys. Rev. X*, 10:031030, Aug 2020. doi: 10.1103/PhysRevX.10.031030. URL `https://link.aps.org/doi/10.1103/PhysRevX.10.031030`.

[140] Ci-Yu Wang, Jun Gao, Zhi-Qiang Jiao, Lu-Feng Qiao, Ruo-Jing Ren, Zhen Feng, Yuan Chen, Zeng-Quan Yan, Yao Wang, Hao Tang, and Xian-Min Jin. Integrated measurement server for measurement-device-independent quantum key distribution network. *Opt. Express*, 27(5):5982–5989, Mar 2019. doi: 10.1364/OE.27.005982. URL `https://opg.optica.org/oe/abstract.cfm?URI=oe-27-5-5982`.

[141] L. Cao, W. Luo, Y.X. Wang, J. Zou, R.D. Yan, H. Cai, Y. Zhang, X.L. Hu, C. Jiang, W.J. Fan, X.Q. Zhou, B. Dong, X.S. Luo, G.Q. Lo, Y.X. Wang, Z.W. Xu, S.H. Sun, X.B. Wang, Y.L. Hao, Y.F. Jin, D.L. Kwong, L.C. Kwek, and A.Q. Liu. Chip-based measurement-device-independent quantum key distribution using integrated silicon photonic systems.

Phys. Rev. Appl., 14:011001, Jul 2020. doi: 10.1103/PhysRevApplied.14.011001. URL https://link.aps.org/doi/10.1103/PhysRevApplied.14.011001.

[142] M Avesani, L Calderaro, M Schiavon, A Stanco, C Agnesi, A Santamato, M Zahidy, A Scriminich, G Foletto, G Contestabile, et al. Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics. *npj Quantum Information*, 7(1):93, 2021.

[143] Xiaodong Zheng, Peiyu Zhang, Renyou Ge, Liangliang Lu, Guanglong He, Qi Chen, Fangchao Qu, LaBao Zhang, Xinlun Cai, Yanqing Lu, Shining N. Zhu, Peiheng Wu, and Xiaosong Ma. Heterogeneously integrated, superconducting silicon-photonic platform for measurement-device-independent quantum key distribution. *Advanced Photonics*, 3(5): 055002, 2021. doi: 10.1117/1.AP.3.5.055002. URL https://doi.org/10.1117/1.AP.3.5.055002.

[144] Wolfgang Killmann and Werner Schindler. A proposal for: Functionality classes for random number generators. *ser. BDI, Bonn*, 2011.

[145] Derrick H. Lehmer. Mathematical methods in large-scale computing units. *Proceedings of 2nd Symposium on Large-Scale Digital Calculating Machinery*, (141–146), 1951.

[146] L. Blum, M. Blum, and M. Shub. A simple unpredictable pseudo-random number generator. *SIAM Journal on Computing*, 15(2):364–383, 1986. doi: 10.1137/0215025. URL https://doi.org/10.1137/0215025.

[147] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, et al. *A statistical test suite for random and pseudorandom number generators for cryptographic applications*, volume 22. US Department of Commerce, Technology Administration, National Institute of Standards and Technology, 2001.

[148] George Marsaglia. Diehard: a battery of tests of randomness. *http://stat. fsu. edu/geo*, 1996.

[149] Hai-Qiang Ma, Yuejian Xie, and Ling-An Wu. Random number generation based on the time of arrival of single photons. *Appl. Opt.*, 44(36):7760–7763, Dec 2005. doi: 10.1364/AO.44.007760. URL https://opg.optica.org/ao/abstract.cfm?URI=ao-44-36-7760.

[150] Ma Hai-Qiang, Wang Su-Mei, Zhang Da, Chang Jun-Tao, Ji Ling-Ling, Hou Yan-Xue, and Wu Ling-An. A random number generator based on quantum entangled photon pairs. *Chinese Physics Letters*, 21(10):1961, oct 2004. doi: 10.1088/0256-307X/21/10/027. URL https://dx.doi.org/10.1088/0256-307X/21/10/027.

[151] P. X. Wang, G. L. Long, and Y. S. Li. Scheme for a quantum random number generator. *Journal of Applied Physics*, 100(5):056107, 09 2006. ISSN 0021-8979. doi: 10.1063/1.2338830. URL https://doi.org/10.1063/1.2338830.

[152] Christian Gabriel, Christoffer Wittmann, Denis Sych, Ruifang Dong, Wolfgang Mauerer, Ulrik L Andersen, Christoph Marquardt, and Gerd Leuchs. A generator for unique quantum random numbers based on vacuum states. *Nature Photonics*, 4(10):711–715, 2010.

[153] C Abellán, Waldimar Amaya, M Jofre, M Curty, A Acín, Jose Capmany, Valerio Pruneri, and Morgan W Mitchell. Ultra-fast quantum randomness generation by accelerated phase

diffusion in a pulsed laser diode. *Optics express*, 22(2):1645–1654, 2014.

[154] Bing Qi, Yue-Meng Chi, Hoi-Kwong Lo, and Li Qian. High-speed quantum random number generation by measuring phase noise of a single-mode laser. *Opt. Lett.*, 35(3):312–314, Feb 2010. doi: 10.1364/OL.35.000312. URL `https://opg.optica.org/ol/abstract.cfm?URI=ol-35-3-312`.

[155] Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin. Quantum random number generators. *Reviews of Modern Physics*, 89(1):015004, 2017.

[156] Stefano Pironio, Antonio Acín, Serge Massar, A Boyer de La Giroday, Dzmitry N Matsukevich, Peter Maunz, Steven Olmschenk, David Hayes, Le Luo, T Andrew Manning, et al. Random numbers certified by Bell's theorem. *Nature*, 464(7291):1021–1024, 2010.

[157] B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, and P. G. Kwiat. Detection-loophole-free test of quantum nonlocality, and applications. *Phys. Rev. Lett.*, 111:130406, Sep 2013. doi: 10.1103/PhysRevLett.111.130406. URL `https://link.aps.org/doi/10.1103/PhysRevLett.111.130406`.

[158] Peter Bierhorst, Emanuel Knill, Scott Glancy, Yanbao Zhang, Alan Mink, Stephen Jordan, Andrea Rommal, Yi-Kai Liu, Bradley Christensen, Sae Woo Nam, et al. Experimentally generated randomness certified by the impossibility of superluminal signals. *Nature*, 556 (7700):223–226, 2018.

[159] Yang Liu, Qi Zhao, Ming-Han Li, Jian-Yu Guan, Yanbao Zhang, Bing Bai, Weijun Zhang, Wen-Zhao Liu, Cheng Wu, Xiao Yuan, et al. Device-independent quantum random-number generation. *Nature*, 562(7728):548–551, 2018.

[160] David P. Nadlinger, Peter Drmota, Bethan C. Nichol, Gabriel Araneda, Dougal Main, Raghavendra Srinivas, David M Lucas, Christopher J. Ballance, Kirill Ivanov, EY-Z Tan, et al. Experimental quantum key distribution certified by bell's theorem. *Nature*, 607 (7920):682–686, 2022.

[161] Hong-Wei Li, Zhen-Qiang Yin, Yu-Chun Wu, Xu-Bo Zou, Shuang Wang, Wei Chen, Guang-Can Guo, and Zheng-Fu Han. Semi-device-independent random-number expansion without entanglement. *Phys. Rev. A*, 84:034301, Sep 2011. doi: 10.1103/PhysRevA.84.034301. URL `https://link.aps.org/doi/10.1103/PhysRevA.84.034301`.

[162] Tommaso Lunghi, Jonatan Bohr Brask, Charles Ci Wen Lim, Quentin Lavigne, Joseph Bowles, Anthony Martin, Hugo Zbinden, and Nicolas Brunner. Self-testing quantum random number generator. *Phys. Rev. Lett.*, 114:150501, Apr 2015. doi: 10.1103/PhysRevLett.114.150501. URL `https://link.aps.org/doi/10.1103/PhysRevLett.114.150501`.

[163] Davide G. Marangon, Giuseppe Vallone, and Paolo Villoresi. Source-device-independent ultrafast quantum random number generation. *Phys. Rev. Lett.*, 118:060503, Feb 2017. doi: 10.1103/PhysRevLett.118.060503. URL `https://link.aps.org/doi/10.1103/PhysRevLett.118.060503`.

[164] Jonatan Bohr Brask, Anthony Martin, William Esposito, Raphael Houlmann, Joseph Bowles, Hugo Zbinden, and Nicolas Brunner. Megahertz-rate semi-device-independent

quantum random number generators based on unambiguous state discrimination. *Phys. Rev. Appl.*, 7:054018, May 2017. doi: 10.1103/PhysRevApplied.7.054018. URL https://link.aps.org/doi/10.1103/PhysRevApplied.7.054018.

[165] Davide Rusca, Thomas van Himbeeck, Anthony Martin, Jonatan Bohr Brask, Weixu Shi, Stefano Pironio, Nicolas Brunner, and Hugo Zbinden. Self-testing quantum random-number generator based on an energy bound. *Phys. Rev. A*, 100:062338, Dec 2019. doi: 10.1103/PhysRevA.100.062338. URL https://link.aps.org/doi/10.1103/PhysRevA.100.062338.

[166] Thomas van Himbeeck. *Quantum Cryptography with Partially Trusted Devices*. PhD thesis, Université libre de Bruxelles, Université libre de Bruxelles, 2019.

[167] Xiongfeng Ma, Feihu Xu, He Xu, Xiaoqing Tan, Bing Qi, and Hoi-Kwong Lo. Post-processing for quantum random-number generators: Entropy evaluation and randomness extraction. *Phys. Rev. A*, 87:062327, Jun 2013. doi: 10.1103/PhysRevA.87.062327. URL https://link.aps.org/doi/10.1103/PhysRevA.87.062327.

[168] Carlos Abellan, Waldimar Amaya, David Domenech, Pascual Mu noz, Jose Capmany, Stefano Longhi, Morgan W. Mitchell, and Valerio Pruneri. Quantum entropy source on an InP photonic integrated circuit for random number generation. *Optica*, 3(9):989–994, Sep 2016. doi: 10.1364/OPTICA.3.000989. URL https://opg.optica.org/optica/abstract.cfm?URI=optica-3-9-989.

[169] Francesco Raffaelli, Philip Sibson, Jake E. Kennard, Dylan H. Mahler, Mark G. Thompson, and Jonathan C. F. Matthews. Generation of random numbers by measuring phase fluctuations from a laser diode with a silicon-on-insulator chip. *Opt. Express*, 26(16): 19730–19741, Aug 2018. doi: 10.1364/OE.26.019730. URL https://opg.optica.org/oe/abstract.cfm?URI=oe-26-16-19730.

[170] Francesco Raffaelli, Giacomo Ferranti, Dylan H Mahler, Philip Sibson, Jake E Kennard, Alberto Santamato, Gary Sinclair, Damien Bonneau, Mark G Thompson, and Jonathan C F Matthews. A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers. *Quantum Science and Technology*, 3(2): 025003, feb 2018. doi: 10.1088/2058-9565/aaa38f. URL https://dx.doi.org/10.1088/2058-9565/aaa38f.

[171] Tommaso Bertapelle, Marco Avesani, Alberto Santamato, Alberto Montanaro, Marco Chiesa, Davide Rotta, Massimo Artiglia, Vito Sorianello, Francesco Testa, Gabriele De Angelis, Giampiero Contestabile, Giuseppe Vallone, Marco Romagnoli, and Paolo Villoresi. High-speed source-device-independent quantum random number generator on a chip, 2023.

[172] A. V. Masalov, A. Kuzhamuratov, and A. I. Lvovsky. Noise spectra in balanced optical detectors based on transimpedance amplifiers. *Review of Scientific Instruments*, 88(11): 113109, 11 2017.

[173] Xiaoxiong Zhang, Yichen Zhang, Zhengyu Li, Song Yu, and Hong Guo. 1.2-GHz balanced homodyne detector for continuous-variable quantum information technology. *IEEE Photonics Journal*, 10(5):1–10, 2018.

[174] Ruiqi Liu, Georgi Gary Rozenman, Neel Kanth Kundu, Daryus Chandra, and Debashis

De. Towards the industrialisation of quantum key distribution in communication networks: A short survey. *IET Quantum Communication*, 3(3):151–163, 2022.

[175] United Nations (General Assembly). International covenant on economic, social, and cultural rights. *Treaty Series*, 999:171, December 1966.

Acknowledgements

I have an endless number of thank yous to do to so many people that I have met, that have been present, who have influenced, encouraged and supported me these last four years. Since this final section is finite, certain expressions of gratitude will be carried out in person rather than written down here. To these people, you are well aware of my sincerest appreciation.

Firstly, I express my deepest gratitude to my supervisor, Hugo Zbinden, for letting me work in his group and for introducing me to the wonderful world at GAP, both in terms of research and camaraderie. I thank you Hugo for always having been available for a chat in your office, it be work-related or not.

I would also like to extend my deepest gratitude to Alberto Boaron, my colleague, supervisor and friend throughout my thesis. Thank you Alberto for always, without any exception, having been there to reply to my questions and help me solve experimental difficulties in the laboratory. I could not have dreamt of a better supervisor to work with. A huge thank you for taking your time to proof-read my thesis, even though you no longer work at the University.

My sincerest thanks go to the rest of the QKD team. Thank you Fadri Grünenfelder for teaching me how to work hard and for your constant support whenever needed. A special thanks to you for maintaining and debugging our code. Thank you Davide Rusca for, without exception, having had a reply to a question I had about our protocol, experiment or else, it be QKD/QRNG related or not, and for taking your time to explain the answer in a pedagogical way. Thank you Maria Pereira for your patience and support these last months and for proof-reading my thesis. Thank you for replying to all my detector-related questions, even though I keep on asking the same things. I very much appreciated all the delicious sweets you brought to the office, thank you! I also want to thank Raphaël Houlmann, our FPGA engineer, for preparing and maintaining the FPGAs we work with, for being there whenever problems need solving and for being a fun office mate.

The well-going of my various projects would not have been possible without the constant support of our electronics engineer Claudio Barreiro. Thank you for being there for me when I needed help, for your enthusiasm, energy and for coming back and helping us even though you are retired. Special thanks goes to our new electronics engineer, David Cabrerizo Pastor, who prepared the electronics for the QRNG project. Thank you for your kindness and for being available to help.

I am also grateful to our group leader Rob Thew, whom I have always appreciated to be around. Thank you for being kind, calm and always available for chats, work-wise or not. I looking forward to continue working with you.

I would also like to wholeheartedly thank all my colleagues (current and former) and friends at GAP, within and outside of our group. Thank you for all your support these last months, re-reading sections of my thesis, taking care of me when I was stressed and listening to my trial presentation over and over again. A huge thanks for your general presence in my life these

last years. I loved spending time with you all, it be having a beer, skiing, climbing, going on conferences, taking a coffee or simply hanging out.

Special thanks to Lorenzo for always being available to chat and have a coffee, to Giovanni for always being good company and for helping me with the bondings of my chip and to Patrik who I very much appreciated discussing with around the coffee machine or at La Dôle at night. Special thanks should also go to Moritz, whom I enjoyed doing sports with, Tiff for being always a calm presence ready to give a hug if I needed one and Dmitry for fun conversations and useful climbing tips. Many thanks for fun discussions and for creating a lovely atmosphere should also go to current and former colleagues (in no particular order) Evi, Theo, Adrian, Joey, Alberto R., Towsif, Georgios, Matthieu, Antonio, Alexandre, Louis, Jinging, Pavel, Roope, Sophie, Farid, Nicolas and Emna.

Importance and huge appreciation also goes to the incredibly crucial members of GAP, Isabel and Corinne. Thank you for always being availble to help when needed (which happened often). I also want to thank Michel for his presence. I always had fun talking with you. Many thanks for all your help, it be moving-related or (non-)technical.

I also want to thank other members of GAP for keeping the ambience and spirits up! Special thanks go to Geraldine, whom I had the chance to work with in Physique Générale, Nicolas, for supporting and sharing contacts with me for my future in education and to Mikael, my fellow Swedish friend! I always appreciated our chats in swedish.

I am also greatful for the collaboration I had with Sicoya. Thank you for providing a great Alice. Special thanks to Hanjo, Danilo and Sebastian, who were all available when I had questions, even during the writing of this thesis, when the project was over. I am also in debt to our colleagues in Milano who furished an outstanding Bob. Special thanks to Roberto, Simone and Giulio, who were always available for a call, fun to chat with and ready to answer any questions I had. Many thanks goes also to Martin and Moritz from HHI Fraunhofer for providing and helping us with our QRNG chips. Thanks should also go to Gabriel Pelleriti for his help, countless times now, fixing and repairing bondings. I also thank Gianluca Boso for his kind and calm presence. Thank you, especially, for helping me settle in to the project. I am glad you, and Alberto, come by from time to time to continue working in our lab.

Thanks to the teams of Physique Générale, which I had the chance to take part of, especially the leaders Anna Sfyrla and Luigi Bonacina, for a warm collaboration. I particularly enjoyed trying new methods of teaching. Thanks also to the team at Physicsope for a friendly collaboration, particularly to Olivier and Céline L. for their support regarding the shows, my thesis and even my future adventures. Thanks also to Miguel and Céline C. for preparing our amazing shows and for repairing the various objects I broke.

I also want to thank Sandro D'Aléo for nice chats and for lending me amazing material for parties at GAP (even though there was a lot of smoke exiting the smoke machine and the lasers were probably too powerful to be legal nowadays) and Nathalie Chaudrion for having been present at the physics section since my very first day in 2014. Thank you for always being positive and caring.

The four years wouldn't have passed so fast nor were so fun without my friend and former colleague, Marie. I loved our lunch runs and I am happy that you live close by so we can continue that tradition. Thank you for being such an honest and loyal friend and the most profound thanks to you for re-reading my thesis a countless amounts of times.

I also want to thank my friends from physics, but outside of GAP, Julien, Yannick and Nicolas whom I had the chance to study my Master with. I will not forget our study sessions, laboratory adventures and other moments. I am glad we still meet. Thanks also to other physics friends: Hugo, Theo, David and Killian for being supportive and interested in what I have been doing these last years.

I am extremely grateful for my (non-physics) friends. Thank you for accepting me as I am, even though you think I am a crazy scientist. Thank you for listening to me and being there for me when I needed it the most. This thank you list is non-exhaustive and in no particular order. Thanks to Heather (for early coffees), Charlotte (for even earlier runs), Sofia (for late beers and dinners) and Romane (for ski and boat adventures). I want to extend my gratitude to Giulia, Claire, Noémie, Béa, Sara, Viktoria, Maggie, Steph, Carmelo, Raph, Andrea, Yuri, Ale, Stefano, Lucas and Antoine for their constant support, presence, and kindness.

My deepest gratitude goes also too my friends in Sweden, Matilda, Klara, Amanda and Lea, who are always there when I come or ready to pick up their phone if I call. Your support and belief in me during my PhD has been priceless.

Mes remerciements vont aussi à ma famille suisse, Marie-Françoise, Bernard, Amandine et Coralie. Merci pour les repas, les intentions, les messages, l'aide quand j'en avais besoin et votre soutien pendant ma thèse. Merci de m'avoir acceuilli, les bras ouverts, chez vous.

I am in huge debt to my entire family (Sax, Björkdahl, Wallin, Naudo, Bergman) for always and unconditionally believing in me. Thank you for coming all the way to Geneva for proving this point! Thank you for your kind messages and being interested in what I do, even though it is not your passion. I would also like to thank my Mormor and Morfar from the deepest of my heart for their endless support with whatever I take on.

Special thanks goes to my brother David, his partner Johanna and my cousin Pierre. Thank you for your care, encouragements and craziness and for always picking up the phone whenever I need to laugh or talk.

Coming towards the end of my gratitudes, one of the most significant ones is directed towards Coco (Corentin). Thank you for having stood out with me these last years, for having motivated me when I needed it, brought food to my office when I wanted to stay and cooked when I came home late. Thank you for having listened to me when I needed to discuss a problem in the lab. I am incredibly grateful that you have been an unconditional presence, which I (try to) never take for granted.

Finally, none of this would be possible without the unlimited and eternal support from my parents Sessan (Cecilia) and Tulle (Karl-Erik). Thank you for showing me how to work hard and also how to relax and have fun. Thank you for letting me arrive on my own in Geneva when I was 18 and for encouraging me to, at least, give the physics course there a try. If I didn't like it, then I was more than welcome home (back to Sweden). Thank you for having had the courage to settle down in various places (and continents) with young kids. I would not be the person I am today without our memorable experiences.

To each and every individual mentioned and those not named but equally instrumental throughout this endeavor – my sincerest and most profound thanks.

Rebecka Sax