High-dimensional quantum key distribution with time-phase encoding

Adam Widomski

A thesis submitted for the degree of Doctor of Philosophy

Optics Division
Institute of Experimental Physics
Faculty of Physics
University of Warsaw

Supervised by:
prof. dr hab. Czesław Radzewicz
dr Michał Karpiński

Warsaw, 2025

I dedicate this thesis to my beloved wife Patrycja.

Abstract

The time-phase encoding has emerged as a promising tool for quantum information technology. Modulating time and phase of quantum light enables generating qubits, or high-dimensional quantum states which can be further used for noise-resilient quantum technologies. Among quantum communication techniques, quantum key distribution (QKD) stands out as a leading solution to address the growing demand for secure communication systems in the face of potential threats posed by quantum computing advancements.

Current QKD systems based on qubit encoding have been widely demonstrated, particularly with time-phase and polarization degrees of freedom. Time-phase encoding is particularly attractive due to its compatibility with telecom infrastructure, robustness to polarization drift, and potential for efficient, high-speed implementations. In this work, I investigate the benefits of extending time-phase QKD toward high-dimensional encoding to further enhance noise tolerance and key generation efficiency.

The overall goal of this thesis is the construction of a quantum key distribution (QKD) link using time-phase encoding. I developed a system capable of transmitting and detecting high-dimensional quantum symbols, allowing encoding multiple bits of information per photon. The main achievement is the experimental demonstration of the advantages provided by high-dimensional encoding, along with a theoretical analysis comparing the impacts of imbalanced measurement probabilities between key-generation and control bases.

Initially, I investigated the potential of photonic integrated circuits (PICs) for generating optical communication symbols. I characterized the properties of on-chip components, verifying their performance and key parameters. Using integrated modulators, I generated optical pulses with tailored temporal and spectral properties. I experimentally validated the parameters through time-to-frequency mapping and time-correlated single-photon counting techniques. These results demonstrate the feasibility of using generic indium phosphide PIC platforms for applications in QKD.

Subsequently, I proposed a novel detection method for detecting high-dimensional time-bin quantum superpositions based on the temporal Talbot effect—a time-domain counterpart of the well-known near-field diffraction self-imaging phenomenon. By carefully tuning the temporal parameters and dispersion properties, I achieved frequency-to-time mapping with substantially lower dispersion requirements compared to the standard approach. Additionally, I analyzed the effects of post-selection strategies and timing noise on the correct discrimination of quantum superpositions.

The primary achievement of this thesis is the experimental demonstration of QKD using two- and four-dimensional quantum superpositions, detected through a newly introduced method based on the temporal Talbot effect. I performed controlled laboratory tests and extended the validation to the fiber-optic infrastructure at the University of Warsaw. Through these experiments, I demonstrated that high-dimensional encoding enhances noise resilience and increases information entropy per detection event. I analyzed the experimental results using two differ-

ent security models—both accounting for and neglecting detection efficiency imbalances—and observed significant differences in the achievable key rates. The findings pave the way for the development of secure QKD systems based on both high-dimensional states and traditional qubits. Further theoretical refinements could improve the modeling of QKD systems, particularly under finite-key conditions.

Streszczenie

Kodowanie czasowo-fazowe pojawiło się jako obiecujące narzędzie dla technologii informacji kwantowej. Modulowanie czasu i fazy światła kwantowego pozwala generować kubity oraz wielkowymiarowe stany kwantowe, które umożliwiają implementację technologii kwantowych o zwiększonej odporności na szum. Jedną z najbardziej pożądanych technologii komunikacji kwantowej jest kwantowa dystrybucja klucza (QKD). QKD wyłoniła się jako wiodące rozwiązanie, aby sprostać rosnącemu zapotrzebowaniu na bezpieczne systemy komunikacyjne w obliczu potencjalnych zagrożeń związanych z rozwojem komputerów kwantowych.

Obecne systemy QKD oparte na kubitach zostały szeroko zademonstrowane, szczególnie z wykorzystaniem czasowo-fazowego oraz polaryzacyjnego stopnia swobody. Kodowanie czasowo-fazowe jest szczególnie atrakcyjne ze względu na kompatybilność z istniejącą infrastrukturą telekomunikacyjną, odporność na dryf polaryzacji oraz możliwość wydajnej i szybkiej implementacji. W niniejszej pracy badam korzyści wynikające z rozszerzenia kodowania czasowo-fazowego w QKD na stany o wysokiej wymiarowości w celu dalszego zwiększenia tolerancji na szumy oraz poprawy efektywności generowania kluczy.

Głównym celem pracy jest budowa systemu QKD wykorzystującego kodowanie czasowo-fazowe. Opracowałem system umożliwiający transmisję i detekcję kwantowych symboli o wysokiej wymiarowości, pozwalający na kodowanie wielu bitów informacji w pojedynczym fotonie. Głównym osiągnięciem jest eksperymentalna demonstracja zalet wysokowymiarowego kodowania, poparta teoretyczną analizą porównującą wpływ niezrównoważonych prawdopodobieństw pomiaru między bazą generacji klucza i bazą kontrolną.

W pierwszej częsci pracy oceniłem potencjał fotonicznych układów scalonych (PIC) do generowania symboli, które mogłyby być wykorzystywane w komunikacji kwantowej. Zbadałem właściwości kompoentnów umieszczonych na chipie celem sprawdzenia poprawności wykonania oraz zbadania kluczowych parametrów. Wykorzystałem zintegrowane modulatory na chipie do generacji impulsów optycznych o pożądanych właściwościach czasowo widmowych. Zweryfikowałem wyniki za pomocą przybliżonego mapowania czasu na widmo zrealizowanego za pomocą ośrodka dyspersyjnego i techniki dyspersyjnego przekształcenia Fouriera i czasowo-skorelowanego zliczania pojedynczych fotonów. Uzyskane wyniki potwierdzają możliwość zastosowania generycznych platform PIC opartych na fosforku indu na poczet QKD.

Następnie zaproponowałem nową metodę detekcji wysokowymiarowych czasowych superpozycji kwantowych, opartą na efekcie Talbota w dziedzinie czasu — odpowiedniku dobrze znanego efektu samoobrazowania obiektów periodycznych związanego z dyfrakcją w strefie bliskiego pola. Dzięki precyzyjnemu dostrojeniu parametrów czasowych oraz własności dyspersyjnych osiągnąłem mapowanie częstotliwość-czas przy znacznie niższych wymaganiach dotyczących dyspersji w porównaniu do standardowych metod. Dodatkowo przeanalizowałem wpływ strategii post-selekcji oraz szumu czasowego na poprawność rozróżniania kwantowych superpozycji.

Najważniejszym osiągnięciem niniejszej pracy jest eksperymentalna demonstracja QKD z wykorzystaniem dwuwymiarowych i czterowymiarowych superpozycji kwantowych, wykrywanych

za pomocą nowo wprowadzonej metody opartej na efekcie Talbota w dziedzinie czasu. Przeprowadziłem kontrolowane testy laboratoryjne oraz rozszerzyłem walidację systemu o pomiary z wykorzystaniem infrastruktury światłowodowej Uniwersytetu Warszawskiego. W trakcie badań wykazałem, że kodowanie wysokowymiarowe zwiększa odporność na szumy oraz podnosi entropię informacji przypadającą na pojedyncze zdarzenie detekcji. Wyniki eksperymentalne zostały przeanalizowane w oparciu o dwa różne modele bezpieczeństwa — zarówno uwzględniające, jak i pomijające niezrównoważoną wydajność detekcji — ujawniając istotne różnice w osiągalnych wartościach informacyjnych generowanych kluczy. Uzyskane wyniki otwierają drogę do budowy bezpiecznych systemów QKD opartych zarówno na stanach wysokowymiarowych, jak i na kubitach. Dalsze analizy teoretyczne mogą poprawić dokładność modelowania systemów QKD, w szczególności w scenariuszach ograniczonej skończonej kluczy kryptograficznych.

Acknowledgements

My journey toward completing this dissertation has been a challenging yet transformative experience, profoundly shaping my personal and professional development. I would like to take a moment to reflect on and express my gratitude to the people who have been part of this journey.

First and foremost, I would like to express my deepest gratitude to my supervisor, dr Michał Karpiński. Pursuing a PhD was not something I had originally considered, but you encouraged me to join the Quantum Photonics Laboratory at the University of Warsaw for my Master's studies and later to embark on the PhD program. Throughout this time, your mentorship and guidance have been invaluable, from my first steps in research to the final stages of this work. You broadened my horizons and introduced me to the rich and complex world of academia. For that, I am truly grateful.

I would also like to extend my thanks to prof. dr hab. Czesław Radzewicz and to you, Michał, for giving me the opportunity to work on the National Laboratory for Photonic Quantum Technologies project. It was a unique and invaluable experience that allowed me to engage in the deployment of quantum key distribution systems. My gratitude also goes to Piotr Rydlichowski from the Poznań Supercomputing and Networking Center and Paweł Celmer from the IT department at the University of Warsaw. Running the final QKD experiments and preparing the infrastructure for deployment required continuous adjustments and problem-solving, and you made it possible.

A part of this thesis is related to photonic integrated circuits, a field I was able to explore thanks to the European design hub at the Warsaw University of Technology. I sincerely appreciate the support of dr hab. inż Ryszard Piramidowicz and dr inż. Stanisław Stopiński for their openness to project proposals and for sharing their outstanding expertise in photonic integration.

Many enriching experiences, workshops, and initiatives were made possible through the Optica-SPIE-EPS-IEEE student chapter – Koło Naukowe Optyki i Fotoniki (KNOF). Special thanks go to Piotr Węgrzyn, who first inspired me to become an active member and later encouraged me to take on a leadership role. The experience gained through KNOF ultimately led Piotr, Mihai Suster, and me to establish the Candela Foundation, dedicated to supporting the photonics community beyond what a student association could offer. Being part of Candela alongside you has been an incredible journey. Thank you for the great memories and the shared satisfaction of having a real impact on the community. The scale and reach of Candela's projects have far exceeded anything I had initially imagined, and I am excited that this story continues.

I would like to appreciate the company of my lab colleagues – Ali Golestani, Michał Mikołajczyk, Sanjay Kapoor, Maciej Ogrodnik, Jerzy Szuniewicz, and Filip Sośnicki. It was a pleasure to be part of the team. In particular I would like to thank you Maciej for the time we spend on measurements and discussing theoretical aspects of quantum technologies.

Final words of appreciation I direct to my family. Your support and understanding helped me to go beyond my own limits.

Contents

Chapter 1

Motivation

The modern world is driven by vast amounts of data, much of which must remain confidential and be delivered precisely to its intended recipient. Every day, personal and financial information, industrial secrets, medical diagnoses, and administrative decisions are exchanged between multiple parties. The security of our current infrastructure relies on encryption, which uses mathematical properties of numbers to secure information. We assume that encrypted data remains confidential until it reaches its destination. However, this assumption may change with the advent of quantum computing.

Many widely used encryption standards are vulnerable to quantum attacks. Even more concerning is the potential strategy of 'download now, decrypt later', where hackers store encrypted data until they acquire sufficient quantum resources to break it. This approach is especially dangerous for long-term sensitive information, such as archived data. To counter future privacy breaches, researchers have developed post-quantum encryption algorithms. However, these methods are not yet widely adopted, and most of today's infrastructure still relies on conventional encryption techniques. Theoretically, one of the encryption methods—known as the Vernam cipher—remains secure against quantum attacks. It operates using a one-time pad, where each bit of the message is encrypted with a corresponding bit of a secret key. The same key is required for both encryption and decryption, making key exchange a critical challenge. This is where quantum key distribution (QKD) comes in. QKD enables secure key exchange using the principles of quantum mechanics. Instead of relying solely on mathematical encryption strength, QKD detects potential eavesdropping through the laws of physics. If an interception attempt is detected, the key is discarded, preventing any risk of data exposure.

Optical fiber communication is the backbone of modern data transmission due to its low signal loss and high resistance to electromagnetic interference and environmental factors. Additionally, fiber-optic cables can be mass-produced at a relatively low cost. However, the most expensive and time-consuming aspect of fiber-optic infrastructure is installation, which often requires burying cables underground or suspending them along power grids. Supply cannot always keep pace with the growing demand, particularly in rapidly developing regions. The strain on network capacity was particularly evident during the COVID-19 pandemic, when remote work and online learning surged. To maximize efficiency without requiring costly modifications to existing infrastructure, various high-dimensional encoding techniques have been developed. These techniques utilize different properties of light to encode more than one bit of information per optical pulse. Optical pulses carrying such encoded data are referred to as symbols, forming a distinct alphabet of information transmission.

However, the size of this alphabet is limited by technical constraints and imperfections in the

system. Identifying the optimal scenarios and applications for quantum communication remains an ongoing challenge. Additionally, network traffic can be multiplexed across various dimensions, such as time or frequency, to increase capacity. The most widely used method is dense wavelength division multiplexing (DWDM), where multiple carrier waves are precisely separated before being transmitted through a shared fiber. While DWDM enhances efficiency, it also increases network complexity and costs, and its scalability is constrained by the number of available channels and launch power limitations.

To further reduce costs and improve the reliability of optical communication systems, photonic integrated circuits (PICs) have been introduced. These circuits integrate optical, electronic, and optoelectronic components into compact modules, reducing overall system size, heat dissipation, and power consumption. Advances in hermetic sealing and bonding technologies enable the development of ready-to-use modules, lowering costs and improving large-scale reliability. Various platforms and components are available for PICs, each offering distinct advantages. Some of these technologies, initially designed for classical optical communication, are now gaining attention in the quantum communication community. Following successful deployments, they have demonstrated feasibility for secure quantum data transmission, paving the way for more robust and efficient communication systems.

Quantum key distribution benefits from all of the aforementioned technologies, and is faced with more challenges. Quantum signals are susceptible to loss, noise, and crosstalk, particularly when co-propagating with high-power classical channel in networks when using multiplexed channels. QKD protocols require accurate description of real-world devices to provide realistic estimates of performance. As QKD matures from theoretical promise to practical deployment, its integration with existing telecom infrastructure becomes not only desirable but necessary. Leveraging the vast reach and capacity of optical fiber networks ensures that quantum-secure key distribution can scale alongside modern data demands. Photonic integrated circuits emerge as a key enabler in this domain, allowing for miniaturization and scaling of transmitters and receivers. Crucially, PICs offer the flexibility to adapt components originally designed for classical data transmission to the quantum regime. This reuse of mature telecom technology accelerates the development of platforms that can handle quantum information tasks within the same hardware infrastructure as classical communication, paving the way for future quantum-safe networks.

The information capacity of QKD systems can be increased using high-dimensional protocols, which allow encoding more than one bit of information per symbol. However, the choice of encoding must be supported by a corresponding security proof that rigorously demonstrates the protocol's security. Developing such proofs is essential not only for ensuring secure implementations, but also represents a critical step toward certifying quantum systems—an important prerequisite for the widespread adoption of quantum cryptographic technologies.

Chapter 2

Introduction

In this chapter, I briefly revisit the fundamental concepts of optical communication, as they are closely linked to quantum key distribution (QKD) methods. I begin by discussing selected encoding techniques and explore ways to enhance efficiency through alphabet expansion and multiplexing. I then examine the role of photonic integrated circuits and the current state of the art in the field. To provide context for quantum cryptography, I compare asymmetric and symmetric encryption, highlighting their relevance to modern networks. Finally, I introduce QKD, covering its theoretical foundations and recent advancements.

2.1 Optical communication

Communication fundamentally relies on electromagnetic (EM) waves, which originate from Maxwell's equations [1]. The wave equation describing dynamics of electric field $\vec{E}$ in a source-free, anisotropic, and linear medium reads:

$$\nabla^2 \vec{E}(\vec{x},t) - \frac{1}{c^2}\frac{\partial^2 \vec{E}(\vec{x},t)}{\partial t^2} = 0, \tag{2.1}$$

where $\nabla^2 = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2}$ is the Laplacian operator, c is the speed of light, t is time, and $\vec{x}$ is the position vector. Spatial distribution of the electric field is given by the Helmholtz equation:

$$\nabla^2 \vec{E}(\vec{x},t) + k^2 \vec{E}(\vec{x},t) = 0, \tag{2.2}$$

where $k = \frac{\omega n}{c}$ is the wavenumber, ω is the angular frequency of the wave, and n is the refractive index. Boundary conditions and constants determine the the solutions, which correspond to different spatial modes, which can be used for information transfer. Within the scope of this thesis, only linear polarization of light and single spatial mode are of interest, therefore polarization and space dependencies are omitted. Assuming that slowly varying envelope approximation (SVEA) [2] applies, the solution to the wave equation is:

$$E(z,t) = A(z,t)e^{i(\omega_0 t - kz + \varphi_0)}, \tag{2.3}$$

where $A(z,t)$ is the time-dependent envelope of an optical pulse, ω_0 is the central angular frequency, and φ_0 is the initial phase. Amplitude, frequency, time, phase, spatial mode, and polarization can be used to encode information in optical pulses. The signal's spectrum is given

by the Fourier transform of the temporal pulse profile:

$$\tilde{E}(z,\omega) = \int_{-\infty}^{\infty} E(z,t)\, e^{-i\omega t}\, dt. \tag{2.4}$$

Nowadays optical communication benefits from various modulation formats [3] allowing for tremendous data transfer speeds. Majority of optical communication systems are based on single-mode [4] or multi-mode [5] fibers due to low attenuation and dispersion [6, 7]. Recent trends also include attempts on using multicore fibers for enhanced capacity [8]. A simple fiber-optic link comprises a directly or indirectly-modulated light source (laser diode), communication channel, optical amplifier and a receiver (photodiode). Specific setup depends on implementation and modulation format. In the following part of the chapter I briefly discuss the ones that are most relevant to the topic of the thesis.

2.1.1 Pulse position modulation

Pulse position modulation (PPM) is a method of encoding information based on the time of arrival of optical signals relative to a reference. PPM operates by dividing a time frame into discrete time slots and shifting the position of the pulse within these slots according to the value of the modulating signal. In its simplest form, signals are detected as either "early" or "late", with binary values assigned accordingly—this is known as binary pulse position modulation (BPPM). This scheme can be extended to d-ary PPM, where d symbols encode $\log_2(d)$ bits per symbol by increasing the number of available pulse positions. An example of four-dimensional PPM is shown in Fig. 2.1.PPM requires a common clock for synchronization. Unlike other modulation

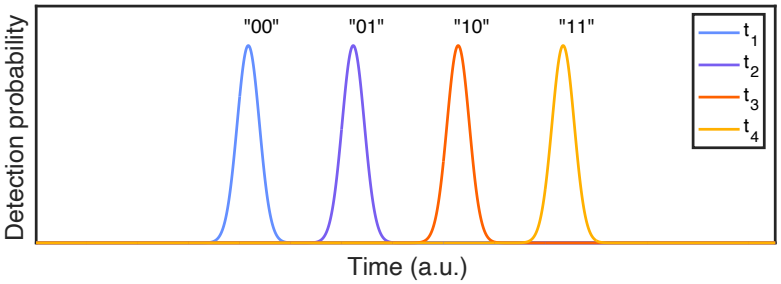

Figure 2.1: Gaussian envelopes of optical pulses representing symbols used for four-dimensional pulse position modulation.

schemes, it does not require phase-locked loops (PLLs) and can be implemented in a differential manner, where one symbol serves as a time reference for the next. This encoding method is widely used in satellite and free-space communication due to its robustness. While PPM is sensitive to synchronization quality, it is resistant to amplitude noise and can require less bandwidth than other modulation formats [9].

2.1.2 Differential phase shift keying

Differential phase shift keying (DPSK) is a phase modulation technique where information is encoded in the difference between successive phase states of the carrier signal rather than in absolute phase values. In standard phase shift keying (PSK), each symbol is represented by a specific phase value. However, in DPSK, each symbol is encoded as a change in phase relative to

the previous symbol. This means that instead of directly modulating the carrier phase with the input data, DPSK encodes the difference $\Delta\Phi$ between consecutive symbols. Binary "0" can be represented by no phase shift, and "1" by a shift by π. Example of phase-encoding is presented in Fig. 2.2. This scheme can be extended to d-array modulation by using d distinct phase levels to

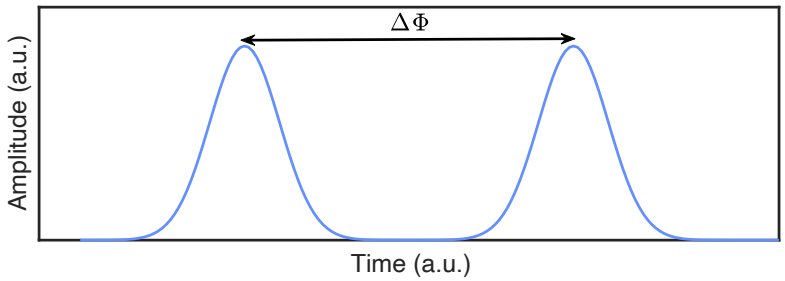

Figure 2.2: Gaussian envelopes of optical pulses used for binary differential phase shift encoding.

represent different symbols. The detection process is performed using a delay line interferometer (DLI), as illustrated in Fig. 2.3.The delay line interferometer (DLI) splits the incoming signal

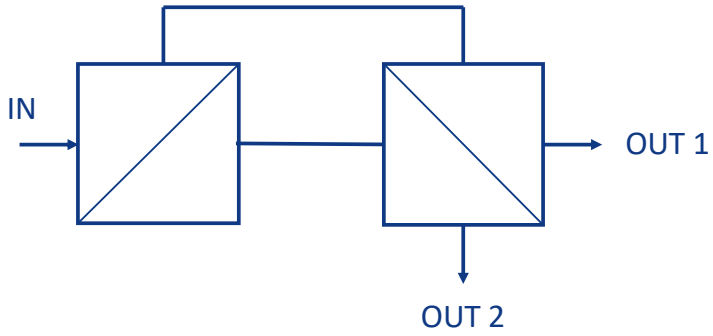

Figure 2.3: Delay line interferometer schematic.

into two paths of unequal lengths, introducing a controlled time delay. This delay corresponds to the separation between consecutive symbols. The information is decoded from the output intensity after interference between the two signals. A key advantage of DPSK is that it does not require a local oscillator or an absolute phase reference for detection. However, it is sensitive to timing errors, as the introduced time delay must be precisely matched to ensure accurate demodulation [10].

2.1.3 Frequency shift keying

Frequency shift keying (FSK) is another method of encoding information [11]. FSK is a digital modulation technique in which data is transmitted by varying the frequency of the carrier wave while keeping its amplitude and phase constant. In the binary version (Binary FSK, or BFSK), binary "0" and "1" are represented by two distinct carrier frequencies. This scheme can be extended to a d-array FSK format by using d different frequencies to encode multiple bits per symbol. An example of four-dimensional FSK is shown in Fig. 2.4. FSK signals can

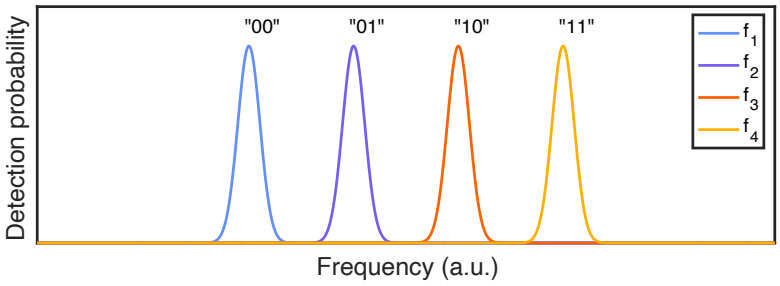

Figure 2.4: Gaussian envelopes of optical pulses representing four-dimensional frequency shift keying.

be discriminated using spectral filters combined with multiple photodiodes or by referencing known frequency values. While FSK offers strong resistance to noise, it generally requires more bandwidth compared to other modulation formats [12].

2.1.4 Multiplexing

To increase network capacity and make optimal use of existing infrastructure, traffic must be efficiently managed through multiplexing. Multiplexing in fiber-optic telecommunications is a technique that enables multiple signals to be transmitted simultaneously over a single optical fiber. This approach helps reduce costs by maximizing fiber utilization. The two most common multiplexing techniques are wavelength division multiplexing (WDM) and time-division multiplexing (TDM). In WDM, multiple data streams are transmitted simultaneously using different wavelengths of light, corresponding to different channels, within the same optical fiber, as illustrated in Fig. 2.5. Depending on the separation between the channels WDM can be coarse [13],

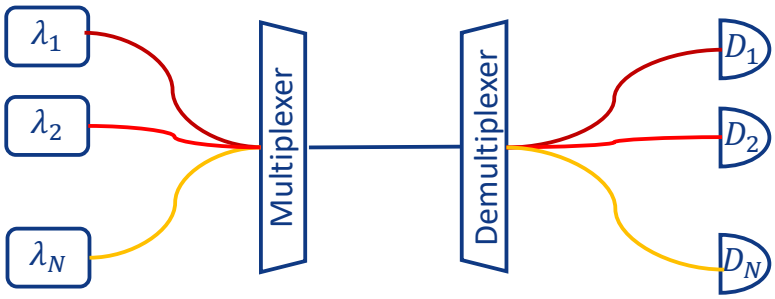

Figure 2.5: Wavelength division multiplexing. Each transmitter operates on a distinct carrier wavelength $(\lambda_1, \lambda_2, \ldots, \lambda_N)$. These individual signals are combined and launched into a single optical fiber using a multiplexer. At the receiving end, a demultiplexer separates the combined signal by wavelength, routing each channel to its corresponding detector $(D_1, D_2, \ldots, D_N)$.

dense [14], or ultradense [15]. The performance of WDM is limited by inter-channel crosstalk and dispersion-related effects. Crosstalk arises from the finite extinction ratio of spectral filters used for combining and separating wavelengths. Additionally, photons can leak into adjacent channels due to Rayleigh scattering and nonlinear effects such as four-wave mixing (FWM) and self-phase modulation (SPM). As a result, the power of leaking signals depends on the launch power of each channel.

In TDM, each signal is assigned a specific time slot in a high-speed data stream, as illustrated in Fig. 2.6. Unlike WDM, TDM is less prone to crosstalk since signals are transmitted in separate

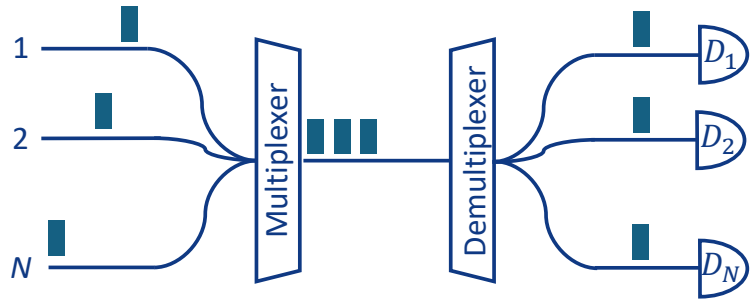

Figure 2.6: Time division multiplexing. Signals originating from different channels $1, 2, \ldots, N$ are combined in time by the multiplexer. At the receiving end, signals are directed to the corresponding receivers $D_1, D_2, \ldots, D_N$ by the demultiplexer.

time slots, reducing spectral interference. However, precise synchronization is required to avoid timing errors and ensure correct data retrieval. Besides WDM and TDM, other multiplexing techniques include polarization division multiplexing (PDM) [16], which utilizes different polarization states of light to transmit independent data streams, and mode division multiplexing (MDM) [17, 18], which uses different spatial modes in multimode fibers to increase capacity. This strategy can be implemented with multicore fibers. Recent research focuses on using hybrid multiplexing strategies, such as combining time and frequency domain multiplexing to leverage the advantages of both techniques [19].

2.1.5 Photonic integrated circuits

Photonic Integrated Circuits (PICs) are the optical equivalent of electronic integrated circuits (ICs), where multiple photonic components—such as lasers, modulators, waveguides, photodetectors, and couplers—are integrated onto a single chip to manipulate and process light signals. These circuits enable high-speed optical communication, sensing, and signal processing. The key advantages of photonic integrated circuits, as compared to bulk or fiber-based optical setups are:

- size reduction: the surface of an individual chip is usually smaller than 200 mm^2.
- cost reduction: one chip with full functionality can be a few times cheaper then an average component itself, e.g. modulator
- low power consumption: majority of on-chip components consume currents < 200 mA.
- easy thermal management: compact size allows for easier and stable control of the temperature by TEC and cryogenic coolers.

Current state of the art chips are either manufactured using experimental processes and platforms or using generic technology. Generic photonic integration refers to a standardized approach to designing and manufacturing PICs, similar to the foundry model in microelectronics. This approach enables the cost-effective development of PICs by utilizing shared process technologies and standardized building blocks across various applications. Like CMOS electronics, generic photonic integration relies on predefined libraries of optical components (waveguides, couplers,

modulators, etc.), allowing designers to create circuits without worrying about low-level fabrication details. This set of libraries is called the process design kit (PDK). Designed circuits are manufactured within the multi-project wafer run (MPW). Manufacturing is a very complex process employing advanced methods, such as photolithography, epitaxy, etching and vapor deposition [20]. It usually starts with a high-quality substrate - the wafer. Manufacturing one architecture at small quantities would therefore be very expensive. The costs are reduced by the foundries by placing different architectures from interested parties on a single wafer, and manufacturing when full surface is occupied. After MPW, each party gets several designs operating within specified tolerances, and possibly "mechanical samples" which may not be fully functional yet useful. An example batch of PICs manufactured by SmartPhotonics is illustrated in Fig. 2.7 Several material platforms support generic photonic integration, each offering differ-

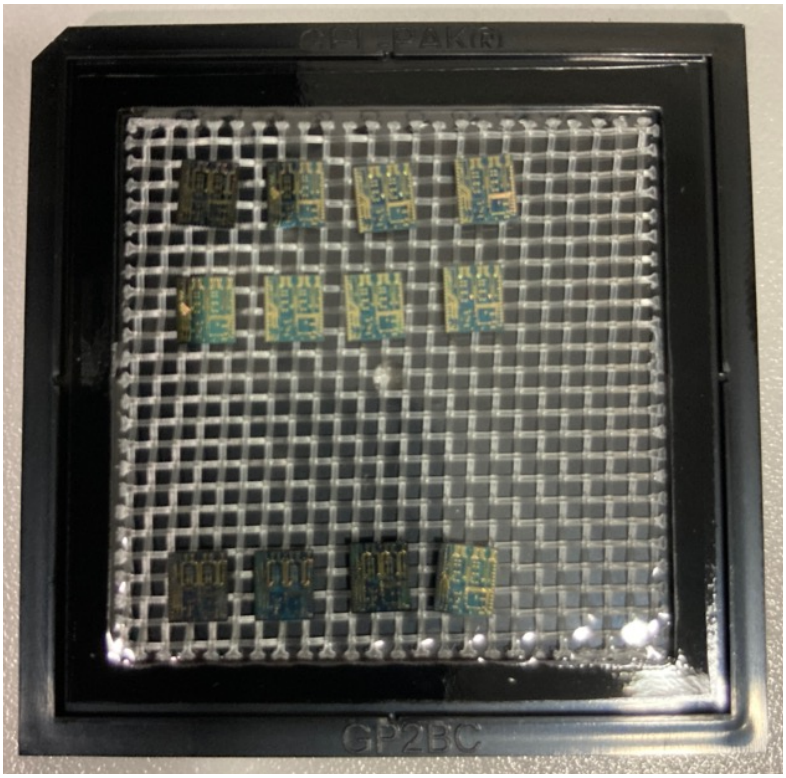

Figure 2.7: Photonic integrated circuits in a gel pack. Working chips are separated from the mechanical samples.

ent functionalities. Silicon photonics is a natural candidate due to CMOS-compatible process allowing for integrating optoelectronic and electronic chips. Another advantage is low transmission loss and a high dielectric contrast allowing for efficient electromagnetic field confinement. However, due to the indirect bandgap of silicon light sources and detectors have to be integrated separately. In contrary, indium phosphite (InP) platform allows for engineering of on-chip light sources and detectors due to direct bandgap. Constructing waveguides is possible as well, but an average loss is higher in comparison to silicon. Silicon nitrite offers the lowest transmission losses rendering it feasible for constructing receivers where long optical paths are required e.g. delay lines. Its weakness lies in the unavailability of active components. Another emerging platform

is lithium niobate, offering excellent electro-optic properties suitable for fast modulation and frequency conversion via nonlinear effects. Since different platforms offer unique features, hybrid integration is gaining growing interest. One example is the PolyBoard developed by Fraunhofer Heinrich-Hertz Institute (Germany). This concept relies on using polymer-based platform as a basis for placing and merging chips manufactured in different technologies to get the best of all of them [21]. PolyBoard allows for manufacturing waveguides, installing electrodes for electrical interfaces and placing free-space optical elements such as thin-film spectral filters or polarizing beam splitters. Moreover, PolyBoard is feasible for designs operating over a broad range of wavelengths. Constructing photonic integrated circuits for quantum communication applications is challenging due to the fact that quantum technologies require low-loss waveguides and efficient single photon sources and detectors operating on different wavelengths for various applications. One of examples being the need for small and scalable entangled photon pair sources. Entangled photon pair generation usually relies on nonlinear light-matter interaction. For a spontaneous parametric down conversion (SPDC) process, the pump, signal, and idler beams can occupy vastly different spectral regions [22]. PolyBoard would be a perfect solution to address this challenge. An entangled photon pair source may also be implemented with micro ring resonators (MRRs) available within silicon nitrite. A hybrid approach would allow to merge the resonator chip with InP chip used for pumping and monitoring of optical power. Recent developments in InP platform allowed for integrating single photon avalanche photodiodes operating in telecom C-band, enabling quantum random number generators [23].

Beyond generic integration, photonic circuits have also been merged with superconductive detectors for demanding applications [24, 25]. Non-generic PICs have also been used for various quantum technologies, such as sources of quantum light, QRNGs, quantum computation, sensing platforms, as well as for quantum key distribution [26, 27].

2.2 Quantum key distribution (QKD)

This section serves as a introduction to QKD. Here I present the assumptions upon the security of this method and introduce the first protocol as a basis for developing other, modern variants. I present a brief overview of other protocols and recent advancements in the field. Finally, I explain fundamental concepts ending with a formula for secret key rate.

2.2.1 Assumptions and security

Quantum key distribution protocols rely on a set of assumptions to ensure their security. These assumptions can be grouped into two categories: foundational and implementation-specific [28]. Before diving into them, it's helpful to introduce the standard terminology used in QKD. Alice and Bob are the two communicating parties, with Alice typically acting as the transmitter and Bob as the receiver. Eve is the eavesdropper or adversary attempting to intercept or tamper with their communication. In some protocols, a third party—Charlie—assists with certain operations, such as entanglement distribution or measurement. The foundational assumptions underlying QKD security are as follows:

1. **Correctness of Quantum Theory:**
   Quantum mechanics is assumed to accurately predict measurement outcomes.

2. **Completeness of Quantum Theory:**
   Quantum theory, combined with the assumption of free choice (measurement settings can be independently chosen), fully describes the quantum system. No hidden variable theories or alternative explanations contradicting quantum theory exist.

3. **Authenticated Classical Communication:**
   Parties must authenticate each other, ensuring that no adversary can impersonate legitimate users without detection.

Realistic implementations of QKD protocols must consider the following assumptions:

1. **Isolation of Devices:**
   Quantum and classical devices are assumed secure, though adversary has access to practical interfaces e.g. the quantum channel and might explore its vulnerabilities.

2. **State Preparation Fidelity:**
   It is assumed that Alice can prepare quantum states exactly as specified. Deviations from ideal states may introduce vulnerabilities, which may be the case for practical implementations.

3. **Measurement Device Imperfections:**
   Imperfections or inaccuracies in measurement devices must be accounted for to prevent exploitation by an adversary.

4. **Timing and Synchronization:**
   Accurate synchronization and consideration of detector dead times are required for correct post-processing of data. Timing issues could lead to security breaches.

5. **Accurate Parameter Estimation in Post-processing:**
   All information potentially leaked to an adversary during quantum and classical transmission must be properly estimated and corrected in post-processing steps, including error correction and privacy amplification.

Theoretical security in QKD must be established through rigorous mathematical proofs. These security proofs generally fall into three categories—device-dependent, device-independent, and semi-device-independent—each defined by the specific assumptions they make about the adversary's capabilities.

Device-dependent security proofs assume a prepare-and-measure protocol, where the quantum states are generated and measured using trusted and well-characterized devices. The prepared states are assumed to follow known probability distributions. The key rate optimization problem in this scenario is a convex optimization task, typically of non-deterministic polynomial-time (NP) complexity, which guarantees the existence of a global optimum. Efficient algorithms have been developed to solve these problems [29, 30], making device-dependent QKD the most practically implemented form today.

Device-independent security proofs, on the other hand, make no assumptions about the internal workings of the devices used by Alice and Bob. The devices are treated as black boxes, and security is based solely on the violation of a Bell inequality [31]. In this model, Eve is assumed to be all-powerful. She can even choose the measurement settings and influence the output distributions of the devices. Achieving secure key generation in this scenario requires high-quality entangled photon sources, ultra-low-loss channels, and high-efficiency detectors. Any loss is treated as a potential attack. While DI-QKD offers the strongest form of security, it is experimentally extremely demanding. The key rate estimation in this case can often be formulated as a polynomial-time optimization problem [32, 33].

Semi-device-independent (semi-DI) security proofs lie between the two aforementioned ones. These protocols relax some assumptions compared to DD-QKD, while not requiring full device independence. For example, measurement-device-independent (MDI) QKD is secure even if the

detectors are untrusted, but still assumes trusted state preparation. Other semi-DI approaches rely on assumptions such as bounded dimension [34] or energy [35] of the quantum systems. These protocols aim to balance experimental feasibility with improved robustness against implementation flaws.

A security proof yields a formula for the secret key rate. There exists a variety of frameworks in popular programming languages for simulating key rates considering different protocols and scenarios [36, 37]. Exploiting the weaknesses of QKD systems is the domain of quantum hacking. Various imperfections can be used to pose threat to QKD systems [38, 39, 40, 41]. German Federal Office for Information Security (BSI) published a report about the maturity of QKD systems [42] and a comprehensive list of attacks including security recommendations and risk levels [43]. Constructing commonly-accepted QKD systems requires certification and standardization procedures. This however, is an upcoming effort. It involves works on a rigorous and detailed security proof without loopholes, analysis of quantum hacker's possibilities and preparing measurement procedures for building and calibrating the systems.

2.2.2 The first idea: BB84 protocol

The first QKD idea was proposed by Bennet and Bassard in 1984 [44]. They proposed using polarization degree of freedom for quantum key distribution. This historic example is presented as a blueprint for understanding QKD in general. This is a device-dependent prepare and measure protocol. A general structure, universal for such protocols is the following:

- 1. Generating random bits. Alice uses quantum random number generator (QRNG) to generate perfectly random bits which will be encoded in the key generation and control bases.
- 2. State preparation and transmission. Alice encodes the random bits using one of the randomly-selected mutually-unbiased bases. Prepared quantum states are sent to Bob over a quanutum channel.
- 3. Measurement. Bob decodes the incoming quantum signals with a randomly-selected measurement basis, and records both the outcome and the corresponding basis selection.
- 4. Sifting. Alice and Bob publicly announce measurement bases. Results obtained when encoding basis doesn't match the decoding basis are discarded.
- 5. Parameter estimation. The fraction of erroneus measurements reveals amount of information that Eve has on the bit strings. The parameter quantifying that is the quantum bit error rate (QBER). QBER can be used to estimate the resultant raw secret key rate. If this value is too high, the protocol is aborted. The exact maximal tolerable value depends on the protocol.
- 6. Information reconciliation. At this stage Alice and Bob share some information to correct discrepancies between their respective raw keys. Information about bit parity of key blocks or error correction schemes can be used.
- 7. Error verification and correction. Even after information reconciliation, there's a small probability that undetected errors remain in Bob's key. This step allows Alice and Bob to detect any such residual mismatch before moving on to privacy amplification. Alice and Bob independently compute a one-way function, the hash of their corrected keys using a publicly agreed-upon hash function, such as e.g. the Toeplitz Hash [45]. Then they

compare the hash values over the authenticated classical channel, and if the values match the key can be considered identical with high confidence.

- 8. Privacy amplification and key generation. Privacy amplification serves reducing even further any potential information about the system that Eve may have. This is obtained sacrificing even more raw key bits and transforming it into the secret key according to a security proof. The resultant secret key would be indistinguishable from a completely random one as perceived by adversary up to a very small protocol failure probability.

For the polarization-based BB84 Alice uses four qubits based on four polarization states of single photons: horizontal ($|\mathrm{H}\rangle$), vertical ($|\mathrm{V}\rangle$), diagonal ($|\mathrm{D}\rangle$), and antidiagonal ($|\mathrm{A}\rangle$). Those states allow creating two mutually-unbiased bases (MUBs): the key generation $\{|\mathrm{H}\rangle, |\mathrm{V}\rangle\}$ and control basis $\{|\mathrm{D}\rangle, |\mathrm{A}\rangle\}$, where:

$$|\mathrm{D}\rangle = \frac{|\mathrm{H}\rangle + |\mathrm{V}\rangle}{\sqrt{2}}, \tag{2.5}$$

$$|\mathrm{A}\rangle = \frac{|\mathrm{H}\rangle - |\mathrm{V}\rangle}{\sqrt{2}}. \tag{2.6}$$

Alice uses those bases to encode random "0" and "1" bits. Bob randomly selects one of the MUBs for measurements and assigns bit values to outcomes. The protocol continues along the aforementioned structure. To present how the procedure reacts to a presence of the adversary, let us consider a simple intercept-and-recent strategy [46]. During this attack, Eve measures Alice's signals, stores the outcomes, and attempts to generate the same states she received and forward them to Bob. The states cannot be cloned due to no-cloning theorem. At this point of the protocol, Alice has not yet announced her choice of basis, so Eve has to guess in which basis she has to measure the states, thereby randomly choosing the basis she measures in. That choice will be wrong in approx. 50 % cases. Exemplary round is illustrated in the table below:

Key bit	1	0	0	0	1	1	0	0	0	1
Alice's basis	X	X	Z	X	X	Z	Z	X	Z	Z
Alice's state	$\|\mathrm{D}\rangle$	$\|\mathrm{A}\rangle$	$\|\mathrm{V}\rangle$	$\|\mathrm{A}\rangle$	$\|\mathrm{D}\rangle$	$\|\mathrm{H}\rangle$	$\|\mathrm{V}\rangle$	$\|\mathrm{A}\rangle$	$\|\mathrm{V}\rangle$	$\|\mathrm{H}\rangle$
Eve's basis	Z	X	X	Z	X	Z	X	Z	X	Z
Eve's state	$\|\mathrm{H}\rangle$	$\|\mathrm{A}\rangle$	$\|\mathrm{A}\rangle$	$\|\mathrm{H}\rangle$	$\|\mathrm{D}\rangle$	$\|\mathrm{V}\rangle$	$\|\mathrm{A}\rangle$	$\|\mathrm{V}\rangle$	$\|\mathrm{A}\rangle$	$\|\mathrm{H}\rangle$
Bob's basis	Z	X	Z	Z	X	X	Z	X	Z	X
Bob's result	1	0	1	1	1	1	0	0	1	1
Sifting	x	ok	ok	x	ok	x	ok	ok	ok	x
Key bit		0	1		1		0	0	1	
Parameter estimation			x				ok	ok		

One of the most popular protocols for nowadays implementations is the time-phase variant of the BB84. It is inspired by PPM and DPSK. Bit values in the key generation basis are encoded in time of arrival. Information in the control basis is imprinted in relative phase between the pulses forming a superposition based on early and late pulses (see Fig. 2.8). The superpositions are measured with a delay line interferometer, and bit value is assigned based on the interference outcome [47, 48]. Selecting the degree of freedom comes with different technological advantages and disadvantages. Polarization-based qubits can be easily prepared with modern high-quality optical components and pulsed lasers. Using a gain-switched laser randomizes the phase between consecutive qubits which improves security. Polarization is well preserved in air, making it feasible for free-space communication. It was successfully demonstrated using air-ground [49]

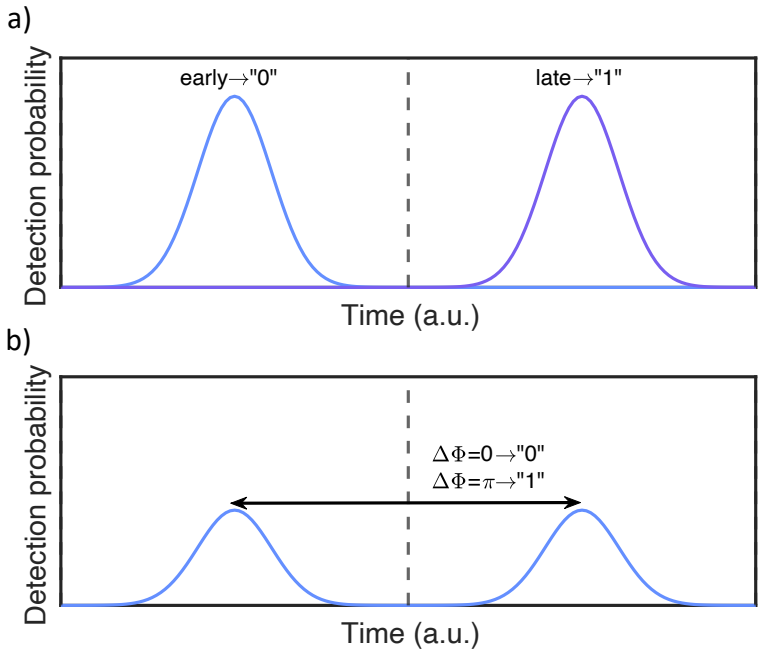

Figure 2.8: Two-dimensional time-phase BB84 encoding: a) key generation basis (Z basis), b) control basis (X basis).

and space-ground [50] links. Receivers do not require interferometric stability. They also require only one time-bin in comparison to time-phase equivalent, which allows for faster information exchange given same repetition rate. The downsides are that separate synchronization channel is required and alignment of polarization states with respect to the receiver can change over time due to birefringence. Losses and properties of photonic components are also polarization-dependent. Additionally, dedicated synchronization channel is required. The time-phase variant can benefit from huge availability of mature telecommunication equipment for practical deployments and therefore high electronic bandwidths for fast signal generation. This encoding is also compatible with generic photonic integrated technology, and its robust to polarization changes. The downsides include necessity to precisely control separations, widths and shapes of the pulses, which can be challenging. This encoding can also be sensitive to the timing uncertainties. Although precise synchronization is required, it can be achieved without distributing a dedicated synchronization signal. The nature of time-phase encoding allows using clocks locally and correct the offset between them based on temporal statistics of single-photon counts [51, 52]. In case of fiber-based systems this allows using only one fiber, which significantly reduces grid exploitation costs.

2.2.3 Other protocols and recent advancements

Just as classical communication can benefit from expansion of the alphabet, QKD protocols can become more efficient by increasing the dimension of the Hilbert space [53]. A time-phase BB84 can be expanded into d dimensions by adding more symbols to the two MUBs. However, this results in a more complex receiver architecture, as distinguishing a d-dimensional superpositions requires $d-1$ DLIs with different settings [54] and d detectors. An example for a $d=4$ case

is shown in Fig. 2.9: One of advantages of high-dimensional encoding is enhanced resilience to

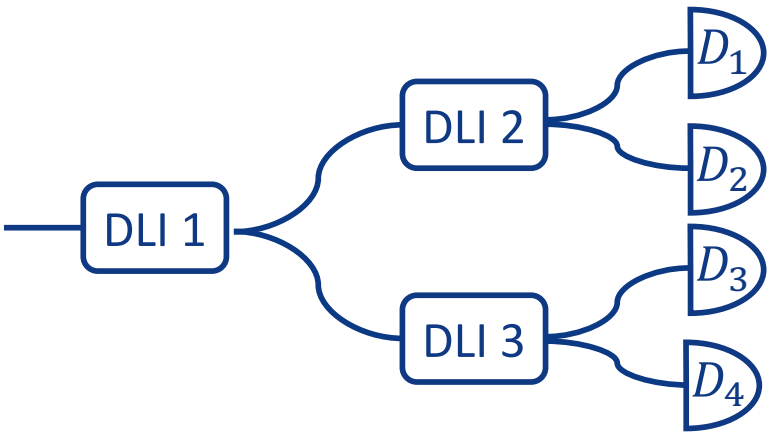

Figure 2.9: Interferometer tree for measuring four-dimensional time-bin superpositions. Three delay line interferometers allow distinguishing four different superpositions by observing interference results with $D_1, \ldots, D_4$ detectors.

noise [55], which may allow to establish QKD over challenging links [56]. Another advantage is increased information entropy, implying that every successful detection event carries more than one bit information [57]. This factor can help to overcome certain flaws of single photon detectors, when their speed is internally limited by the detector properties[58]. Other ways to increase the capacity of QKD links include using multiplexing strategies, using multiple or high-speed single-photon detectors [59, 60], or using high qubit repetition rates [61, 62]. There exists a variety of other QKD protocols and corresponding security proofs and implementations. In continuous variable (CV) protocols Alice sends coherent or squeezed light states [63], and Bob performs homodyne or heterodyne detection to measure the light's quadratures [64]. This protocol is adequate for middle-range communication, and it can rely on standard telecom equipment [65]. Twin-field method is an interesting protocol for long-range communication where Alice and Bob send weak coherent states to a middle untrusted node Charlie. Charlie derives key bits from the interference outcomes [66]. Recent demonstrations show deployment over fiber-based links of length exceeding 300 km [67, 68, 69, 70] and implementation of efficient phase distribution methods [71] over fiber networks.

One of the oldest protocols based on polarization-entanglement is E91 [72]. In this protocol Charlie generates entangled photon pairs. One photon is distributed to Alice and the other to Bob. Alice and Bob perform Bell state measurements, and if corelation value overcomes the Bell bound no Eve was present. Links over 20 km distance have been established [73]. This idea stimulated the development of MDI protocols [74, 75, 76]. Other versions of this protocol can benefit from the time-energy entanglement [77], and have been successfully deployed as well [78, 79]. More detailed information about protocols and mathematical description can be found in [80]. Some of those protocols can benefit from highdimensional approach and the decoy state method for enhanced security, which will be briefly introduced in the next part of this chapter.

Recent advancements in QKD highlight the growing importance of photonic integrated circuits (PICs). Silicon-based PICs have been successfully employed in a variety of QKD protocols, including polarization-based BB84 [81], coherent one-way (COW) [82], three-state protocols [83], continuous-variable QKD [84], time-bin BB84 [85], and measurement-device-independent QKD [86]. Indium phosphide (InP) platforms have also demonstrated significant capabilities, sup-

porting implementations of BB84 [82, 87, 88], COW [82], MDI [89], and differential phase shift protocols [82, 87]. Furthermore, hybrid integration of silicon and InP technologies has enabled QKD transmission over distances exceeding 250 km [90].

2.2.4 Key concepts

The goal of QKD is to generate as much mutual information between Alice and Bob as possible while keeping Eve's knowledge about it minimal. The amount of secret key rate can therefore be intuitively understood as a difference between Shannon mutual information values for Alice and Bob (I_{ab}), and Alice and Eve (I_{ae}) [91]:

$$R = I_{\mathrm{ab}} - I_{\mathrm{ae}}. \tag{2.7}$$

Mutual information between Alice and Bob is proportional to the bit value and error they make in communication [92, 93]: Describing a real-world QKD system and predicting the resultant key

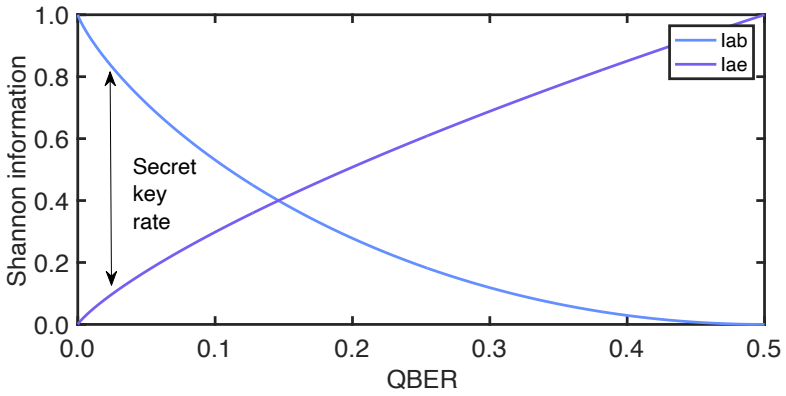

Figure 2.10: Mutual information between Alice and Bob and Alice and Eve as a function of QBER.

rate values requires modeling of single-photon sources, quantum channels, and detectors. The single-photon source of choice for experiments conducted within this thesis a highly-attenuated classical telecommunications laser operating in a continuous wave mode. The output pulses are weak coherent states. Definitions, derivations and limitation presented below are presented in detail in ref. [94]. I am revising some concepts here as a general introduction to modeling QKD systems. The quantum state of these pulses can be represented as follows:

$$|\gamma\rangle = e^{-\frac{|\gamma|^2}{2}} \sum_{n=0}^{\infty} \frac{\gamma^n}{\sqrt{n!}} |n\rangle, \tag{2.8}$$

where $|n\rangle$ denotes a *Fock state*, indicating a state of a single-mode EM field with exactly n photons. Here, $|\gamma|^2$ corresponds to the pulse intensity, representing the average photon number per pulse μ. The probability of detecting exactly n photons in such a coherent state is governed by the Poisson distribution, given by:

$$\Pr(n) = |\langle n|\gamma\rangle|^2 = e^{-|\gamma|^2} \frac{|\gamma|^{2n}}{n!}. \tag{2.9}$$

The probability of detecting a multi-photon pulse is non-zero. This poses a risk of photon number splitting attack (PNS), where Eve uses a beam splitter to split the pulse carrying information.

To mitigate that risk, the decoy state method can be employed [94, 95]. To implement the decoy state method, Alice uses two (or more) μ levels, corresponding to signal and decoy pulses. Alice randomly mixes these decoy pulses with signal pulses. Both pulse types are identical in all characteristics except their mean photon numbers. Eve, unaware of the nature (signal or decoy) of each pulse, treats all pulses equally and consistently according to her attack strategy. After transmission, Alice announces publicly which pulses were decoy states. Bob then evaluates the detection statistics and compares the detection rates of signal states and decoy states. If Eve conducted a PNS attack, Bob would observe significantly higher losses on the signal states compared to the decoy states. This discrepancy in losses between decoy and signal states allows Alice and Bob to detect Eve's presence and counteract the attack. The number of decoy states can differ, and all μ values must be optimized to provide highest possible key rate values.

For fiber-based quantum channels the transmission t_{AB} can be calculated based on the length of the fiber l and loss coefficient α expressed in dB/km:

$$t_{\mathrm{AB}} = 10^{\frac{-\alpha l}{10}}. \tag{2.10}$$

The probability to detect the weak coherent states is dependent on the transmission of Bob's internal components t_{Bob} and efficiency of detectors η_{det}. The overall transmission η reads:

$$\eta = t_{\mathrm{AB}} t_{\mathrm{Bob}} \eta_{\mathrm{det}}. \tag{2.11}$$

The probability to detect single-photon states will further be altered by the properties of the detectors, which are described in Chapter 3. The weakest "vacuum" signal level is bounded by those properties. In general, the transmission of an n-photon state is given by:

$$\eta_n = 1 - (1 - \eta)^i, n = 0, 1, 2... \tag{2.12}$$

The yield is a conditional probability that a pulse containing exactly n photons results in a successful detection at Bob's side. It originates from two parts, the background countrate Y_0 corresponding to detector's dark counts and counts stemming from other parasitic sources, and the signal part Y_i. The i-photon yield Y_n is given by:

$$Y_n = Y_0 + \eta_n - Y_0 \eta_n. \tag{2.13}$$

The most important kinds of yield values are:

- Y_0 – the vacuum yield representing the probability that no photons were send. This value corresponds to other background countrate.
- Y_1 – the single photon yield. This value is estimated through experimental measurements for different μ.
- Y_n – yields corresponding to multi-photon pulses

Knowing the yield allows estimating the gain, the quantity defined as the overall probability of detecting photons successfully, regardless of the number of photons actually sent by Alice. More precisely, the gain refers to the detection probability per sent pulse, including both genuine photon detections and noise. The total gain Q_μ is:

$$Q_\mu = \sum_{n=0}^{\infty} Y_n \cdot e^{-\mu} \frac{\mu^n}{n!}. \tag{2.14}$$

Gain is an experimentally measured quantity. Another crucial parameter is the quantum bit error rate (QBER) – the ratio of false and total counts:

$$QBER = \frac{N_{\text{wrong}}}{N_{\text{total}}}. \tag{2.15}$$

The false counts incorporate the fraction of received bits that are incorrect due to channel noise, misalignment, or potential eavesdropping. The total number of counts is a sum of false counts and detection events stemming from the quantum signal emitted by the transmitter. Mathematically, the total QBER (E_μ) is given by:

$$E_\mu = \frac{1}{Q_\mu} \sum_{n=0}^{\infty} e_n Y_n \frac{\mu^n}{n!} e^{-\mu}, \tag{2.16}$$

where e_n is the error rate of a n-photon state. In the two-decoy state scenario, these values are estimated using observed experimental parameters. The decoy-state method allows Alice and Bob to derive tight bounds on the yields and error rates, thereby optimizing the secure key rate.

The gains, yields and QBERs can be simulated or experimentally obtained for both X and Z basis and various signal intensity levels. The maximal experimentally-obtainable key rate value is called the raw key rate, and is given by:

$$R_{\text{raw}} = f_{\text{rep}} Q_\mu p_{\text{basis}} p_{\text{post}}, \tag{2.17}$$

where: f_{rep} is the frequency at which the symbols are transmitted, p_{basis} is the probability that Alice and Bob use compatible bases (50% for BB84 for passive basis choice), and p_{post} is the fraction of detected events that are actually used for the raw key. Certain events can be discarded due to ambiguous measurement outcomes, multi-click events, temporal filtering or other protocol-specific filtering method. Number of bits that can be securely extracted per transmitted pulse is called the secure key rate r. For a BB84 protocol with one intensity level the theoretical secure key rate formula reads:

$$r = p_Z^2 \left[Q_1^Z (1 - h(e_1^X)) - Q_Z f(E_Z) h(E_Z) \right], \tag{2.18}$$

where:

- p_Z is the probability that Alice and Bob choose the Z basis.
- Q_1^Z is the gain of single-photon states in the Z basis.
- e_1^X is the error rate for single-photon states in the X basis.
- Q_Z is the total gain in the Z basis, i.e., the probability that Bob detects a photon given that Alice sent a weak coherent pulse.
- E_Z is the QBER in the Z basis.
- $h(x)$ is the binary entropy function, given by:

$$h(x) = -x \log_2(x) - (1 - x) \log_2(1 - x). \tag{2.19}$$

- $f(E_Z)$ is the forward error correction efficiency factor.

This formula refers to the asymptotic rate, meaning that an infinite number of quantum signals is exchanged, all parameters (gains, error rates, etc.) are known exactly, and finite-key effects are omitted. The term $Q_1^Z(1 - h(e_1^X))$ represents the contribution of secure bits from single-photon states. The term $Q_Z f(E_Z) h(E_Z)$ accounts for the cost of error correction, where E_Z represents the observed quantum bit error rate in the key generation basis. When two decoy levels ν_1, ν_2 are introduced, the formula reads:

$$r \geq q \left\{ -Q_\mu f(E_\mu) H_2(E_\mu) + Q_1^{L,\nu_1,\nu_2} \left[1 - H_2 \left(e_1^{U,\nu_1,\nu_2} \right) \right] \right\}, \tag{2.20}$$

where:

- q is the protocol efficiency (e.g., 1/2 for standard BB84),
- Q_μ is the gain for signal intensity μ,
- E_μ is the QBER for signal intensity μ,
- $f(E_\mu)$ is the error correction efficiency function,
- $H_2(x)$ is the binary entropy function (see eq. 2.19),
- Q_1^{L,ν_1,ν_2} is the lower bound on single-photon gain, estimated from decoy states ν_1 and ν_2,
- e_1^{U,ν_1,ν_2} is the upper bound on single-photon QBER.

Exemplary key rate values simulated using formulas 2.18 and 2.20 for a range of quantum channel losses are presented in Fig. 2.11. The security enhancement introduced by the decoy

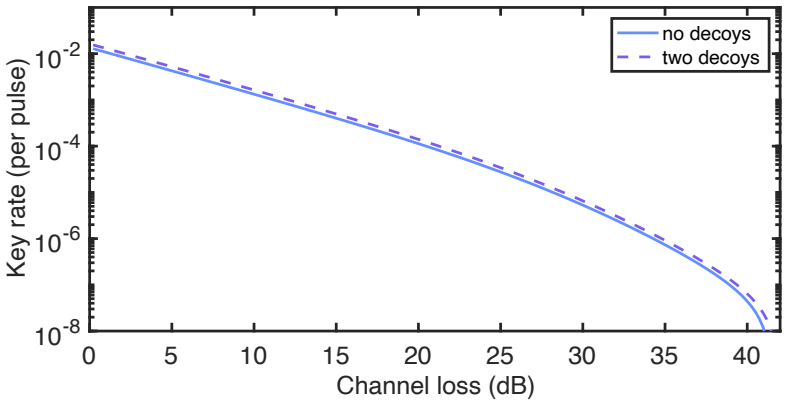

Figure 2.11: Exemplary simulated secret key rate (per pulse) values for BB84 protocol without decoy states and with two decoy states.

states is pronounced in higher key rate values [94]. The final secure key rate R_{sec} is a product of the secure key rate per pulse and the repetition rate:

$$R_{\text{sec}} = r f_{\text{rep}}. \tag{2.21}$$

The exact key rate formula and values are dependent on the security proof and on the focus of the analysis. Yields and QBERs can be upper and lower bounded, and the bounds are case-dependent. In particular, it is challenging to derive the formula for the phase error rate.

The key rate values will change with the number of decoy states, and the formula will differ between asymptotic and finite-key size scenarios [96]. The latter has recently been of greater interest, as they provide realistic estimate of performance for deployed links. The aforementioned analysis was performed for a qubit. Mathematical expressions must be adjusted to account for different dimensionality of encoding. One more challenge is accurate modeling of experimentally-feasible scenarios, in particular consideration of asymptotic key rate formulas stemming from two different security assumptions for high-dimensional encoding. A rigorous and intuitive approach to security proof for the finite-size key scenario is provided in [97]. A good general overview of QKD can be found in the book by Ramona Wolf [28]. Information on different protocols and the related mathematical formalism can be found in the book by Federio Grasselli [98].

2.3 Chapter summary

In this chapter, fundamental principles of optical communication were presented to establish the basis for understanding quantum key distribution schemes. Various classical modulation techniques were introduced, as their operational principles highlight relevance to high-dimensional QKD encoding, which is the subject of this thesis. Multiplexing methods were explored as strategies for increasing transmission efficiency. Then, the role of photonic integrated circuits in enabling compact, scalable, and efficient systems was examined, with a particular focus on generic and hybrid integration platforms suitable for quantum technologies. The chapter then introduced the essential concepts and recent advancements in QKD, including high-dimensional variants that enhance noise resilience and allow for increased information capacity per detection event. Foundational and practical security assumptions were outlined, followed by a detailed overview of the BB84 protocol as a representative example of a device-dependent prepare-and-measure protocol. Emphasis was placed on the time-phase implementation of BB84, as this version of the protocol is the basis for the main experiment of this dissertation. The decoy-state method and its importance for mitigating photon-number-splitting attacks were discussed, alongside essential formulas related to the key rate expression. The chapter concluded with insights into key rate value estimation, setting the foundation for experimental and theoretical analysis in the following sections of this thesis.

Chapter 3

Methods

This chapter serves as an introduction to experimental techniques used for the experiments. I begin by exploring electro-optic phase modulation and its application in amplitude modulation for both lithium niobate and on-chip modulators. Next, I discuss the principles of high-speed electrical signal propagation, including how signals are generated using an arbitrary waveform generator. I then examine time-correlated single-photon counting, focusing on how timing jitter impacts measurements. Finally, I introduce the single-photon spectrum measurement technique, which utilizes dispersive frequency-to-time mapping. Presented methods are crucial for conducting experiments with photonic integrated circuit as well as building and calibrating a QKD setup with advanced commercially-available devices.

3.1 Electro-optic phase modulation

The electro-optic phase modulator is a fundamental tool for encoding electrical signal information onto an optical carrier wave. In this section, I outline the key principles of its operation and discuss the techniques used in optical communication systems.

3.1.1 Pockels effect

The Pockels effect is a phenomenon of refractive index change in proportion to the strength of the electric field occurring in non-centrosymmetric materials [99]. Examples of such materials are lithium niobate (LiNbO3), lithium tantalate (LiTaO3), potassium dihydrogen phosphate (KDP), β-barium borate (BBO), potassium titanyl oxide phosphate (KTP), and compound semiconductors such as gallium arsenide (GaAs) and InP.

In the following analysis, I assume a fixed linear polarization and a single spatial mode of the electric field. Under these conditions, the electric field can be treated as a scalar quantity. This simplification is justified, as the effective electro-optic response along the field direction is sufficient to model changes in the refractive index. Since the refractive index does not strongly depend on the electric field E, this dependency can be expanded in a Taylor series at $E = 0$:

$$n(E) = n + a_1 E + \frac{1}{2} a_2 E^2 + ... \tag{3.1}$$

It is convenient to re-write the formula above in terms of the so-called electro-optic coefficients $\kappa = \frac{-2a_1}{n^3}$ and $\chi = \frac{-a_2}{n^3}$, so:

$$n(E) = n - \frac{1}{2}\kappa n^3 E - \frac{1}{2}\chi n^3 E^2 + ... \tag{3.2}$$

The higher order terms can be neglected due to low values in comparison to n. Media for which the third term is negligibly small in comparison to the second one are called the Pockels media, and the κ is the linear electro-optic coefficient. For centrosymmetric materials the first term in eq. (3.2) vanishes, then material is known as the Kerr medium and the coefficient χ as the Kerr coefficient. Optical properties of crystals can be described with a geometrical construction called index ellipsoid:

$$\sum_{i,j} \eta_{ij} x_i x_j = 1, i, j = 1, 2, 3, \tag{3.3}$$

where η_{ij} are the components of the impermeability tensor:

$$\boldsymbol{\eta} = \epsilon_0 \epsilon^{-1} \tag{3.4}$$

The elements of that tensor will be changed differently upon application of a static electric field E. The resultant phase change is therefore dependent on the input light polarization and the orientation of the crystal with respect to the direction of the elctric field.

3.1.2 Electro-optic phase modulator

Electro-optic phase modulators (EOPMs) are devices that utilize the Pockels effect. Pockels media (or Pockels cells) are preferred over Kerr media for phase modulation because the Pockels effect is stronger. When an electric field E is applied to a cell of length L, it induces a phase shift in the propagating light beam given by:

$$\phi = \phi_0 - \pi \frac{\kappa n^3 E L}{\lambda_0}, \tag{3.5}$$

where λ_0 is the free space wavelength of the beam, and ϕ_0 is a phase offset. The electric field can be applied by changing the voltage at the electrodes separated by a distance:

$$E = \frac{V}{d}. \tag{3.6}$$

The voltage required to introduced a phase shift of π is called the half-wave voltage V_π, and is given by:

$$V_\pi = \frac{d}{L} \frac{\lambda_0}{\kappa n^3}. \tag{3.7}$$

The resultant phase shift can be written as:

$$\phi = \phi_0 - \pi \frac{V}{V_\pi}. \tag{3.8}$$

Originally, phase modulators were constructed using bulk crystals and electrodes to induce phase delay, with the separation between electrodes requiring voltages of up to several kilovolts. Modern devices, however, use waveguides with precisely shaped electrodes, resulting in smaller form factors that enable fiber compatibility and photonic integration [100]. Today, phase modulators are essential building blocks offered by PIC foundries. While bulk modulators are typically made from lithium niobate, photonic integrated technologies often utilize indium phosphide. Recently, however, thin-film lithium niobate has emerged as a promising platform for photonic integrated circuits, marking a shift in the field [101].

The modulation frequency of electro-optic phase modulators is limited by the electrical capacitance and the time it takes for light to propagate through the material. EOPMs are driven by high-speed voltage signals at frequencies reaching tens of gigahertz. Transit-time effects, which arise from the mismatch between the velocities of the traveling optical wave and the driving electrical signal, can be mitigated through careful electrode design. Key parameters describing the EOPM are:

- insertion loss (IL) - loss of power due to propagation through the component (dB),
- V_π - specified for DC and sometimes also RF voltage at 1 GHz (V),
- 3dB bandwidth - frequency for which power of the driving signal drops by a factor of 2, corresponding to the maximal range of practical modulating signal frequencies.

Typically, EOPMs are built as 50 Ω impedance systems. The maximum tolerable optical and electrical power must be carefully considered to avoid permanent damage. Proper alignment of the crystal with the input light's polarization is often achieved through fiber coupling with polarization-maintaining (PM) fibers. Selecting the correct polarization of the input beam is crucial to achieving high modulation depth.

3.1.3 Electro-optic amplitude modulator

The electro-optic amplitude modulator (EOAM) can be build by placing an EOPM in an arm of an interferometer. This can be clearly visualized on the Mach-Zehnder modulator (MZM) example. The mode of operation is dependent on the position of the phase modulating cell (DC bias or RF drive) [102]. By placing it in one of the arms a typical single-rail intensity modulator is obtained. Placing the phase-modulating elements in both arms allows for push-pull operation. EOAMs are also equipped with electrodes for setting the phase with DC voltage to establish an operating point. Typical architectures are presented in Fig. 3.1. The modulators

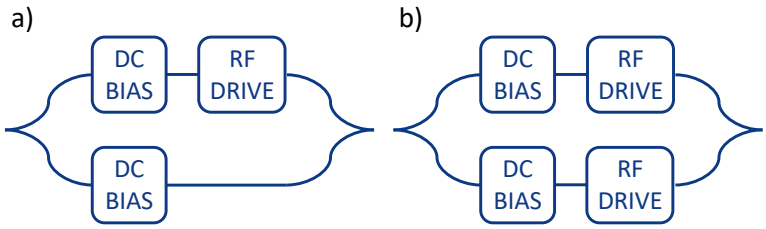

Figure 3.1: MZM modulator architectures. a) Single-rail modulator: fast phase modulation is applied to one of the optical paths. b) Push-pull modulator: fast phase modulation of opposite sign is applied to both arms simultaneously.

are usually driven using one of the two operating points: minimum/maximum transmission point or quadrature point (see Fig. 3.2). Using the minimal transmission point is preferred for driving with return-to-zero (RZ) electrical signals. This point is favorable for QKD systems due the fact that light from the carrier wave is suppressed and optical pulses with high extinction can be generated. The downside is a necessity to use the non-linear part of the transmission curve. The point of minimal transmission has to be precisely localized and adjusted with respect to the exact voltage range of the driving RF signal. The resultant optical pulse may also be chirped and its shape different from the shape of the driving electrical signal. Alternatively, non-return-to-zero

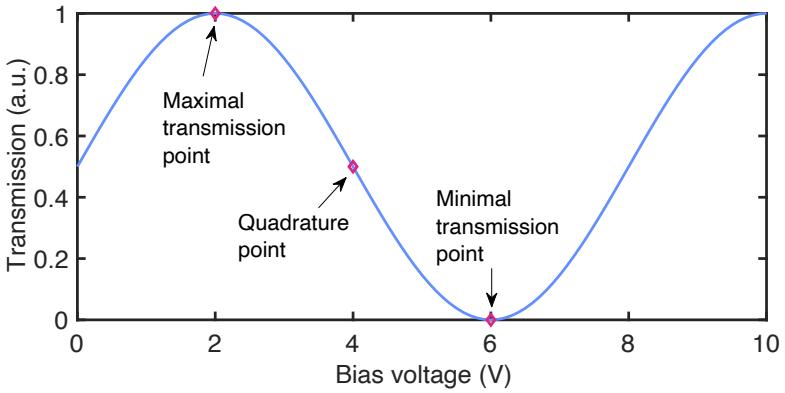

Figure 3.2: Working points of an exemplary MZM.

(NRZ) signals can be used to drive the intensity modulator biased for the quadrature point. This technique allows using the linear part of the transmission curve and mitigate the chirp, but results in residual light leak and requires tuning and controlling two phase shifters instead of one.

Furthermore, phase and intensity modulators can be combined to create an IQ modulator used for classical QAM-based optical communication [3] and CV QKD. All of the aforementioned modulators are available as building blocks within generic photonic integration technology. One of the key parameters describing the EOAM is the extinction ratio (ER, in dB), a ratio between output optical powers when modulator is in the maximal ($P_{\max}$) and minimal transmission ($P_{\min}$) state, given by:

$$ER = 10\log_{10}(\frac{P_{\max}}{P_{\min}}). \tag{3.9}$$

The extinction ratio is limited due to imperfect splitting ratio of the used couplers. Extinction ratio values higher than 35 dB are achievable, and are sufficient for classical and quantum applications. The transmission of a MZM in a perfect case is:

$$T(V) = \frac{I_{\text{out}}}{I_{\text{in}}} = \cos^2(\frac{\phi_0}{2} - \frac{\pi}{2}\frac{(V_{\text{DC}} + V_{\text{RF}})}{V_\pi}). \tag{3.10}$$

Assuming that input electric field E_{in} is split by a coupler with an amplitude splitting ratio k and two independent voltages V_1, V_2 are used to change the phase in the two arms of the MZM and the initial phase ϕ_0 is 0, the complex output electric field reads:

$$E_{\text{out}} = \frac{E_{\text{in}}}{2}((1+k)e^{j\frac{\pi}{2}\frac{V_1}{V_\pi}} + (1-k)e^{j\frac{\pi}{2}\frac{V_2}{V_\pi}}). \tag{3.11}$$

The transmission of a MZM in an imperfect case is equal to:

$$T(V) = (\frac{\sqrt{1-k}+\sqrt{1+k}}{2})^2\cos^2(\frac{\pi(V_1+V_2)}{2V_\pi}). \tag{3.12}$$

Another limitations is the maximal tolerable range of voltages or currents which can be used for biasing the modulator without causing damage. The modulators also exhibit drift over time, and require correction of the transmission to go back to the desired operating point. The point can be established and monitored using feedback loop comprising either a beam splitter, power

meter and a bias control, or a build-in photodiode and bias control. The stability of the selected point depends on the stability of the temperature and the technique of biasing. Temperature change alters the phase of the interferometer, and thus shifts the transmission of the modulator. Avoiding too fast and too big DC bias voltage (or current) changes helps to find the desired working point accurately and ensure stability for longer, as verified experimentally (results are presented in the Chapter 6 of the thesis).

3.2 High-speed electrical signal generation

Both amplitude and phase modulators are driven by high-speed electrical signals. The use of high-frequency electronic bandwidth introduces various imperfections, some of which can significantly affect the properties of the resultant signal or even cause physical damage to the components. In the following section, I describe the principles of signal generation and propagation.

3.2.1 RF signal propagation

Electro-optic modulators are typically driven by high-speed RF signals to modulate the amplitude or phase of the light propagating through them. Real-world systems often require the use of fast signal generators, amplifiers, cables, and attenuators to match the properties of the driving signals with those of the modulators. This results in complex networks comprising components with different amplitude and phase transfer functions, which can significantly alter the properties of the signals. One of the most effective ways to describe the properties of such networks is through scattering parameters, or S-parameters. S-parameters provide a convenient means of analyzing signal propagation and reflection [103]. While they can be applied to n-port networks, for simplicity, I will focus on a two-port network. Using scattering parameters requires terminating the system with a characteristic impedance, typically 50 Ω. These parameters are represented in an S-matrix [104], which can be measured using a vector network analyzer (VNA). The S-parameters are:

- S_{11} - forward reflection coefficient (input port reflection),
- S_{12} - backward transmission coefficient (reverse gain),
- S_{21} - forward transmission coefficient (forward gain/insertion loss),
- S_{22} - backward reflection coefficient (output port reflection).

Describing a system of cascaded 2-port networks requires converting S-matrices to transfer, or T-matrices. The corresponding components of the T-matrix can be obtained via:

$$T_{11} = S_{12} - \frac{S_{21}S_{11}}{S_{21}}. \tag{3.13}$$

$$T_{12} = \frac{S_{11}}{S_{21}}. \tag{3.14}$$

$$T_{21} = -\frac{S_{22}}{S_{21}}. \tag{3.15}$$

$$T_{22} = \frac{1}{S_{21}}. \tag{3.16}$$

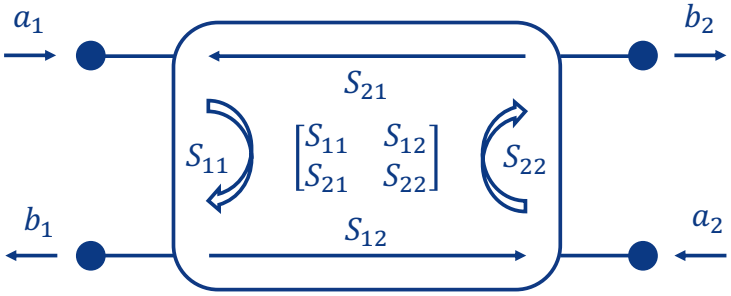

Figure 3.3: S-parameter matrix of a two-port RF device. The matrix describes properties of a RF network in terms of incident (a_1, a_2) and reflected (b_1, b_2) power waves

The resultant T-matrix of a system comprising m elements is given by:

$$T = T_1 \times T_2 \times T_3 \times ... \times T_m \tag{3.17}$$

The T-matrix can then be used to calculate the S-parameter, which determines the final complex transfer function of the RF system [105]. For a system with matched impedances, this is simply given by the S_{21} coefficient. The effect of a complex transfer function is illustrated in Fig. 3.4.

Proper impedance matching and reliable performance in high-frequency electronic systems depend significantly on the condition and handling of RF connectors and cables. Visual inspections often reveal debris, physical damage, or wear on connectors, interfaces, and threads—factors that can compromise signal integrity. When contaminants are present, cleaning is typically performed using isopropanol applied with dust-free cotton swabs, followed by compressed air to remove residues. Care must be taken to prevent alcohol from entering the connectors, and protective gloves are commonly used to avoid transferring oils that might alter impedance characteristics. Maintaining cleanliness and preventing cable strain are essential for preserving connector integrity. Unused interfaces are generally covered with plastic caps to guard against contamination. Connectors are typically secured using calibrated torque wrenches, ensuring they are tightened to manufacturer-specified torque values, which vary by connector type. In systems involving multiple RF connection standards, performance is often optimized by selecting purpose-built cables over adapters, helping to minimize voltage standing wave ratio (VSWR). However, when adapter use is unavoidable, it is generally considered safer to pair a narrower male pin with a broader female pin to reduce the risk of mechanically stressing or deforming the connector.

3.2.2 Arbitrary waveform generation

The Arbitrary Waveform Generator (AWG) is a universal tool for generating RF signals, which further can be used for driving the electro-optic modulators or as triggering signals for other devices. It typically offers a variety of input and output channels serving different purposes. The clock reference sets the time basis for the main FPGA board and determines the sampling frequency. The inverse of the sampling rate corresponds to the duration of one sample, which is further degraded by the finite analog bandwidth. Finite bandwidth limits rising and falling times, effectively increasing the duration of electrical pulses. The clock drives the bit pattern generator, which can produce a series of 0s and 1s of a length up to the maximum size of the memory. The memory size is a power of 2, and data can be uploaded in chunks of a fixed size, referred to as granularity. One drawback of using an AWG is that waveform generation begins at a random time relative to the internal clock reference. This necessitates determining all delays

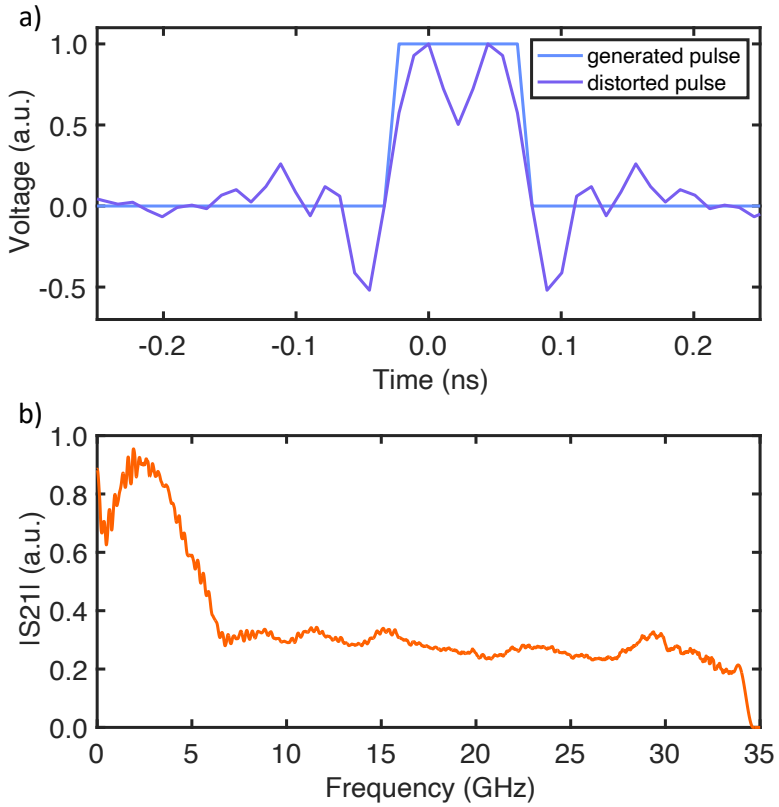

Figure 3.4: Influence of a complex transfer function. a) A 100 ps-wide rectangular RF pulse as generated and after propagation through a RF network comprising an Arbitrary Waveform Generator (AWG) and an amplifier. b) Magnitude of the S_{21} coefficient.

each time the experiment is cold-started. The specific model used in the experiments featured "data" channels for arbitrary waveforms and "marker" channels that output binary signals only. The "marker" channels were synchronized with the "data" channels, enabling the calibration of delays in the experimental setup to be performed just once. However, a finite delay, known as "skew", always exists between channels. This skew can be compensated for during waveform design. The AWG uses a digital-to-analog converter (DAC) to adjust the resulting voltage values corresponding to each bit of data in the data channel. When designing waveforms, the following factors must be considered:

- The first and last sample values must not create a sudden change in output voltage; otherwise, the waveform will be distorted, resulting in an undesired shape.
- The number of points in the waveform must be an integer multiple of the granularity and smaller than the maximum number of samples allowed per channel.
- The sampling frequency and total length must be adjusted to achieve the desired repetition frequency.

An example of correct and incorrect signal generation is shown in Fig. 3.5. As mentioned in the

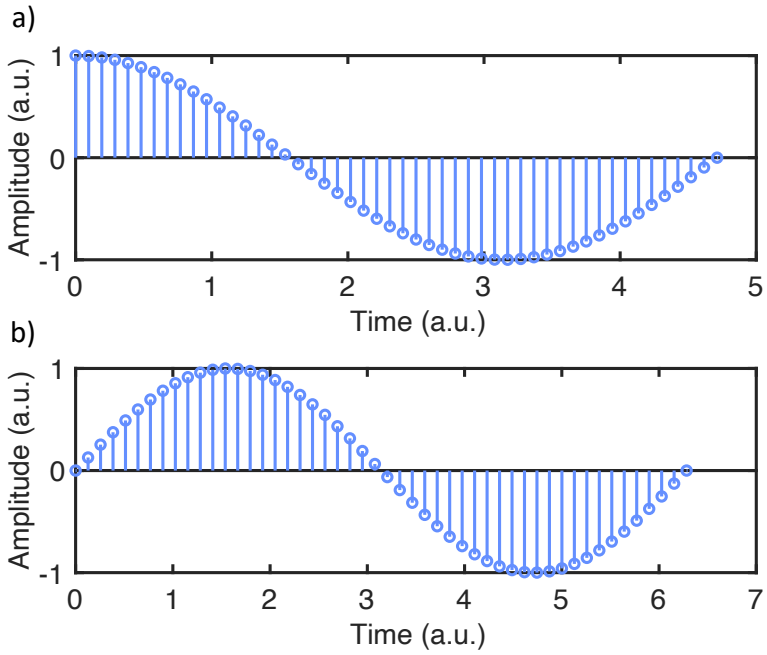

Figure 3.5: Arbitrary waveform generation. a) Incorrect choice of waveform length. Amplitude values for first and last samples are very different, which will result in a rapid amplitude jump causing distortion. b) Correct selection of waveform length.

previous section, every signal is affected by the transfer function of the RF network, including that of the AWG itself. The technique of precompensation can be applied during the design process to achieve the desired pulse amplitude and shape. Furthermore, the AWG's transfer function can sometimes be adjusted using internal filter settings.

3.3 Time-correlated single photon counting

Single-photon signals are measured using single-photon detectors, but the detection events must be processed by precise timing electronics to enable data analysis. In this section, I discuss key technical aspects of single-photon detectors and time-correlated measurements.

3.3.1 Single photon detectors

Single-photon detectors (SPDs) are essential components in a wide range of modern scientific and technological applications, including QKD, light detection and ranging (LiDAR), fluorescence lifetime imaging, and astronomical observations. SPDs can be categorized into the following types:

- Single photon avalanche photodiodes (SPADs),
- Superconducting nanowire single photon detectors (SNSPDs),
- Transition edge sensors (TES),

- Photomultiplier tubes (PMTs).

These detectors have vastly different internal properties. Key figures of merit include:

- Dark count rate (DCR): an internal property of the detector. It is a measured rate of single photon counts while no optical power is present at the input.
- Afterpulsing: a phenomenon in which the detector registers additional false counts following a legitimate photon detection event,
- Dead time: the time interval the detector spends in its recovery state, and is effectively blind to incoming photons.
- Quantum efficiency: percentage of incident photons that are successfully detected and converted into electrical signals.
- Timing jitter: temporal uncertainty of the photon detection event.

For quantum cryptography applications, SPADs and SNSPDs are the most commonly used detectors. The selection of the detector primarily depends on the link attenuation (link length) and the number of detection channels required for the experiment. SPADs are semiconductor-based detectors widely recognized for their efficiency and cost-effectiveness in single-photon detection, particularly within the near-infrared (NIR) spectral range. SPADs leverage the avalanche multiplication effect, where an incoming photon generates electron-hole pairs in the semiconductor. This process triggers an avalanche of charge carriers, resulting in a detectable electrical signal. SPADs operate in Geiger mode, where the semiconductor junction is biased slightly above the breakdown voltage. In this state, the arrival of a photon can initiate an avalanche of electrons. After the avalanche is triggered, a specialized quenching circuit reduces the bias voltage below the breakdown level, stopping the avalanche and rendering the SPAD temporarily insensitive to incoming light. However, residual carriers trapped in the semiconductor can trigger a secondary avalanche, leading to afterpulsing. Once the avalanche is quenched, the excess bias is restored, allowing the SPAD to resume photon detection. The semiconductor nature of SPADs also makes them well-suited for photonic integration, offering further advantages in terms of scalability and application in advanced photonic systems. Another advantage is low dependency of the detection efficiency on the light's polarization. However, they have inherit limitations stemming from their mode of operation. The SPADs typically offer quantum efficiencies $< 30\%$, dead times $> 10\mu s$, DCR < 1000 Hz (depending on quantum efficiency) and jitter $> 150ps$ at temperature of $-50°$C. Stiriling-cooled SPAD versions are able to opearate in lower temepratures (down to $-90°$C) resulting in lower DCR. All these factors are closely interrelated, making it essential to prioritize the key parameters based on the specific requirements of the experiment to achieve optimal performance.

SNSPDs offer significantly better performance compared to SPADs. Their operation is based on the superconducting properties of nanowires. The entire measurement system typically consists of a cryostat containing the detectors, an electronic driver, a vacuum pump, and a helium compressor. The nanowires are cryogenically cooled to approximately 2.5 K and biased close to their critical current. When an incident photon strikes, it adds energy and disrupts the superconducting state, creating a resistive hotspot. During this disturbance, the current flows through a cryogenic amplifier connected in parallel, generating a detectable voltage pulse. In the meantime, the detectors are cooled down again and superconductivity is brought back enabling the detection of the next photon. Quantum efficiency in SNSPDs is often enhanced by applying anti-reflective coatings to the optical windows between the nanowires and the input optical fibers.

Consequently, the efficiency becomes wavelength-dependent, with values exceeding 80%. Polarization dependency arises from the intrinsic structure of the nanowires, and various designs are available to mitigate this effect. For polarization-dependent systems input polarization can be optimized with a polarization controller by monitoring the count rates, which can reach several MHz. SNSPDs generally exhibit dead times greater than 10 ns, DCR below 200 Hz, and timing jitter under 20 ps. Such performance makes them the detectors of choice for demanding applications, including long-range communications and links with parallel channels [59]. However, their practical use is constrained by factors such as system size, high cost, and the requirement for annual maintenance.

It is important to highlight that all detectors should be characterized prior to building a deployable QKD system in order to recognize the influence of parasitic effects on the quantum bit error rate and estimate the basis detection efficiency mismatch. Parasitic factors can be extracted from the measured countrate. The conutrate without detector's DCR is:

$$R_{\text{nodcr}} = R_{\text{measured}} - \text{DCR} \tag{3.18}$$

The countrate without detector's dead time τ is given by:

$$R_{\text{nodeadtime}} = \frac{R_{\text{measured}}}{1 - \tau R_{\text{measured}}}. \tag{3.19}$$

Correction for quantum efficiency η_{det} can be calculated as:

$$R_{\text{real}} = \frac{R_{\text{measured}}}{\eta_{\text{det}}}. \tag{3.20}$$

Applying the aforementioned corrections enables precise determination of the mean photon number of incoming signals, which is crucial for the security of QKD systems. Detailed guidelines for characterizing detectors can be found in the ETSI recommendations [106].

3.3.2 Time tagger

Output signals from the detectors are registered with the time taggers. The time taggers record the exact time of arrival of individual photon detection events with high temporal precision, enabling time-correlated single photon counting techniques (TCSPC). Time taggers are essentially time-to-digital converters (TDCs) implemented using field-programmable gate arrays (FPGAs). These devices are designed to provide precise timestamping by converting the arrival times of signals into digital values. Incoming signals are passed through delay lines or tapped circuits made of logic gates, which divide time into fine intervals. A stable reference clock is employed to establish a consistent time base across the system. The position of each signal within these intervals is digitized, often using advanced techniques such as thermometer coding or interpolation [107]. Upon the arrival of the signal, a delay of the arrival with respect to the reference clock is used to create the timestamp. Key parameters of the time taggers are:

- Digital resolution: measurable time interval between two consecutive events that the system can distinguish and record.
- Jitter: temporal uncertainty of registering an event.
- Dead time: interval during which the device is unable to record events.
- Processing capabilities: number of channels, data transfer rate, maximal input signal frequency.

High accuracy can be achieved by employing low-jitter clock signals, using high-quality FPGA hardware with uniform propagation delays through logic gates, calibrating the time tagger, and setting trigger levels at half the amplitude of the input signal's slope. The range of voltages of detection signals can vary and must be individually adjusted based on the detectors used. Precise adjustment of the detection threshold is vital not only for reducing jitter but also for eliminating false count rates caused by electrical signal ripples.

3.3.3 Timing jitter

Timing jitter refers to the uncertainty in determining the precise time of arrival of a signal. Physically, it can be defined as the deviation from the ideal periodicity of a signal. It can be directly measured using the setup illustrated in Fig. 3.6. In a histogram measurement, jitter appears as a broadening of the pulse. To evaluate the jitter of a detection system, which includes a single-photon detector and a time tagger, one can record a histogram of a signal with a duration significantly shorter than the expected jitter value [106].

In the setup shown in 3.6, a femtosecond laser was used to generate an optical pulse with a full width at half maximum (FWHM) of less than 100 fs. The pulse's spectrum was reduced using a 4f filter, and short optical fibers were utilized to minimize the impact of dispersive broadening. The pulse was then attenuated to the single-photon level, and a histogram was recorded over one minute at the time tagger's maximum digital resolution of 1 ps. An electrical synchronizing signal was first generated using the femtosecond laser's internal photodiode and was subsequently used as a clock input for the AWG. The AWG then produced a final 10 MHz, low-jitter, high-quality reference signal for the time tagger. The resulting histogram, shown in Fig. 3.7, indicates a pulse with an FWHM of 35 ps (15 ps RMS). This value represents the timing jitter of the detection system and was subsequently used in further experiments and simulations.

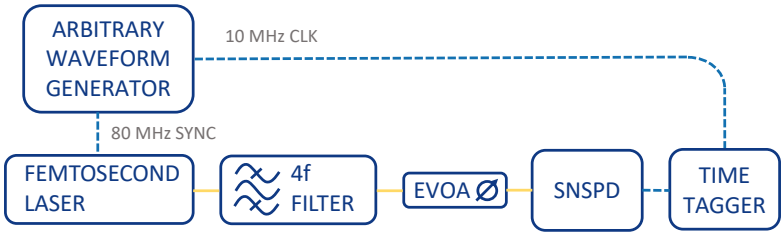

Figure 3.6: Setup for jitter measurement. Jitter is pronounced in the width of the histogram of an attenuated short optical pulse generated with a spectrally-controlled femtosecond laser.

Individual sources of jitter can be modeled with Gaussian distributions of certain widths. Their total effect on the timing uncertainty is represented by the convolution of their individual distributions. For Gaussian distributions, the resultant RMS jitter σ_{total} can be obtained using the widths of n individual distributions as follows [108]:

$$\sigma_{\text{total}} = \sqrt{\sigma_1^2 + \sigma_2^2 + ... + \sigma_n^2}. \tag{3.21}$$

The RMS values of Gaussian distributions can be converted to FWHM values using the following formula:

$$FWHM = 2\sqrt{2\ln 2}\,\sigma \approx 2.3548\,\sigma. \tag{3.22}$$

Simulated effect of pulse broadening due to timing jitter is illustrated in Fig. 3.8:

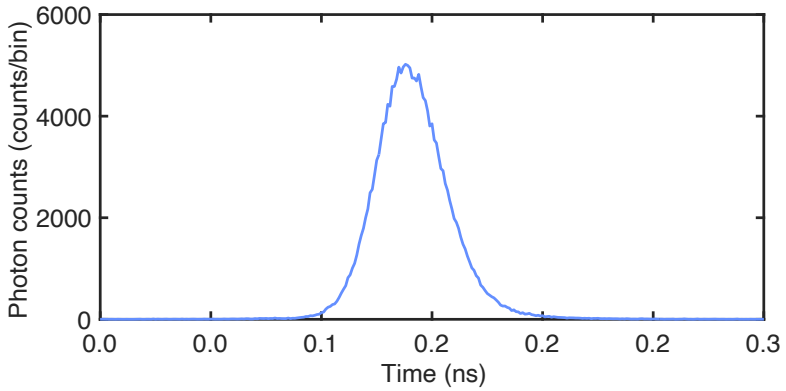

Figure 3.7: Femtosecond laser pulse histogram representing detection jitter measured with the time tagger and a superconducting detector.

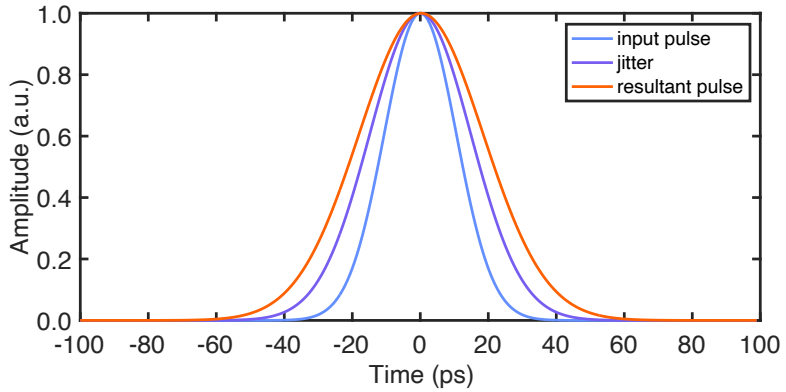

Figure 3.8: Simulated broadening of a measured pulse due to timing jitter: a 25 ps-wide pulse broadens to 43 ps as a result of 25 ps timing jitter.

3.4 Dispersive Fourier Transformation

Spectrally-resolved single-photon level signals can conveniently be measured using the properties of chromatic dispersion. In this chapter, I detail the use of commercially available dispersive media and numerical methods to predict the properties of pulses characterized through frequency-to-time mapping.

3.4.1 Chirped fiber Bragg grating

Dispersion can be introduced by fiber Bragg gratings (FBGs), which consist of periodic variations in the refractive index within the fiber core. A non-uniform refractive index distribution can be achieved using chirped fiber Bragg gratings (CFBGs) [109]. These structures act as mirrors, selectively transmitting and reflecting certain wavelengths. The reflected wavelength, known as the Bragg wavelength λ_B, depends on the effective refractive index of the core n_{eff} and the period of the refractive index variation Λ:

$$\lambda_B = 2\Lambda\ n_{\text{eff}}. \tag{3.23}$$

Unlike uniform FBGs, which reflect a narrow range of wavelengths with a fixed delay, CFBGs can reflect a broader spectrum [110]. In CFBGs, longer wavelengths are reflected from regions with a larger grating period, while shorter wavelengths are reflected from regions with a smaller grating period. This unique property enables precise control over the dispersion profile [111], making CFBGs highly versatile. The principle of operation is displayed in Fig. 3.9. When com-

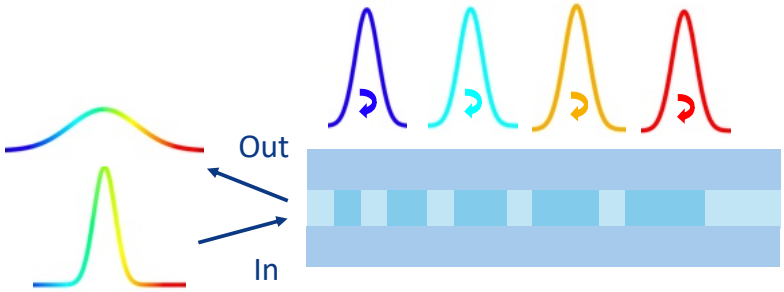

Figure 3.9: CFBG principle of operation.

bined with optical circulators, CFBGs form a dispersion compensating module (DCM), which is designed to mitigate the effects of material dispersion in optical fibers. These modules are highly effective for compensating dispersion over specific propagation distances, ensuring better signal quality in optical communication systems. A DCM offers significant dispersion and relatively low insertion loss, making it an excellent tool for measuring single-photon spectra using frequency-to-time mapping. One DCM can replace the dispersion of several hundred kilometers of standard single-mode fiber (SMF), which would otherwise result in prohibitively high losses. A setup for measuring single-photon spectra is shown in Fig 3.10. Polarizing beam splitters (PBS) and fiber polarization controllers can be incorporated to optimize transmission or enable a double-pass configuration. In the double-pass setup, the effective dispersion is doubled, but this comes at the cost of increased losses. This configuration is achieved by adjusting the polarization controllers so that light exiting the DCM re-enters the input PBS through the second arm, completing a second pass through the module before measurement.

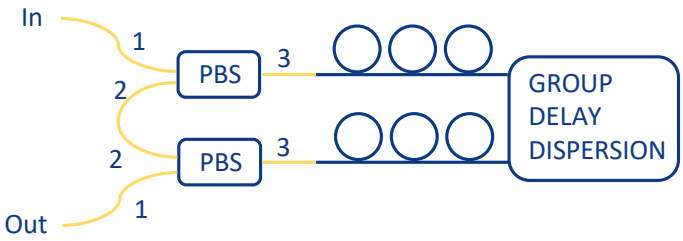

Figure 3.10: Dispersive spectrometer for measuring single-photon signals spectra. Setup can be adjusted for single-pass or double-pass configuration to enable using more dispersion for analyzing pulses of various temporal widths.

3.4.2 Pulse broadening

Propagation of an optical pulse through a dispersive medium is governed by a nonlinear Schrödinger equation [112]:

$$\frac{\partial a}{\partial z} = \frac{j\zeta}{2}\frac{\partial^2 a}{\partial t^2} - j\gamma|a|^2 a, \tag{3.24}$$

where a is a complex field envelope, ζ group velocity dispersion (GVD) coefficient and γ a nonlinearity coefficient. This equation can be efficiently solved numerically using the split-step Fourier method. In this approach, the linear and nonlinear components of the propagation problem are addressed independently: the nonlinear terms are evaluated in the time domain, while the linear terms are processed in the Fourier domain. The computational efficiency of this method is enhanced by employing the fast Fourier transform algorithm to transition between the time and frequency domains. The procedure typically begins with an initial field defined at $z = 0$. The Fourier transform of the initial field is computed as:

$$A(0, \tilde{\omega}) = \int dt\, a(0, t) \exp(-j\tilde{\omega}t). \tag{3.25}$$

Dispersion effects over a small propagation step Δz are introduced in the frequency domain using:

$$A_D(\Delta z, \tilde{\omega}) = A(0, \tilde{\omega}) \exp\left(-j\zeta\tilde{\omega}^2 \Delta z/2\right). \tag{3.26}$$

The field is then transformed back to the time domain via an inverse Fourier transform:

$$a_D(\Delta z, t) = \frac{1}{2\pi}\int d\tilde{\omega}\, A_D(\Delta z, \tilde{\omega}) \exp(j\tilde{\omega}t). \tag{3.27}$$

Nonlinear effects occurring over the same distance Δz are incorporated through the expression:

$$a(\Delta z, t) = a_D(\Delta z, t) \exp\left(-j\gamma|a_D(\Delta z, t)|^2 \Delta z\right). \tag{3.28}$$

This output field serves as the updated input for the next iteration of the method. By repeating this sequence for successive steps, the propagation dynamics can be simulated over the desired spatial range. Since the split-step method neglects the noncommutative behavior of the dispersion and nonlinearity operators, it introduces some error. To minimize this error to an acceptable level, it is necessary to choose a sufficiently small step size Δz. Simulated Gaussian pulse broadening calculated using split-step Fourier method for different dispersions is shown in Fig. 3.11. It was used for all simulations and data analysis in this thesis. Pulse width measurements are influenced by timing jitter. The precise impact of the jitter on the measurement error will be discussed in the next section. For a transform-limited Gaussian pulse the width can be analytically calculated using [99]:

$$\tau = \tau_0 \sqrt{1 + \left(\frac{\lambda^2 D}{\pi c_0 \tau_0^2}\right)^2}, \tag{3.29}$$

where τ_0 is an input pulse FWHM duration, D is the dispersion parameter in ns/mm, λ is a central wavelength and c_0 speed of light in vacuum. Pulse chirp α and amplitude A_{out} change according to [99]:

$$\alpha = -\frac{\left(\frac{\lambda^2}{c}\right) D}{\pi\, \delta\tau^2}, \tag{3.30}$$

$$A_{\text{out}} = \frac{A_{\text{in}}}{\sqrt{1 - i(\alpha)}}. \tag{3.31}$$

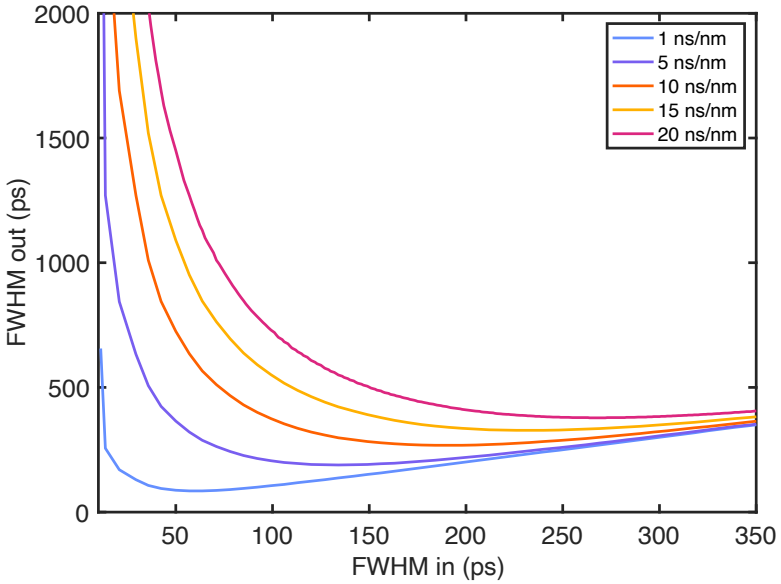

Figure 3.11: Gaussian pulse broadening simulated using split-step Fourier method. Output FWHM was calculated for different dispersion equivalent D and input FWHM values.

Chapter 4

Photonic integrated circuit as a platform for symbol generation

The goal of this thesis is to develop a quantum key distribution link using high-dimensional encoding. Building a setup that supports high-dimensional encoding presents significant challenges due to the large number of photonic components required [113]. To enhance robustness and applicability, photonic integration offers a promising solution. In this chapter I present accurate control of temporal and spectral profiles of optical pulses generated at the telecom wavelengths using an indium phosphide-based photonic integrated circuit. The device enables simultaneous temporally and spectrally resolved measurements using single photon counting. First, I explain the concept of generating high-dimensional symbols in time and frequency. Next, I describe the architecture of the application-specific photonic integrated circuit (ASPIC) and the experimental setup, including guidelines for handling PICs and the necessary procedures. Finally, I present characterization results of key components and the outcomes of the experiments. The outcomes of this work are the result of a collaborative effort between the Quantum Photonics Laboratory (QPL), led by dr Michał Karpiński at the University of Warsaw, and the research group led by dr hab. inż. Ryszard Piramidowicz at the Institute of Microelectronics and Optoelectronics (IMiO), Warsaw University of Technology. I initiated the collaboration, contributed to the conceptual design of the experiments, and was responsible for device characterization and final quantum measurements. The IMiO team designed and fabricated the chip within the MPW process and provided critical expertise essential for conducting the measurements. The results of this work were published in the Journal of Lightwave Technology [114].

4.1 Precise control and symbol generation

One of the recently introduced QKD protocols is the time-frequency protocol [115, 116, 117, 118, 77], which can be seen as a quantum counterpart to PPM and FSK, where these two encodings serve as complementary bases. This approach to cryptographic key exchange is particularly appealing due to its compatibility with spatial, free-space, and fiber-optic communication technologies. Additionally, it allows efficient encoding using high-dimensional quantum states (symbols) [119, 120]. The advantage of employing high-dimensional quantum states lies in their enhanced resistance to noise [53] in the communication channel and the ability to transmit more than one bit of information per photon [113, 121].

To demonstrate and validate precise control, I aimed to encode bits of information in either

the central frequency or the time of arrival of photons. This method facilitates the use of M-dimensional quantum states, enabling the transmission of $\log_2 M$ bits of information per symbol. It was anticipated, that the security of this protocol can be derived from the inherent time-frequency uncertainty [122]. An additional motivation behind this investigation was to assess the feasibility of achieving precise signal generation and control using generic photonic integrated circuits.

When the pulse parameters are chosen such that states from the two non-orthogonal bases overlap, any information will be lost if a measurement is made in the incorrect basis [123]. The relationships between the spectral or temporal FWHM (δf or δt) and the spectral or temporal separations (Δf or Δt) of Gaussian-shaped photon profiles are as follows:

$$\delta f \approx \sqrt{\ln 2}\Delta f, \tag{4.1}$$
$$\delta v \approx M\delta f, \tag{4.2}$$
$$\delta t \approx \frac{0.441}{\delta v}, \tag{4.3}$$
$$\Delta t \approx \frac{\delta t}{\sqrt{\ln 2}}, \tag{4.4}$$
$$\delta \tau \approx M\sqrt{\ln 2}\Delta t. \tag{4.5}$$

where δv and $\delta \tau$ are FWHMs of symbols measured in the complementary basis. A four-dimensional scheme ($M = 4$) is utilized, allowing each symbol to encode two bits of information per photon, as illustrated in Fig. 4.1.

Table 4.1: PPM and FSK Parameters for $M = 4$

Symbol	**Quantity**	**Target value**
δf	Spectral symbol FWHM	3.08 GHz
Δf	Spectral symbol separation	3.70 GHz
$\delta \tau$	Spectral symbol FWHM in the time domain	143 ps
δv	Temporal symbol FWHM in the frequency domain	12.32 GHz
δt	Temporal symbol FWHM	36 ps
Δf	Temporal symbol separation	43 ps

The efficiency of the protocol increases with the dimensionality of the quantum state. However, its performance is constrained by factors such as the electrical bandwidth and timing jitter. Additionally, the spectral widths and separations required to ensure protocol security impose further limitations on the photon source and receiver architecture, as shown in Table 4.1. The parameters are based on a spectral separation of $\Delta f = 3.70$ GHz, which corresponds to the measured resolution of the dispersive spectrometer that was used in the experiment for detecting symbols, and represents the minimum spacing between the FSK symbols.

4.2 Chip architecture

The core component of the transmitter setup is a photonic integrated circuit designed and fabricated using the n+ multi-project wafer (MPW) process provided by the SMART Photonics foundry [100]. The indium phosphide platform enables the realization of highly complex systems through monolithically integrated active and passive waveguiding components. Although InP

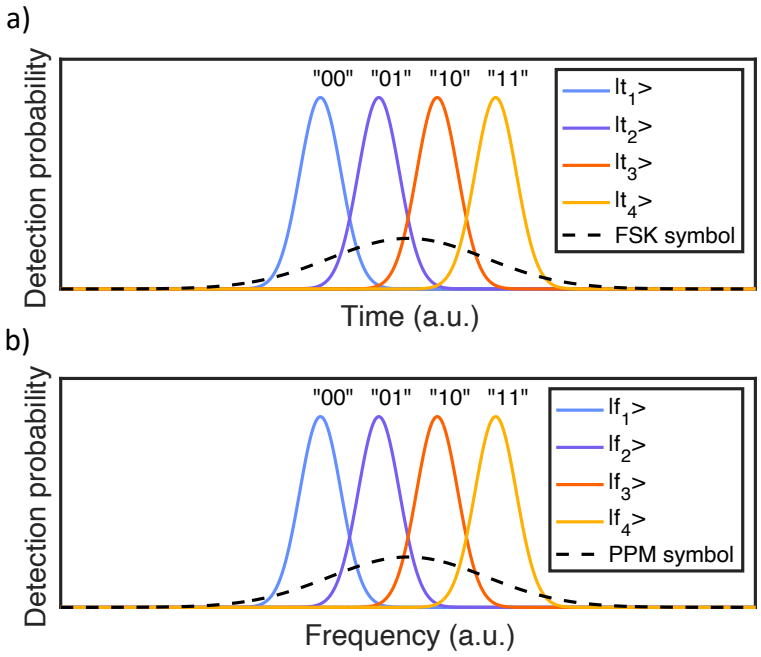

Figure 4.1: Four-dimensional FSK symbols. The security stems from the fact that when a temporal (PPM) symbol is measured in the frequency basis, the resulting probability distribution spans the entire range of the FSK symbol set.

waveguides exhibit higher losses compared to their silicon counterparts, they offer a significant advantage by allowing the integration of active components such as lasers, modulators, and photodiodes, which enables the realization of complex transmitter architectures. The schematic of the designed photonic integrated transmitter is shown in Fig. 4.2, and a microscope image of the chip is presented in Fig. 4.3.

The transmitter utilizes a matrix of four distributed Bragg reflector (DBR) lasers with a nominal wavelength of $\lambda_1 = 1561.80\,\text{nm}$, adjusted to match the spectral parameters of the receiver. All components are interconnected using passive waveguides with an attenuation coefficient of 2 dB/cm. A 2×2 matrix of 3 dB multi-mode interference (MMI) couplers enables signals from all four sources to be injected into a single output waveguide. This waveguide is connected to a cascade of three MZMs and an output EOPM, which are controlled by both DC and RF electrical signals. The MZMs also have additional optical outputs connected to PIN photodiodes (responsivity $R = 0.85\,\text{A/W}$) with DC interfaces. These photodiodes allow monitoring of the output power and setting the operating points for all modulators. Additionally, the circuit can generate a clock signal at a nominal wavelength of $\lambda_2 = 1529.79\,\text{nm}$, with power several orders of magnitude higher than the λ_1 channels. To achieve this, the transmitter includes an additional DBR laser and MZM. Both the quantum and clocking signals are coupled into a common output waveguide using a 2×2 MMI coupler. The properties and operation of the on-chip components is described in detail in the following sections.

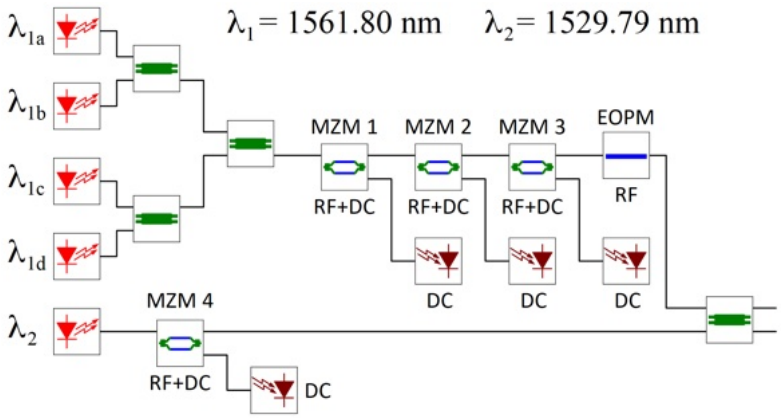

Figure 4.2: The functional schematic of the application-specific-photonic integrated-circuit (ASPIC)-based transmitter. MZM – Mach-Zehnder modulator, EOPM – electro-optic phase modulator, DC – direct current electrical interface, RF – radio-frequency electrical interface.

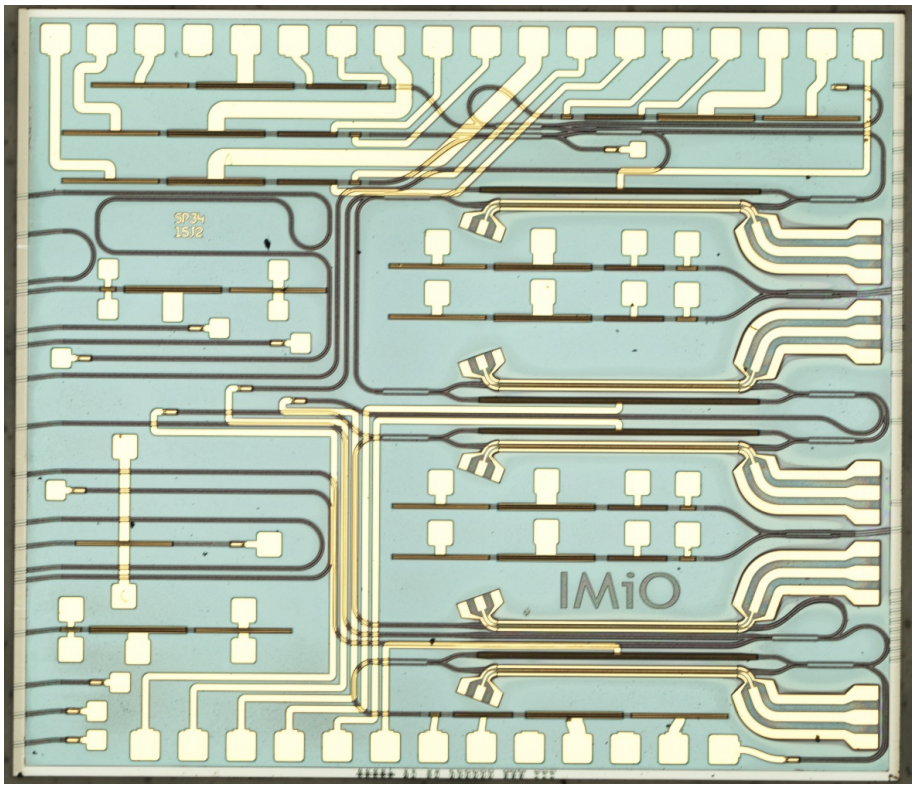

Figure 4.3: Microscope image of a InP photonic integrated circuit (4.6mm × 4.0mm) provided by the SMART Photonics foundry.

4.3 Probing, handling, and interposing the ASPIC

After the fabrication, the ASPICs were inspected with the microscope for visual sings of damage. Prior to main measurements, the chip was placed on a TEC-controlled table and characterized

with DC and RF probes in laboratory conditions 4.4 a). This is a crucial step for verification of correct operation of all the on-chip components, which is necessary before bonding (or packaging) in order to reduce the risk of failure.

Operating with a PIC requires careful handling and adherence to safety measures due to its fragility. The indium phosphide material is particularly delicate, and any mechanical damage to the edges can result in self-propagating cracks or self-cleaving of the chip. It is important to note that PICs are typically finished through a grinding thin-down process, leaving the final substrate thickness at approximately 200 μm. Both the waveguides and metallic components on the surface are extremely fragile, so contact with hard objects—even plastic tweezers—is strictly prohibited. Releasing chips from a Gel-Pak box requires the use of a vacuum releaser. The vacuum releaser reforms the gel surface, allowing the chips to be gently freed from the gel. A separate vacuum pen is then used to pick up the chip and move it to the desired location. Only a proper Gel-Pak vacuum releaser and vacuum pen should be used when handling PICs. Any mechanical contact with the optical input or output edges can easily damage the waveguides and degrade their optical properties, as these edges are typically coated with high-reflection (HRC) or anti-reflection (ARC) coatings. Electrostatic discharge (ESD) protection is essential when handling PICs. Always ensure the ground connection is established first and disconnected last, and wear appropriate protective clothing, such as ESD wrist straps and ESD-safe shoes. Electrical charges can accumulate in the capacitive components, leading to accidental discharges with voltages or currents exceeding the damage threshold. An example of damage caused by accidental discharge is shown in Fig. 4.4 b). The damage typically appears as a crack on the glass, which can break the waveguide or sever electrical tracks, rendering the entire PIC non-functional. Scratches on

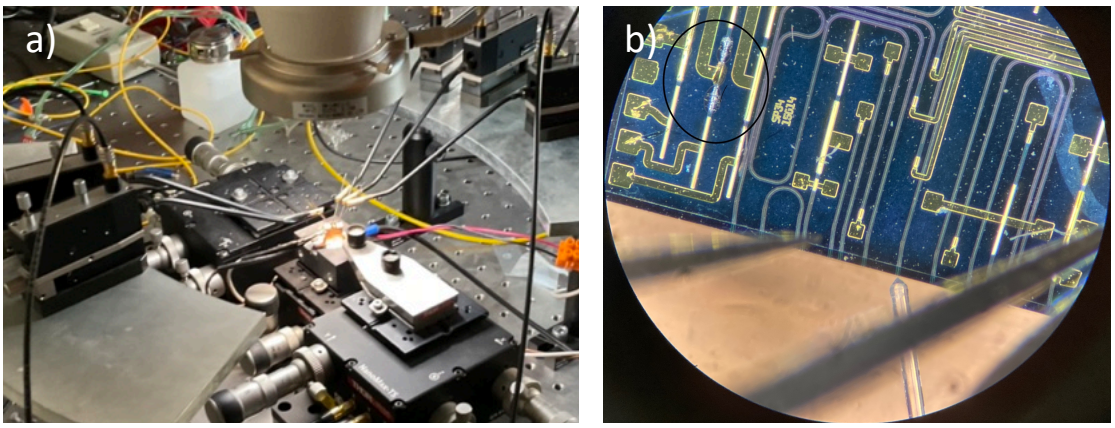

Figure 4.4: Characterizing PIC with probes. a) Probing station. b) Microscope image showing damage of an on-chip laser due to electrostatic discharge. The damaged section is enclosed with a black circle, and appears as a crack in the glass.

the golden pads are expected as natural wear of the material. Dust particles can be removed using a gentle blow from an air duster, but this should only be done when absolutely necessary to avoid additional risks.

The selected ASPIC was mounted on a custom-designed printed circuit board (PCB) to provide a convenient interface for both RF and DC connections to the on-chip active photonic elements [4.5]. Additionally, this setup ensured mechanical stability, which was essential for coupling optical signals into an external optical fiber. Wire bonding was used for all the DC and RF interfaces, supporting bandwidths exceeding 10 GHz.

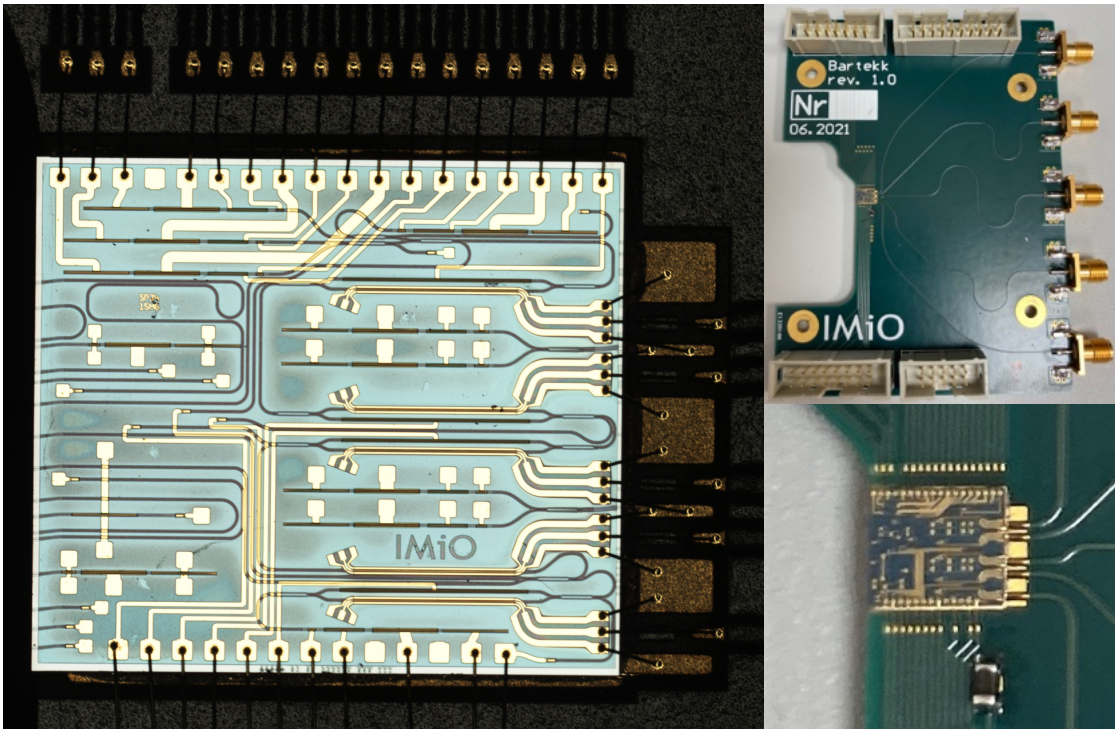

Figure 4.5: A PIC mounted on a PCB interposer (7cm × 12cm) and connected using ball-bonding. The PCB interposer allows for easy access to the RF and DC interfaces and improves mechanical stability of the layout.

4.4 Component characterization

The precise generation and detection of FSK symbols with the desired properties require meticulous control of several factors, including temperature, laser supply current, the voltage applied to modulators, and synchronization between the transmitter and receiver. Another critical factor is the electrical bandwidth, which limits the minimum pulse duration and may impact the channel capacity. Due to statistic nature of manufacturing [124], exact characterization of all the components is necessary for precise operation. In this part of the thesis I demonstrate properties of on-chip components and methods of characterizing them to display chip capabilities for generating symbols feasible for quantum communication.

4.4.1 IVL measurements

IVL measurement, which stands for current-voltage-luminescence measurement, is a technique used to characterize semiconductor devices, particularly light-emitting components such as lasers. This method involves simultaneously measuring the electrical properties (I-V) and optical output (L) of the device as a function of the driving current. Non-emitting components can be characterized by a simplified IV (current-voltage) measurement. IVL and IV measurements serve as an excellent health check for semiconductor components because the shape of the curves (I-V and L-I) is characteristic of their expected behavior. Deviations from the typical shape can indicate issues such as material defects, improper fabrication, or degradation of the component over time.

It also allows to determine the lasing threshold and mode hopping of a laser device. The lasing threshold is the point at which the device transitions from spontaneous emission to stimulated emission, marking the onset of coherent light output. An unexpected change of power may be an early indicative of mode hopping. Moreover, IVL measurements can also be utilized to determine the static and dynamic impedance of a semiconductor device. The static impedance of a semiconductor gain medium describes its electrical resistance in a steady-state condition, where no rapid variations or time-dependent signals are present. It reflects the medium's opposition to a constant (DC) or gradually changing current or voltage. The dynamic impedance of a semiconductor gain medium refers to its electrical impedance when subjected to time-varying signals, such as alternating currents (AC) or modulated inputs. Unlike static impedance, which describes the response under steady-state conditions, dynamic impedance characterizes the medium's behavior under small-signal or high-speed operating conditions. Dynamic impedance is a key parameter for designing and optimizing semiconductor gain media for high-speed operation, e.g. for gain switching with fast-changing current pulses. Below the lasing threshold, dynamic impedance is dominated by carrier recombination and junction capacitance. Above the lasing threshold the impedance changes due to the saturation of carrier density and increased optical gain. Knowledge about the lasing threshold is critical for security of QKD systems where symbols are generated by means of gain switching. Reducing the current below the threshold allows to randomize the phase between consecutive key generation rounds. Precise control of current can be used for imposing phase difference and realizing encoding with optical injection locking technique (OIL) [125]. Gain switching can also be used for constructing quantum random number generators (QRNG) [126].

4.4.2 On-chip laser

The on-chip distributed feedback laser (DFB) is constructed by combining the following building blocks: a semiconductor optical amplifier (SOA), front and back Bragg reflectors, and a phase shifter. In this section, I will introduce these components and show the results of characterization.

The semiconductor optical amplifier is a device similar to a semiconductor laser. SOAs are active optical components that amplify an input optical signal through stimulated emission [127]. They are typically designed as waveguide structures, where the optical signal is guided through a gain medium under electrical injection. A forward current bias is used to control the stimulated emission rate, and consequently, the gain. In the context of on-chip lasers, SOAs are positioned between Bragg gratings and a phase shifter. A combination of spontaneous emission and current injection in the resonator enables sustainable lasing action. The output power of the laser is directly influenced by the intensity of the driving current. Key performance metrics for an SOA include noise figure, gain, saturation output power, and polarization dependency. Proper thermal management is essential to ensure reliable operation and to mitigate the risk of damage from overheating.

Bragg reflectors are formed by periodic variations in the refractive index of the semiconductor waveguide. They act as wavelength-selective reflectors, providing feedback necessary for laser oscillation [128]. Bragg reflectors are placed in front and behind the SOA to form an on-chip laser. The period of the grating can be changed with forward current bias. Tuning the grating allows to tune the length of the resonator and thus the wavelength of the laser.

Phase shifters introduce a controllable phase delay to the optical signal propagating through a waveguide. This is typically achieved by varying the refractive index of the waveguide material. The refractive index can be adjusted using the thermo-optic effect, electro-optic effect, or changes in carrier concentration. Precise phase adjustment is crucial for stable lasing, fine wavelength tuning, and mode selection, although mode hopping may still occur. In the case of SMART

Photonics generic technology, a reverse voltage bias is used to tune the phase shifter.

The general structure of the laser is presented in Fig. 4.6. The DBR laser is available as a building block in the PDK. The SOA, Bragg reflector, and phase shifters are also available as separate building blocks.

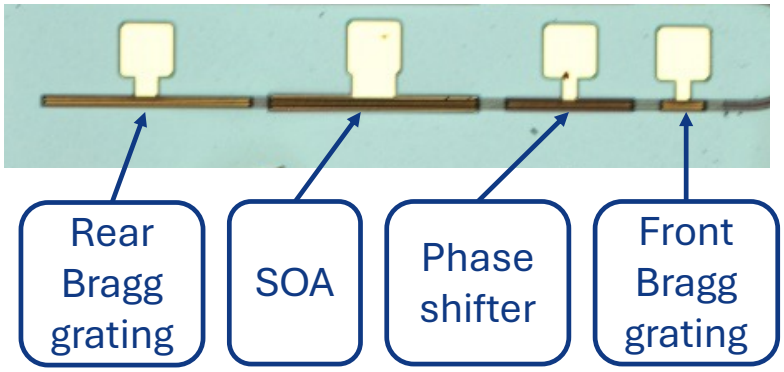

Figure 4.6: Structure of an on-chip DBR laser. The laser is formed by surrounding the SOA with Bragg reflectors and a phase shifter.

Exemplary spectra of the DBR laser are shown in Fig. 4.7 The spectrum may have significant side-peaks, which can be eliminated by either tuning the SOA driving current, tuning Bragg gratings or the phase shifter.

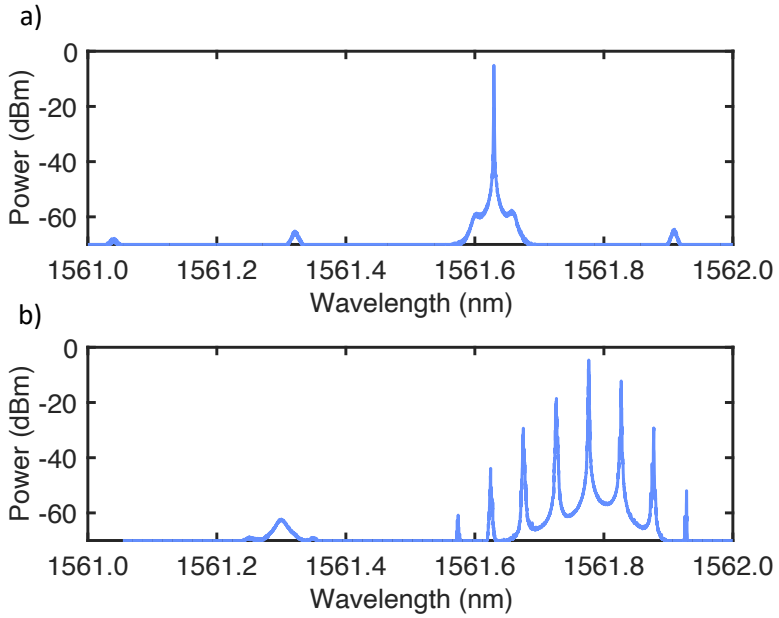

Figure 4.7: Exemplary measured DBR laser spectra. a) A single-mode laser with high side mode suppression ratio. b) The same laser showing multimode structure due to different SOA driving current.

The influence of temperature and SOA current on the central wavelength is illustrated in Fig. 4.8.

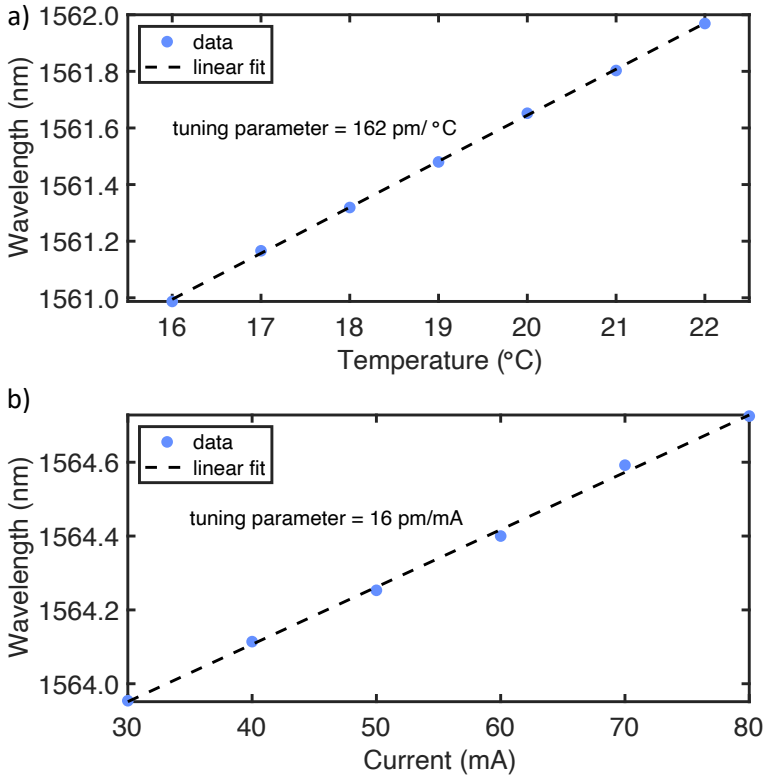

Figure 4.8: Temperature and current tuning of central wavelength.

Exemplary IVL measurement is presented in Fig. 4.9. The lasing threshold is approximately $30 - 35$ mA for the on-chip lasers. The corresponding static and dynamic impedance plots are

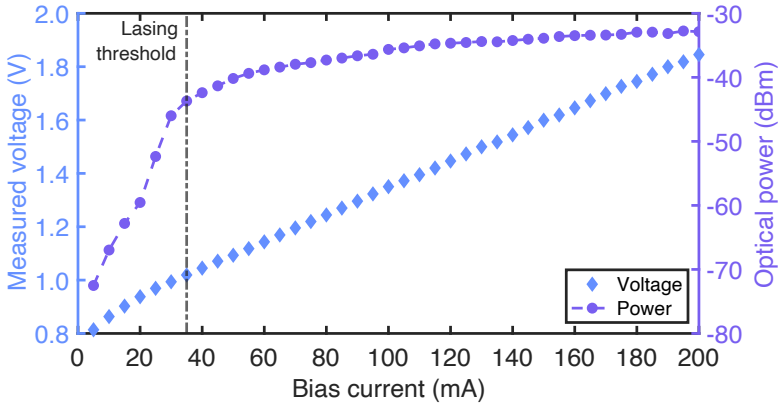

Figure 4.9: IVL curve of the DBR laser.

shown in Fig 4.10 and 4.11.

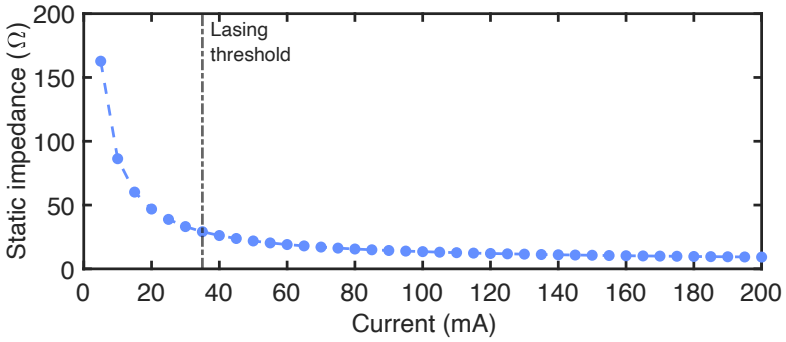

Figure 4.10: Static impedance.

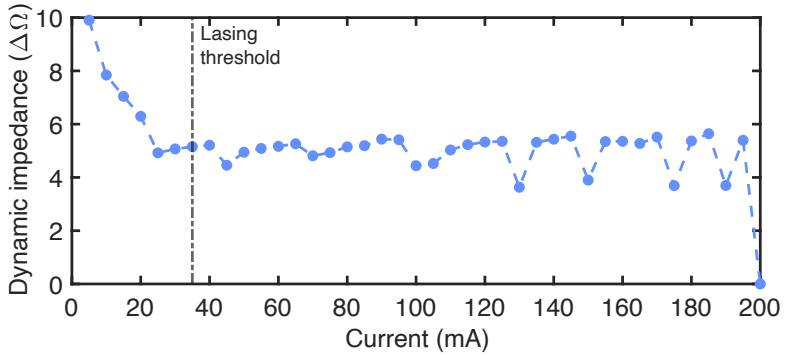

Figure 4.11: Dynamic impedance.

The stability of the DBR laser's central wavelength was measured using a heterodyne optical spectrum analyzer (Apex AP2681A). It could be further improved by hermetic packaging of the laser module. Packaged PICs show greater stability and allow user-friendly access to the control pins, but increase the lead time and price of the ASPICs. Packaging is beyond the scope of this experiment. For a packaged laser, the central wavelength fluctuation would be reduced to 2 pm.

Wavelength tuning with the front Bragg grating is shown in Fig. 4.12 The rear Back grating can be used in a similar fashion, as illustrated in Fig. 4.13. In this particular case, mode-hopping phenomenon is exposed as a sudden change in the central wavelength. The laser's spectral line shape and central wavelength can also be adjusted with the phase shifter, as shown in Fig. 4.14:

4.4.3 On-chip modulators and photodiodes

On-chip Mach-Zehnder modulators are constructed using 1×2 or 2×2 MMI couplers, along with slow (DC) and fast (RF) phase shifters. The 2×2 variant allows for switching the output port, and therefore it may act like a tunable beam splitter. Additionally, the 2×2 MMI coupler offers advantages such as reducing on-chip light scattering and reflections, which could otherwise destabilize laser operation. Photonic-integrated MZMs can operate in both single-rail and push-pull configurations. While the modulators are available as building blocks within the PDK, their

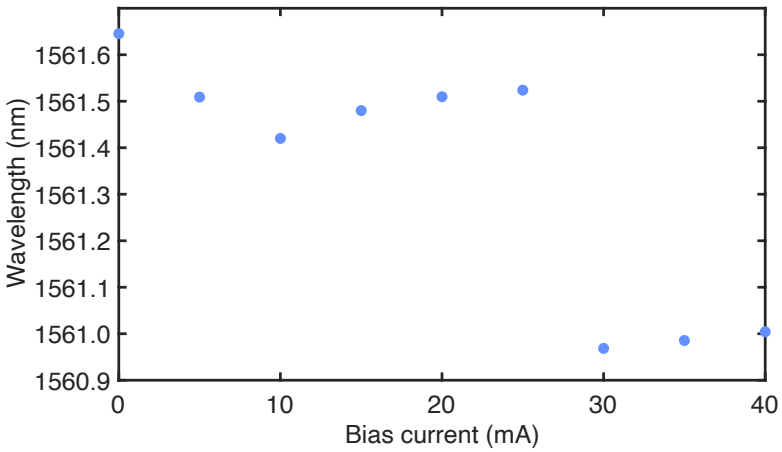

Figure 4.12: Front Bragg grating current tuning

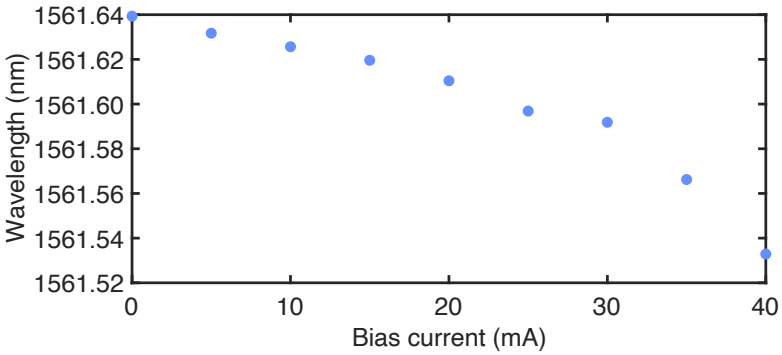

Figure 4.13: Rear Bragg grating current tuning.

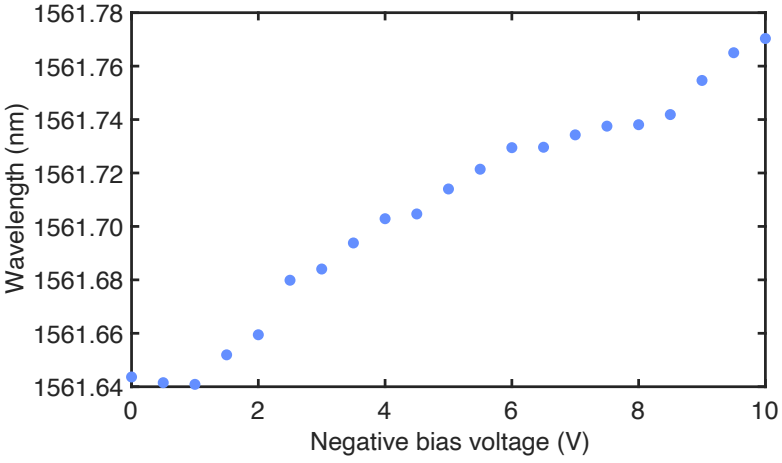

Figure 4.14: Wavelength tuning with a phase shifter.

individual parameters must be carefully adjusted for specific applications. For instance, altering the modulator's length impacts both the bandwidth and the V_π, but at the cost of increased footprint and changes to the properties of the high-speed RF tracks. The design of traveling wave electrodes must also be tailored to the intended application. Signal lines can be configured as signal-ground (SG) or ground-signal-ground (GSG). The SG configuration is simpler to fabricate and requires less chip area, whereas the GSG setup provides superior electromagnetic shielding, ensuring impedance matching and signal integrity, which is critical for demanding applications. The characteristic impedance of the modulators is 50 Ω, ensuring compatibility with commercial driving and testing electronics. In SMART Photonics generic technology, a reverse voltage bias is employed to tune and drive the modulators. The general operating principles are consistent with those described in Chapter 3. The maximum safe negative bias voltage for SMART Photonics modulators is -10 V. Exceeding this limit can damage the gold electrical pads or the modulator structure. In semiconductors, excessive bias voltage can also introduce electroabsorption as a dominant mechanism, leading to an exponential non-permanent reduction in transmission and modulation depth. Exemplary transmission curve of the InP MZMs is presented in Fig. 4.15.

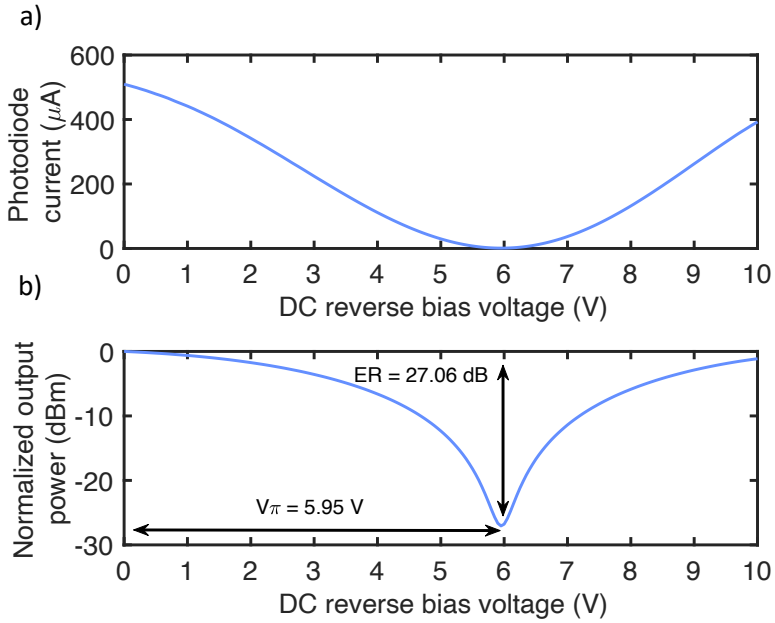

Figure 4.15: Measured transmission curve of an on-chip MZM. a) Photocurrent as a function of reverse bias voltage measured with an on-chip photodiode. b) Normalized output power obtained from the measured photocurrent assuming responsivity of 0.85 A/W.

Modulators are typically used in tandem with PIN photodiodes, which serve as key components in photonic integrated circuits. The SMART Photonics foundry offers high-performance PIN (p-type, intrinsic, n-type) photodiodes. When operated under a reverse bias voltage of -2 V, these photodiodes achieve a responsivity in the range of $0.8-0.9$ A/W. Increasing the reverse bias voltage can further enhance sensitivity, but this must be done within safe operating limits (-5 V) to prevent potential damage. The SMART Photonics PIN photodiodes support both DC and RF operation. A general structure of an on-chip MZM with a photodiode is shown in Fig. 4.16.

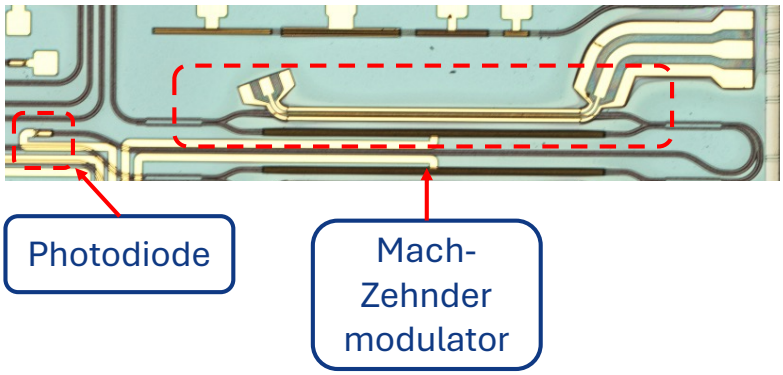

Figure 4.16: Structure of an on-chip MZM and a photodiode. The MZM is formed by combining two 2×2 couplers and placing electrically-controlled phase shifter in either one or both arms of an interferometer.

4.5 Experimental setup

Experimental setup is presented in Fig. 4.17. Thermal stability is ensured by mounting the PCB, which houses the photonic PIC, onto a Peltier module placed on a heat sink. The temperature is regulated using a TEC module, enabling simultaneous wavelength tuning of all lasers. The on-chip DBR lasers are driven and finely tuned by precisely controlling the current injected into their gain sections. The measured performance of the DBR lasers (λ_{1a}–λ_{1d}) is similar, with threshold currents ranging from 30 to 35 mA. The output power is approximately 1.5 mW for lasers $1a$, $1b$, and $1d$, while laser $1c$ has a slightly lower output power of 0.8 mW, which remains suitable for this application. Tuning a single laser via temperature and current was sufficient to generate FSK symbols, although it was also confirmed that two lasers could be tuned simultaneously using these methods. The DBR lasers are equipped with current-driven Bragg reflectors and phase shifters, which enable additional fine-tuning of the central wavelength. Electro-optic amplitude modulation is introduced to generate the FSK symbols.

The temperature and laser driving current were adjusted to achieve the desired central wavelengths. The spectra were measured using a high-resolution optical spectrum analyzer (Apex AP2681A) with a resolution of 0.05 pm/5 MHz. The MZMs were biased using a precise DC power supply (Keysight E36313A). Since indium phosphide technology requires negative voltage signals, electrical signal levels were adjusted with bias tees and amplified with a RF amplifier to match the modulators' half-wave voltage (V_π) levels. The MZMs were driven by a high-speed arbitrary waveform generator (AWG, Keysight M8196A). Four DBR lasers and two cascaded MZMs were used to generate approximately Gaussian optical pulses with the desired temporal widths and wavelengths. Additionally, another DBR laser, operating at 1533.022 nm, and an MZM were used to generate the optical synchronization signal required for measuring the time of arrival of single photons. In the integrated transmitter, both the synchronization and data signals were transmitted through a common waveguide and coupled from the chip to an external lensed fiber with a coupling loss of 4˘5 dB, which is typical for this configuration [129]. Finally, the two signals were separated by splitting the beam evenly and applying a 40 dB bandpass filter. Experimental verification confirmed that this filtering approach effectively suppressed the strong synchronization pulses, even when both signals operated within the C-band. Sensitive superconducting single-photon detectors were used, and no further crosstalk effects were observed during the experiment. The weak data signal did not interfere with the synchronization stream

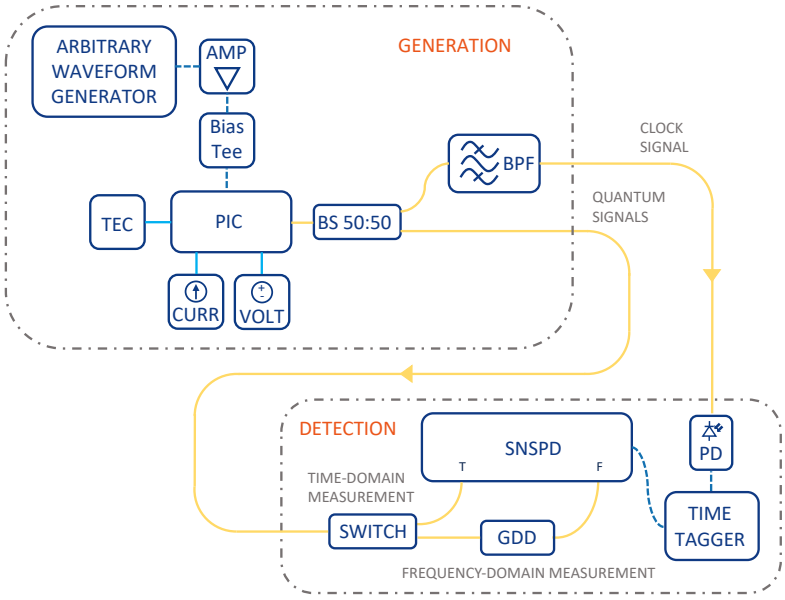

Figure 4.17: The schematic of the experimental setup. The ASPIC, which integrates multiple DBR lasers and MZMs, is used for generating optical pulses with specific widths, separations and approximately Gaussian shape. It is mounted on a PCB (see Fig. 4.5) and controlled by external laboratory equipment, represented by blue boxes: an arbitrary waveform generator (AWG), RF amplifier (AMP), thermo-electric controller (TEC), current source (CURR), and voltage source (VOLT). Yellow lines represent optical fibers, and blue lines denote electrical connections. The PCB functions as a submount, ensuring efficient multi-channel RF and DC interfacing, and includes a thermistor for temperature monitoring. The optical pulses can be measured in either the time or frequency domain. For frequency-domain measurements, the pulses pass twice through a dispersion-compensating module based on a chirped fiber Bragg grating (CFBG). In both cases, the pulses are analyzed using time-of-arrival histograms, with the photodiode signal serving as the time reference.

due to its low power. Synchronization was achieved using 250 ps-wide rectangular pulses at a repetition rate of 80 MHz.

On the receiver side, optical synchronization signals were converted into electrical triggering signals for the time tagger (PicoQuant HydraHarp 400) using a photodiode. The measurement basis—either time of arrival or spectrum—was selected manually by reconnecting the fibers to transmit optical signals either directly or through a chirped fiber Bragg grating (CFBG)-based dispersion compensation module. Pulses were characterized by measuring time-of-arrival histograms using low-jitter ($\sim$ 5 ps root mean square, RMS) niobium-nitride superconducting nanowire single-photon detectors (SingleQuantum, 70% quantum efficiency, dark count rate $<$ 1000 counts per second) and a time tagger with jitter as low as 10 ps RMS. This resulted in a total system jitter of approximately 11 ps RMS. For time-domain analysis, the histograms represented the probability distribution of detecting a photon within a specific temporal bin. Spectral measurement was achieved by stretching the pulse in time using a medium with a well-known dispersion, effectively creating an approximate time-to-frequency mapping as described in Chapter 3.

4.6 Symbol generation and detection

A cascaded fast electro-optic amplitude modulation technique was employed to address the challenge of generating short optical pulses satisfying parameters given in table 4.1. Satisfying those relations is necessary for implementing spectral-temporal encoding scheme. Modulators were driven by electrical sine waves and rectangular pulses. The MZMs were biased for minimal transmission using feedback signals from the on-chip PIN photodiodes. This approach minimized light leakage through the modulators, which would otherwise increase noise during single-photon regime measurements. It also enabled the generation of optical pulses shorter than the electrical bandwidth would typically allow. An additional MZM was used as a variable optical attenuator to reduce the optical signal power to the single-photon level. This setup could also be conveniently adapted to implement the decoy state method [95]. The measured extinction ratios of the three cascaded MZMs were 27 dB, 25 dB, and 21 dB, respectively, resulting in a total extinction ratio of 73 dB. Detailed modulation method is presented in Fig. 4.18. The first Mach-Zehnder modulator was driven by a sinusoidal signal, resulting in an optical signal with a doubled frequency. Frequency doubling occurs due to the fact, that negative voltage also increases the transmission of the modulator, according to eq. 3.12. To ensure proper information encoding and accurate pulse characterization in the single-photon regime, only one pulse per clock cycle could be generated. To achieve this, the second MZM was used as an optical gate. It was driven by a rectangular pulse, allowing the selection of a single optical pulse per clock cycle. As a result, an approximately Gaussian-shaped optical signal was generated. To control the timing, both electrical driving signals were time-shifted relative to the synchronization signal from the AWG. This setup enabled temporal pulse shifting with a resolution of 1 ps. To manipulate the temporal—and consequently the spectral—width, sine waves and rectangular pulses of varying frequencies and widths were used. For the FSK symbols, a 2 GHz sine wave and a 250 ps-wide rectangular pulse were applied. The simulated dependency of the resultant FWHM on the frequency of the driving sine wave is shown in Fig. 4.19. Electro-optic amplitude modulation was employed to generate the FSK symbols. The temperature and laser driving current were adjusted to achieve central wavelengths of 1562.581 nm, 1562.550 nm, 1562.513 nm, and 1562.484 nm. These spectra were measured using a high-resolution optical spectrum analyzer.

The histogram's widths, shapes, and locations on the time axis were analyzed to evaluate the performance and estimate their applicability in a time-frequency QKD system. Spectral pulses in the time domain were very uniform, Gaussian, and indistinguishable, which was necessary to ensure the erasure of information in the case of a measurement in a wrong basis. In the frequency domain, the pulses were distinguishable, allowing assigning bits of information (Fig. 4.21). The FWHM durations and separations are given in Table 4.2 The measured temporal widths align with the expected 143 ps, while the separations are around 1 ps, which corresponds to the maximum digital resolution of the time tagger. As a result, the pulses can be considered indistinguishable in the time domain. In the frequency domain, the symbols were slightly broader than anticipated but remained clearly distinguishable, with separations close to the target value of 3.70 GHz. The single-photon pulses were successfully characterized in both the PPM and FSK bases, despite the trade-offs imposed by experimental limitations. The generation and characterization of PPM symbols demonstrated precise control over setup timing. To achieve the desired FWHM widths and separations, an additional commercial lithium niobate MZM (Thorlabs LNA6213), operating at speeds up to 40 GHz, was employed. This modulator was used to generate short rectangular gating electrical signals, as the ASPIC lacked sufficient bandwidth. All PPM symbols were generated at a fixed wavelength. The expected and measured parameters are summarized in Table 4.3. Measured histograms exhibit an approximately Gaussian distribution of the single-photon optical signals (Fig. 4.22). Unfortunately, measuring spectrum of

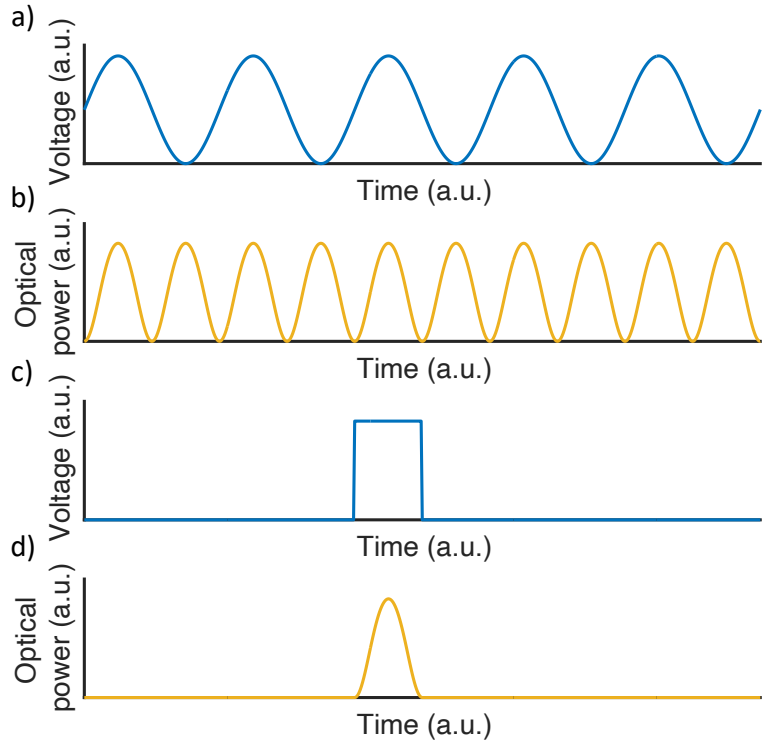

Figure 4.18: The electrical signals driving the MZMs and the corresponding optical outputs are illustrated. (a) The first MZM is driven by an RF sine wave and configured for minimal transmission. (b) This produces an optical sine wave signal with a frequency twice that of the RF driving signal. (c) A rectangular pulse drives the second MZM, selecting a single lobe of the optical sine wave signal. (d) As a result, one approximately Gaussian-shaped optical signal is generated per clock cycle.

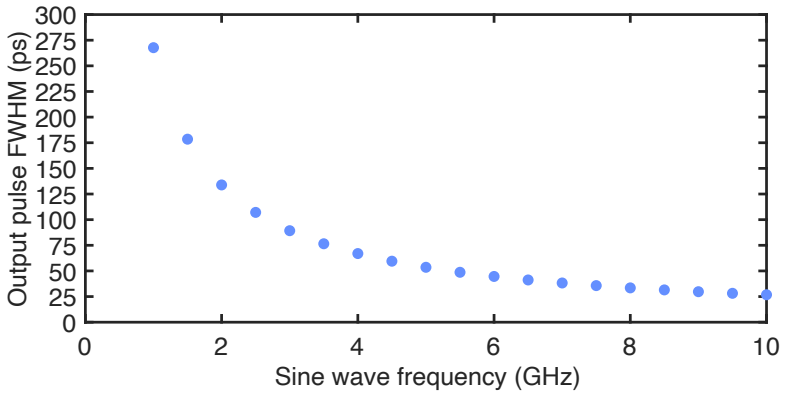

Figure 4.19: Simulated temporal full-width at half maximum (FWHM) of the output pulses as a function of the driving RF sine wave frequency.

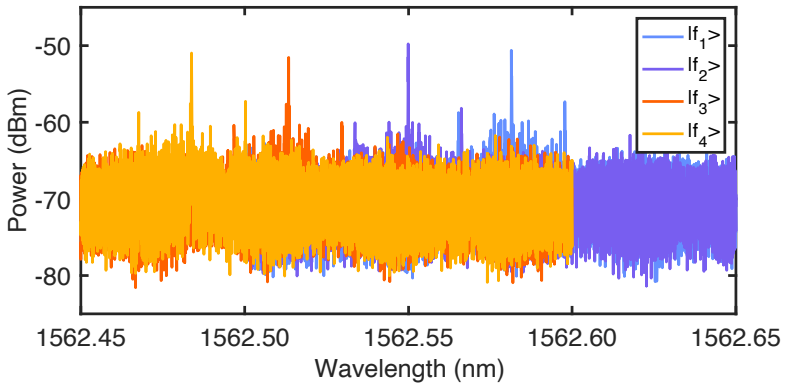

Figure 4.20: Spectra of FSK symbols measured in the classical light regime. The high noise level is due to losses caused by multiple MZMs used for carrier wave modulation.

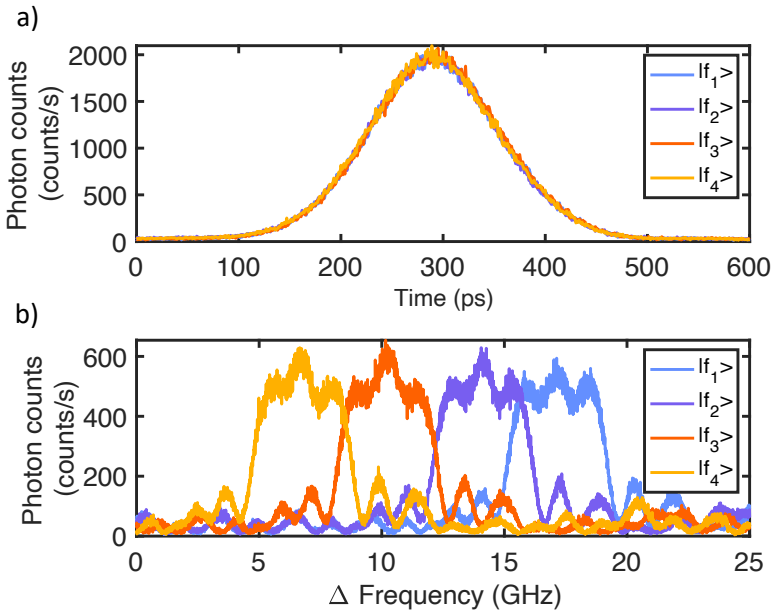

Figure 4.21: Histograms of spectral symbol's arrival times measured in (a) the time domain and (b) the frequency domain. In the time domain, the symbols overlap and are indistinguishable, while in the frequency domain, they become broadened and separated after dispersive Fourier transformation.

those pulses was impossible due to very strong phase ripples, that distorted the output signal. Temporal parameters show a strong agreement with theoretical predictions.

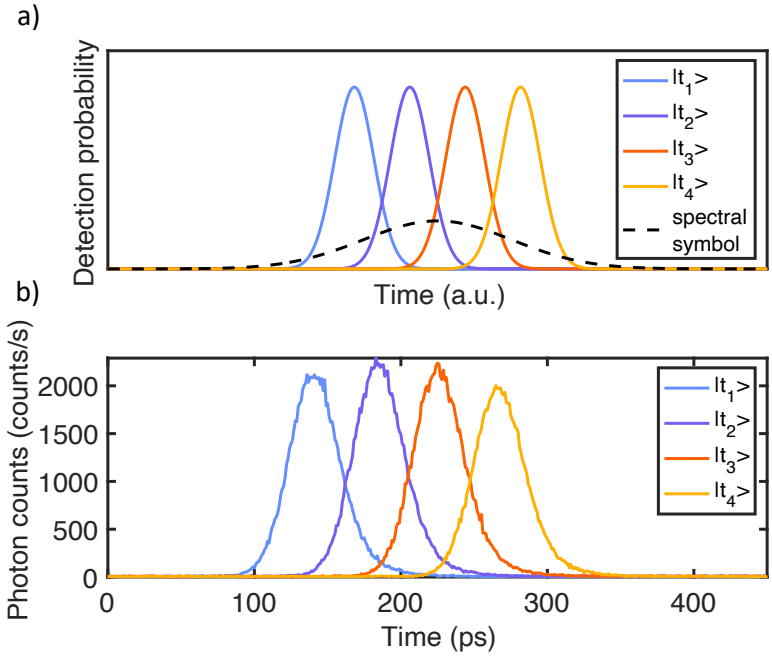

Figure 4.22: (a) Simulated four-dimensional PPM symbols. (b) Histograms of temporal symbol's arrival times measured in the time domain.

Table 4.2: FSK Symbols Measured Parameters

Symbol	**Temporal width**	**Temporal separation**	**Spectral width**	**Spectral separation**
$\|f_1\rangle$	146 ps	-	3.88 GHz	-
$\|f_2\rangle$	143 ps	1 ps	3.77 GHz	3.05 GHz
$\|f_3\rangle$	145 ps	2 ps	3.76 GHz	3.90 GHz
$\|f_4\rangle$	141 ps	1 ps	3.83 GHz	3.50 GHz

Table 4.3: PPM Symbols Expected and Measured Parameters

Symbol	**Expected temporal width**	**Expected temporal separation**	**Measured temporal width**	**Measured temporal separation**
$\|t_1\rangle$	36 ps	-	40 ps	-
$\|t_2\rangle$	36 ps	43 ps	39 ps	47 ps
$\|t_3\rangle$	36 ps	43 ps	40 ps	42 ps
$\|t_4\rangle$	36 ps	43 ps	40 ps	40 ps

4.7 Chapter summary

In this chapter, I demonstrated the precise generation and control of temporal and spectral profiles of symbols at C-band telecom wavelengths using an indium phosphide photonic integrated

transmitter. This setup enabled temporal and spectral measurements at the single-photon level. The modulation scheme proved effective in generating pulses with the desired temporal and spectral profiles, achieving short pulse durations relative to the available bandwidth. The available bandwidth and quality of the dispersive receiver was insufficient for generating PPM symbols using on-chip modulators and detecting them with the dispersive receiver due to distortions introduced by the DCM. Nevertheless, the pulses were adequate for frequency shift keying. Generating FSK symbols was possible with the on-chip components and by carefully controlling the central wavelength with temperature and current tuning. I characterized spectral profile of single-photon level optical pulses and verified the assumptions underlying time-frequency quantum key distribution systems. This work represents an important step toward high-dimensional on-chip quantum communication and tightly wavelength-multiplexed systems.

Chapter 5

Measuring high-dimensional superpositions with temporal Talbot effect

The ability to generate and detect high-dimensional time-bin quantum superpositions results in more complex architecture of the receiver, as discussed in Chapter 2. Typical receiver architectures employ nested interferometers, multiple single-photon detectors or active manipulation of received signal. As a part of this thesis, a problem of building a robust and resource-efficient receiver was addressed. I this chapter I present a method of measuring time-bin quantum superopsitions with the temporal Talbot effect, the analog of better-known spatial self-imaging effect. In the first section I present the theoretical background for this method stemming from space-time duality. Then I present the experimental setup and results obtained for a four-dimensional superposition. Finally, I discuss how timing jitter impairs the quality of the measurements and how post-selection methods can be used to mitigate negative effects. The results and techniques described in this chapter will be used for constructing the quantum key distribution link described in Chapter 6. This work was carried out in collaboration with Maciej Ogrodnik, who provided valuable insights into data analysis and post-processing methods, and contributed to the development of the simulation software. I was responsible for creating the simulation and measurement automation software, as well as building, calibrating, and operating the experimental setup, and data acquisition. The results were published in Optica [130].

5.1 Space-time duality

The optical space-time duality can be shown by using mathematical equivalency of equations describing space-confined beam and dispersion of narrow-band pulses in dielectrics. The first step is using Maxwell's equations to derive the light wave equation. The most general solution to the wave equation provides a description of the space-time evolution of a wave function with an arbitrary shape. Consequently, we must rely on approximations that make the wave equation solvable [131]. Typically, we focus on either the spatial or temporal evolution of the wave function. When analyzing the spatial problem, we begin by assuming that the wave has a monochromatic frequency spectrum. This means the wave exhibits only harmonic time variation, and as a result, the time derivatives in the wave equation are reduced to multiplicative constants. We also assume fixed polarization. Additionally, we permit variations in the transverse spatial structure, provided

that wave propagation predominantly occurs in one direction and is initially confined near the axis along which it propagates. This approach is known as the paraxial approximation and leads to a parabolic partial differential equation that describes the evolution of the wave's transverse profile:

$$\frac{\partial^2 E}{\partial x^2} + \frac{\partial^2 E}{\partial y^2} - 2ik\frac{\partial E}{\partial z} = 0, \tag{5.1}$$

where k the wavenumber, and x, y, z are the spatial coordinates. The temporal problem is addressed in a similar manner, but with a different set of approximations. Since we aim to describe the evolution of pulses or generally modulated waves, we can no longer assume a monochromatic field. However, by restricting the temporal-frequency spectrum to an appropriate range, we can account for the propagation of each spectral component within the wave by expanding the propagation constant β in a Taylor series up to the second order in. Additionally, we can simplify the problem by ignoring the spatial profile of the wave and treating it as an infinite plane wave [131]. After changing the variables to a traveling-wave coordinate system:

$$\tau = (t - t_0) - \left(\frac{z - z_0}{v_g}\right), \tag{5.2}$$

$$\xi = z - z_0, \tag{5.3}$$

where v_g is the group velocity, these approximations reduce the wave equation to a parabolic differential equation that describes the space-time evolution of the pulse envelope or "wave packet":

$$\frac{\partial A(\xi,\tau)}{\partial \xi} = \frac{i}{2}\frac{d^2\beta}{d\omega^2}\frac{\partial^2 A(\xi,\tau)}{\partial \tau^2}. \tag{5.4}$$

A consequence of those similarities can also be seen in spatial and temporal imaging [132]. Those analogies allowed to develop techniques for manipulating the bandwidth of single-photon pulses by means of electro-optic modulation just as lenses allow to shape the spatial profiles of beams [133]. The final, yet substantial consequence is that there exists a temporal equivalent of the self-imaging effect, known as the Talbot effect.

5.1.1 Spatial Talbot effect

The Talbot effect is an effect of self-imaging of periodic diffractive structures [134]. It can be observed by illuminating a periodic diffraction grating with a plane wave and using a magnifier for imaging. An alternating pattern of interference maxima and minima will become visible. The pattern will change its characteristic shape as the distance between the magnifier and the grating changes. The image of the grating will repeat itself at regular distances away from the plane of the grating. This regular distance is known as the Talbot length, and the repeated images are referred to as self-images or Talbot images. Additionally, at half the Talbot length, a self-image appears, but it is phase-shifted by half a period, meaning it is laterally shifted by half the width of the grating period. At smaller fractional distances of the Talbot length, sub-images can also be observed. For instance, at one-quarter of the Talbot length, the self-image appears with half the period of the grating, resulting in twice as many images. At one-eighth of the Talbot length, the period the images is halved again, leading to a fractal pattern of sub-images often referred to as a Talbot carpet. This effect is a direct consequence of Fresnel diffraction [134]. The Talbot length is given by:

$$z_T = \frac{\lambda}{1 - \sqrt{1 - \frac{\lambda^2}{a^2}}} \tag{5.5}$$

A simulated result of self-imaging of periodically-distributed light sources created with a diffraction grating illuminated with $\lambda = 500$ nm light is shown in Fig. 5.1 Experimentally, this effect

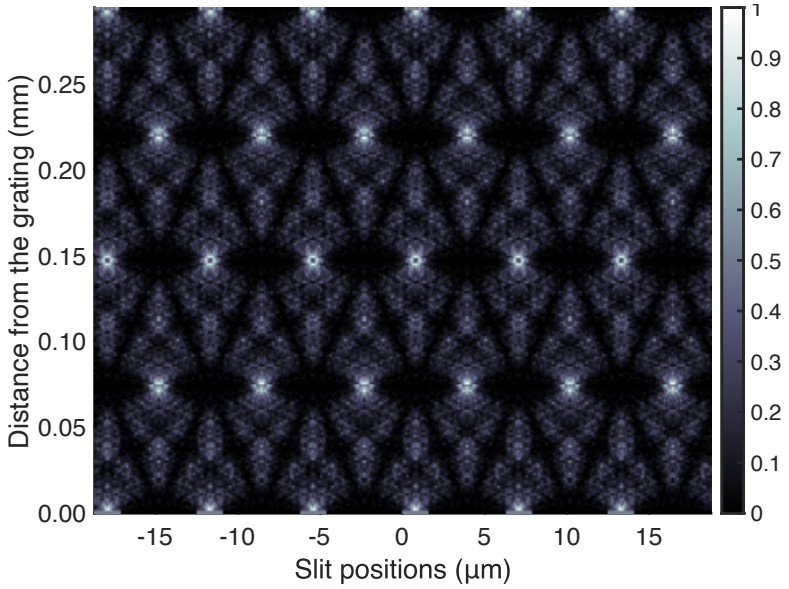

Figure 5.1: Spatial Talbot carpet: self imaging of a periodic light sources (diffraction grating). Color brightness corresponds to the optical power at a given position in space.

can be observed with a microscope by changing the position of an illuminated diffraction grating. Exemplary self-imaging is shown in the following Figure 5.2. The measurements were carried out by me in the Quantum Imaging Laboratory at the Faculty of Physics, University of Warsaw.

The Talbot effect can be used in structured illumination fluorescent microscopy to overcome the diffraction limit [135], to create patterns for lithography [136], and measurement of displacement in experimental fluid dynamics [137].

5.1.2 Temporal Talbot effect

A phenomenon analogous to the spatial Talbot effect can be observed when periodically separated optical pulses are subverted to dispersive broadening. For certain values of group delay dispersions (GDD), the pattern of input pulses will be reproduced with different temporal separations [138]. An exemplary temporal Talbot carpet simulated for 16 light pulses separated by 284 ps is shown in Fig. 5.3 The exact technique of detecting superpositions with that effect is described in the following parts of this chapter.

5.2 Detecting superpositions with the temporal Talbot effect

Temporal mode superpositions were measured using the optically nonlinear quantum pulse gate [139, 140], which facilitates quantum tomography [141], as well as through electro-optic sideband generation in frequency bins, enabling both the detection of frequency-bin superpositions [142] and the verification of time-frequency entanglement [143, 144, 145]. However, these methods rely

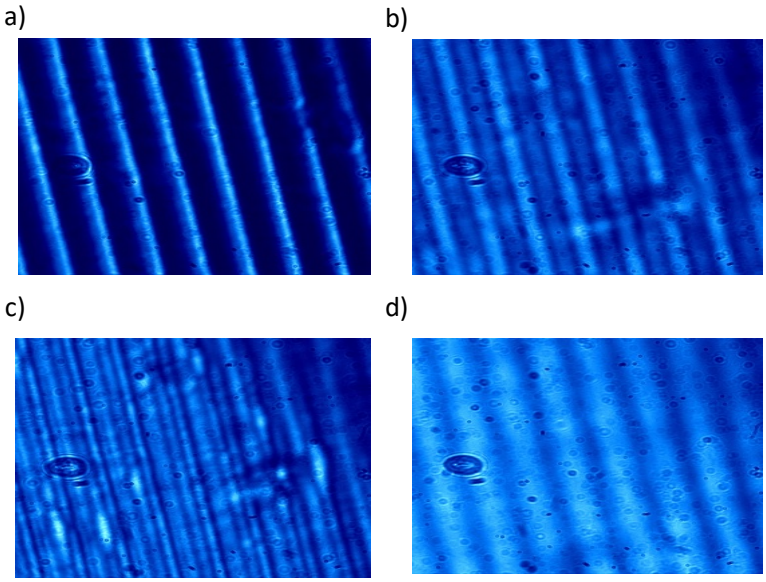

Figure 5.2: Spatial Talbot carpet: self imaging of a periodic object (diffraction grating). a) The image of the diffraction grating taken in very close proximity. Bright stripes are the illuminated slits. b) Image of the grating taken at a one quarter of the Talbot length. Spatial frequency of the interference fringes is doubled. c) Image of the grating taken at the one eighth of the Talbot length. Spatial frequency of the fringes is quadrupled. d) Image of the grating at the half of the Talbot distance. Contrast of the fringes is inverted with respect to a), and original spatial frequency is restored.

on active spectral modifications, achieved either through electro-optic techniques or nonlinear optical interactions. An alternative approach for detecting time-bin superpositions is the use of Franson interferometers [146, 118]. However, a single interferometer is limited to measuring the phase relationship between only two time bins. Achieving multidimensional state discrimination necessitates the nesting of multiple interferometers [54, 147], which introduces greater complexity, cost, and, most notably, optical losses. In the Franson interferometer tree method, the likelihood of detecting a $d-$dimensional superposition decreases proportionally to $1/d$ as the number of possible paths in the nested interferometer increases [54].

Another possibility to approximately detect time-bin superpositions is by directly resolving their spectrum. However, resolving the signals in time and frequency simultaneously at the single-photon level is challenging due to the limits given by the time-frequency uncertainty relation [148, 114]. The highest resolution of efficient multiplexed single-photon spectral measurements is offered by means of the dispersive Fourier transform [149, 150, 151, 152, 153], however, the large values of group dispersion delay needed to reach the required spectral resolution can result in prohibitively high losses [148]. An alternative possibility to approximately detect time-bin superpositions is to directly resolve their spectrum. However, simultaneously measuring signals in both time and frequency at the single-photon level is inherently difficult due to constraints imposed by the time-frequency uncertainty relation [148, 114]. The dispersive Fourier transform [149, 150, 151, 152, 153] provides the highest resolution for efficient multiplexed single-photon spectral measurements. However, achieving the required spectral resolution demands large group dispersion delays, which can lead to prohibitively high losses [148].

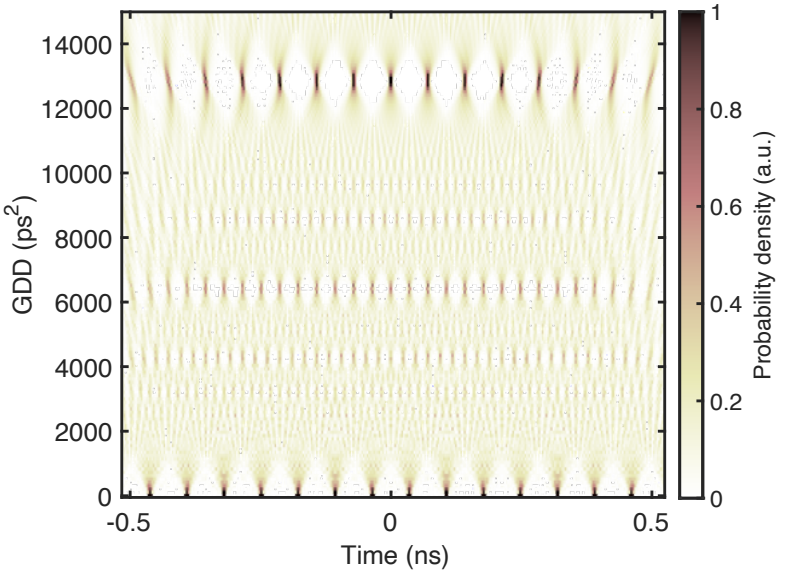

Figure 5.3: Temporal Talbot carpet: self imaging of a a series of optical pulses due to dispersion.

I propose an alternative method based on the Talbot effect, a well-known near-field diffraction phenomenon [154], which enables the discrimination of d orthogonal states of a $d-$ dimensional time-bin superposition. This approach requires only a passive experimental setup consisting of a dispersive medium and a single time-correlated single-photon counter. While the discrimination is not perfect, I demonstrate that the information content increases with the dimensionality. The setup can be built using readily available components, requires significantly less dispersion than a conventional dispersive Fourier spectrometer, and maintains a constant detection loss regardless of the dimension d.

5.2.1 Superposition generation

In this section I explain the method, assumptions and experimental setup for generating superpositions. The detection methods will be presented in the following section.

Let us consider optical pulses in different time bins $|t_0\rangle$, $|t_1\rangle$,..., $|t_m\rangle$ forming the Z (key generation) basis, and four superpositions of those states that form a discrete Fourier transform of the Z basis [155], which is the X (control) basis:

$$|f_n\rangle = \frac{1}{\sqrt{d}} \sum_{m=0}^{d-1} e^{\frac{-2\pi i n m}{d}} |t_m\rangle \,. \tag{5.6}$$

The two bases are mutually unbiased and satisfy the relation [98]:

$$|\langle f_n | t_m \rangle|^2 = \frac{1}{d} \quad \forall\, m, n. \tag{5.7}$$

This fact is relevant for the next chapter describing the quantum key distribution experiment, as eavesdropper who measures in the wrong basis gains no information and introduces detectable errors [156].

To observe s-order temporal self images, the following relation between pulse separation (τ) and GDD (β_2) must be met [138]:

$$\tau = \sqrt{\frac{2\pi\beta_2}{s}}, s = 1, 2.... \tag{5.8}$$

Those conditions are a basis for designing the experiment. The superpositions will be detected using the first-order temporal self-images. This requires adjusting the separation with respect to medium with an available group delay dispersion GDD and electrical bandwidth enabling generation of short optical pulses. The advantage of this technique is that it requires less group delay dispersion (GDD) compared to a conventional dispersive spectrometer. The minimum GDD needed to observe superpositions in the far-field regime is given by [157]:

$$\beta_2 \gg \frac{\sigma_0^2}{4\pi}, \tag{5.9}$$

where σ_0 is a parameter describing the width of the input pulse.

The experimental setup is shown in Fig. 5.4. A laser operating at a telecom wavelength of

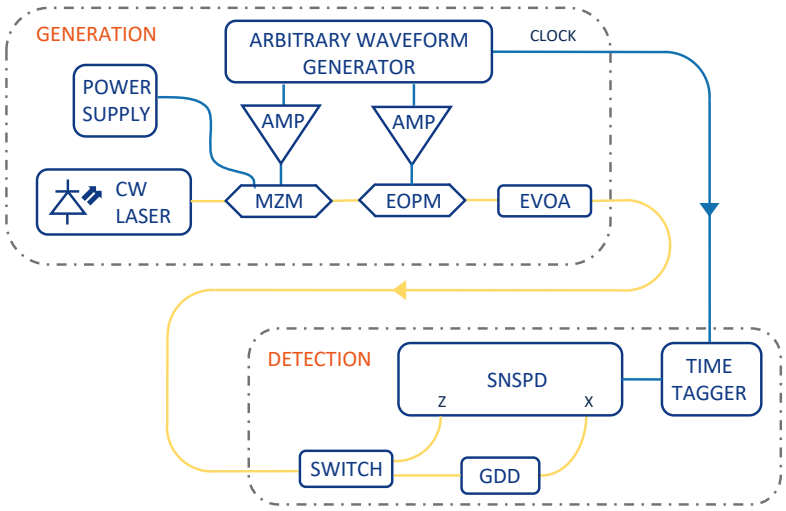

Figure 5.4: A continuous wave (CW) telecommunication-wavelength laser light is modulated using a MZM and EOPM to produce optical pulses forming superpositions. The optical signals are then attenuated to the single-photon level using an electronic variable optical attenuator (EVOA). Photons are measured with SNSPDs either in the Z basis (Z) through direct photon counting or in the X basis (X) via the temporal Talbot effect, which is implemented using a DCM that introduces DGG. Photon arrival time histograms are recorded using time-correlated single-photon counting (TCSPC). Optical fiber connections are represented by yellow lines.

1560 nm in continuous wave (CW) mode served as the light source. To ensure sufficient power for a feedback loop used to bias the modulator, the optical signal was amplified with an erbium-doped fiber amplifier (EDFA, Pritel, HPP-PMFA-22-10), followed by a bandpass spectral filter to minimize noise. Optical pulses were generated using fast amplitude electro-optic modulation via MZM (Thorlabs, LNA6213). These pulses were then used to create superpositions of $d = 4$ single states with predefined phase relationships. The superpositions were directed to EOPM (EOSPACE Inc.), which applied the necessary phase shifts to each component of the superposition. Both modulators supported an analog bandwidth of 40 GHz and were driven by an

amplified RF signal. This RF signal was generated using a fast AWG (Keysight, M1896A), which provided an analog bandwidth of 33 GHz and a sampling rate of up to 92.16 GSa/s. Consequently, the full-width at half maximum (FWHM) duration of a one-bit signal was approximately 12 ps. The phase adjustments were implemented by programming the EOPM with four driving voltage signals composed of rectangular pulses about 150 ps wide [Fig. 2(a)], with amplitudes corresponding to fractions or multiples of the half-wave voltage (V_π). Optical signals were generated by allocating three bits per symbol from the AWG memory, with symbol separation set at 282 ps rather than 284 ps due to the finite sampling frequency. The AWG also generated a 10 MHz clock (CLK) signal, which was transmitted via an electrical cable to the detection section. The MZM was biased for minimal transmission using a direct current (DC) voltage supplied by a power source (Keysight, E36313A). This biasing was automatically adjusted through a feedback loop incorporating a 90 : 10 fiber optic beam splitter and a power meter (Thorlabs, PM400). Finally, the pulses were attenuated to the single-photon level using an electronic variable optical attenuator (EVOA, Thorlabs, EVOA1550F).

On the detection side, the optical path was reconfigured to enable either direct photon count measurements in the time domain or the detection of superpositions. For time-domain measurements, the signals were directed to niobium nitride SNSPDs (Single Quantum) with a 70% detection efficiency and a dark count rate of less than 1000 counts per second. The recorded time tags were then processed using a time-to-digital converter (Swabian Instruments, Time Tagger Ultra) with a resolution of 1-ps-wide bins. The time tagger exhibited a jitter of approximately 10 ps root mean square (RMS), while the SNSPDs contributed about 5 ps RMS, resulting in a total receiver system jitter of around 11 ps RMS.

For superposition measurements, the photons were additionally passed through a DCM based on a CFBG, which induced dispersive stretching of the optical pulses. The DCM had a measured insertion loss of 2.7 dB, representing the primary source of detection loss, whereas other optical losses, mainly due to fiber connector losses, remained below 0.2 dB. The module provided GDD of $12,900$ ps^2, as specified by the manufacturer (Proximion, DCMHDC-100H-P510). While this level of dispersion was insufficient for performing a full dispersive Fourier transform, it was adequate for observing the temporal Talbot effect (see far-field GDD in Fig. 5.8), which was utilized to distinguish superpositions of optical signals with varying phase relationships. The generation scheme for two and four-dimensional case and corresponding interference fringes stemming from dispersive stretching are presented in figures 5.5, 5.6

Achieving this effect requires careful calibration of the phase modulating signal's amplitude and delay between the amplitude and phase modulating pulses. A first estimate of the RF signal's amplitude can be based on the gain data provided by the manufacturer and measuring signals with a fast oscilloscope. The initial delay can be found by replacing the phase modulator with another intensity modulator. Then peaks are visible in the histogram. Further fine calibration of amplitude and delay was performed by the histogramming the two different two-dimensional superpositions generated using two sets of parameters. The optimum is obtained when fringes are equally separated, as illustrated in Fig. 5.7

5.2.2 Detecting the superpositions

Just as periodically placed intensity distributions would be self-imaged due to diffraction, a superposition of equally spaced pulses is self-imaged by propagation in a medium with a certain GDD (which I will further refer to as the Talbot GDD). Similarly to the spatial case, the temporal positioning of the self-images is influenced by the relative phases of the sources. This allows to utilize the temporal Talbot effect for detecting different time-bin superpositions. Specifically, the temporal Talbot effect can be seen as a discrete Fourier transform (DFT) on input pulse trains.

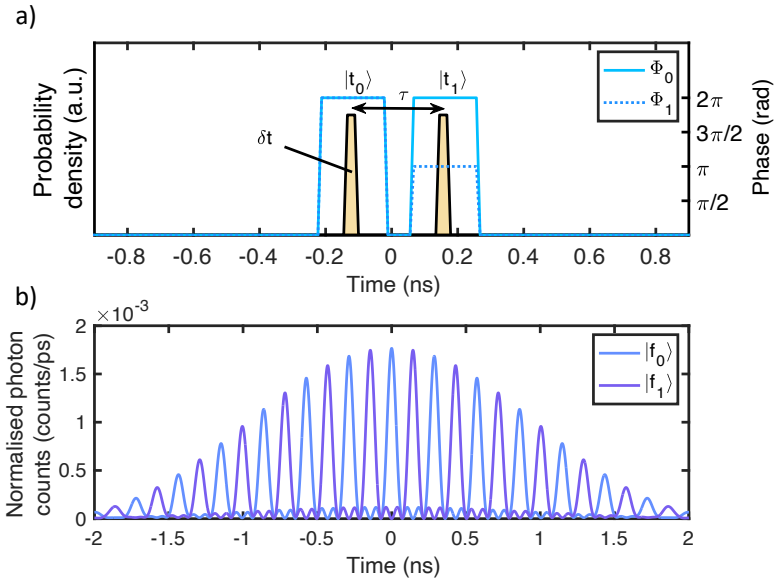

Figure 5.5: Two-dimensional superpositions. (a) Numerical simulation of the signal's temporal profiles. Yellow rectangles illustrate the optical signal profiles used in the simulation, as well as the electrical signals employed to generate temporal symbols through high-speed electro-optic amplitude modulation. Blue rectangles depict the voltage signals applied for phase modulation. (b) Simulated distributions of single-photon arrival times for the temporal Talbot effect, based on the experimental parameters.

With a fixed experimental setup with dispersive medium each symbol from the discrete Fourier transform basis has a distinct probability distribution of the time of arrival.

In the figures 5.8, 5.9 and 5.10 I present simulated temporal Talbot carpets and their cross-sections for different dimensions. For each simulation Gaussian pulse profile is assumed. The FWHM is 34 ps and separation 284 ps in order to match the CFBG-based GDD medium with 12900 ps^2.

In a real-world scenario, the superpositions comprise finite number of components, have a finite width, and are corrupted by timing jitter leading to overlap in the interference fringes. As a result, some detection events may be ambiguous. This contrasts with the Franson interferometer tree method[146], where a portion of the detections yield unambiguous measurement results.

For single-shot state discrimination using the Talbot effect method, a procedure is needed to assign a symbol based on the measured time of arrival. The goal is to maximize accuracy, defined as the ratio of correct assignments to errors. The following mathematical interlude serves as a demonstration showing that the optimal approach is to simply select the most probable symbol for a given detection time. For a fixed measurement setup, state detection can be understood as distinguishing between classical random variables, which represents a straightforward case of Bayesian decision theory [158]. The probability of selecting the right symbol at a given instance will be further referred to as correctness.

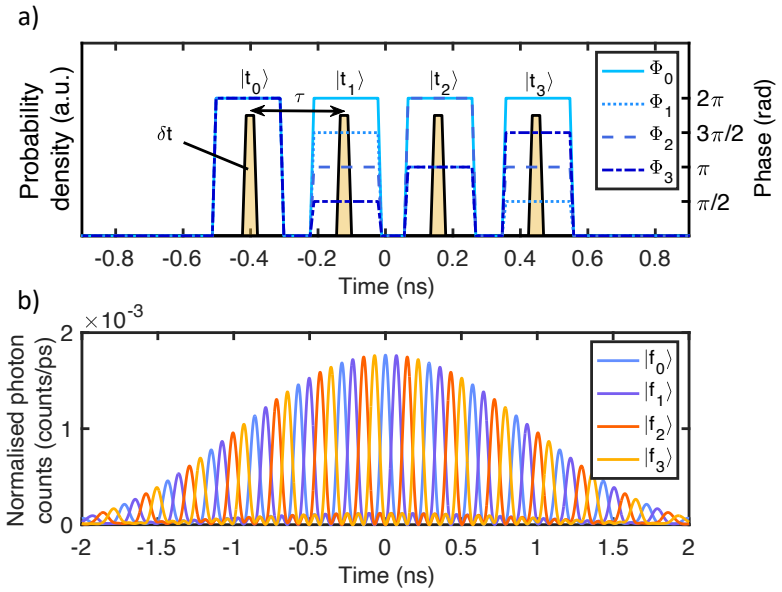

Figure 5.6: Four-dimensional superpositions. (a) Numerical simulation of the signal's temporal profiles. Yellow rectangles illustrate the optical signal profiles used in the simulation, as well as the electrical signals employed to generate temporal symbols through high-speed electro-optic amplitude modulation. Blue rectangles depict the voltage signals applied for phase modulation. (b) Simulated distributions of single-photon arrival times for the temporal Talbot effect, based on the experimental parameters.

5.2.3 Post-selection

Rejecting certain measurements can enhance distinguishability, as quantified by correctness. For instance, if all possible states are equally probable at a given detection time, that measurement provides no useful information about the state. Conversely, in cases where only one state has a nonzero probability at a specific arrival time, the measured state can be identified with high certainty, with the remaining uncertainty stemming from experimental factors such as dark counts. Here, I utilize a postselection strategy proposed by Maciej Ogrdonik, based on conditional probabilities. For each detected time of arrival, we evaluate the conditional probability of each state. A measurement is discarded if the highest probability at that time is below a predefined cutoff threshold. Increasing the cutoff probability leads to a higher rejection rate and improved correctness, reaching an upper bound of 1 in the extreme case where all measurements are rejected. For any rejection rate $r \in [0, 1]$, there exists a corresponding cutoff probability that produces that exact rejection rate. This approach allows us to analyze postselection performance by examining correctness at the cutoff probability associated with a given rejection rate. The relationship between rejection rate and correctness depends on both the system's dimensionality and detection noise. This effect arises due to the shape of the overlapping probability distribution functions, which are further influenced by timing jitter—one of the dominant sources of error in practical systems. Figure 5.18 illustrates the impact of postselection on correctness in a simulation of four-dimensional discrete Fourier transform state detection. The curve corresponding to 2 ps RMS detection noise suggests that recent advancements in single-photon detector technology [159] could significantly enhance the performance of the Talbot technique, bringing it closer to

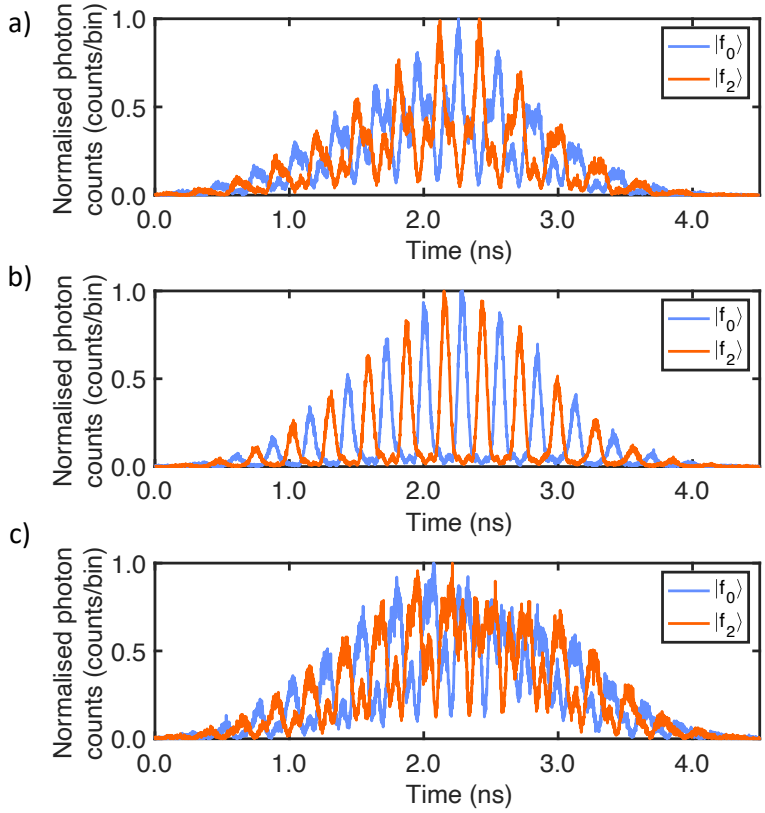

Figure 5.7: Histograms of two four-dimensional superpositions used for adjusting parameters of driving RF signals: a) undercalibrated b) calibrated c) overcalibrated.

the ideal 0 ps RMS jitter detection limit. This ultimate limit is defined by the spectral overlap of the superposition states. The way rejection rate translates to considered data, and therefore the area of interest of the interference fringes is shown in Fig. 5.18.

5.2.4 Detecting four-dimensional superpositions with temporal Talbot effect

The technique of detecting quantum superpositions with temporal Talbot effect was demonstrated using four distinct four-dimensional superpositions and four distinct pulses from the temporal encoding alphabet. To validate this approach, the widths, shapes and positions of the histograms along the time axis were analyzed. The measurements were conducted with the experimental setup described in 5.4. The temporal symbols exhibited an approximately Gaussian profile, with a width of about 46 ps and a separation of roughly 284 ps, consistent with expectations. Figure 5.13 displays histograms of qubits and Fig. 5.14 of ququarts as measured in time domain and after propagation through the DCM. The resulting fringes were temporally distinguishable, enabling the identification of each state within the X basis. The probability of successful state identification was measured for symbol separations both below and above the first Talbot separation. The results of these measurements are shown in Fig. 5.15. Correctness was evaluated by selecting the most probable symbol at a given detection time, following the

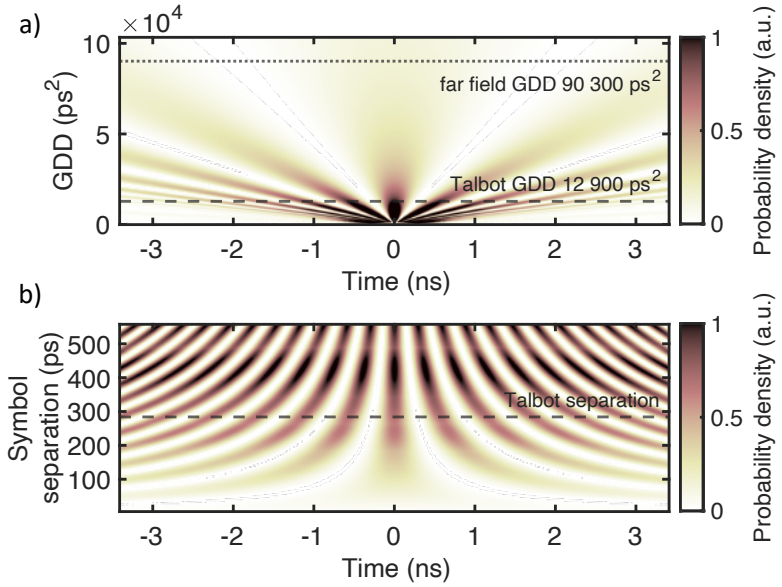

Figure 5.8: a) Temporal Talbot carpet generated with a two-dimensional superposition. b) A corresponding orthogonal Talbot pattern showing how the likelihood of photon detection varies over time with changing symbol separation.

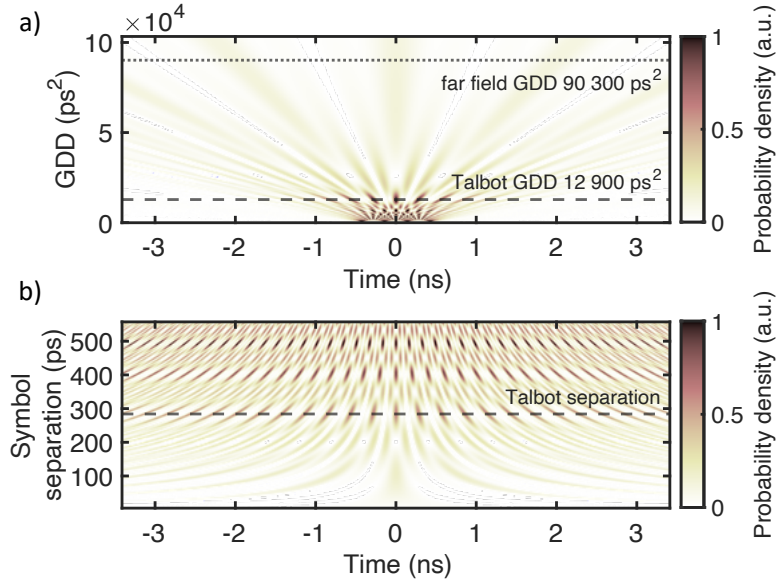

Figure 5.9: a) Temporal Talbot carpet generated with a four-dimensional superposition. b) A corresponding orthogonal Talbot pattern showing how the likelihood of photon detection varies over time with changing symbol separation.

reasoning outlined in the "Detecting superpositions" chapter. Maximal correctness was equal

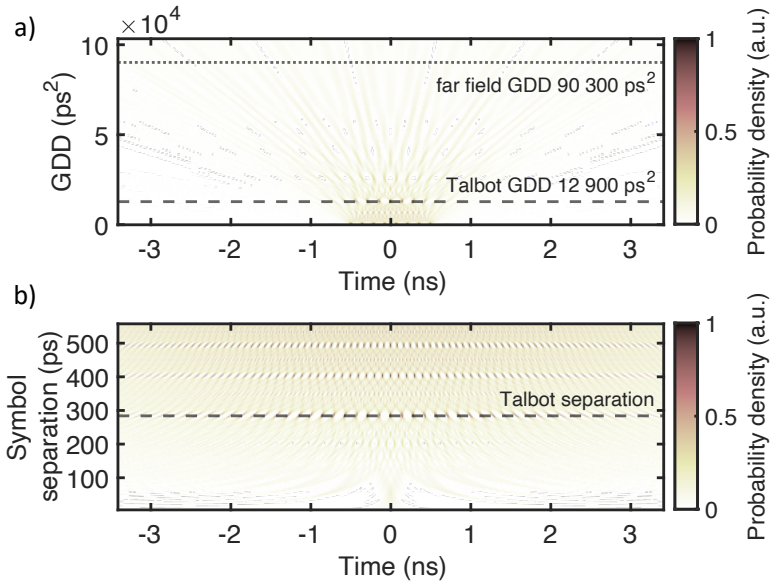

Figure 5.10: a) Temporal Talbot carpet generated with a eight-dimensional superposition. b) A corresponding orthogonal Talbot pattern showing how the likelihood of photon detection varies over time with changing symbol separation.

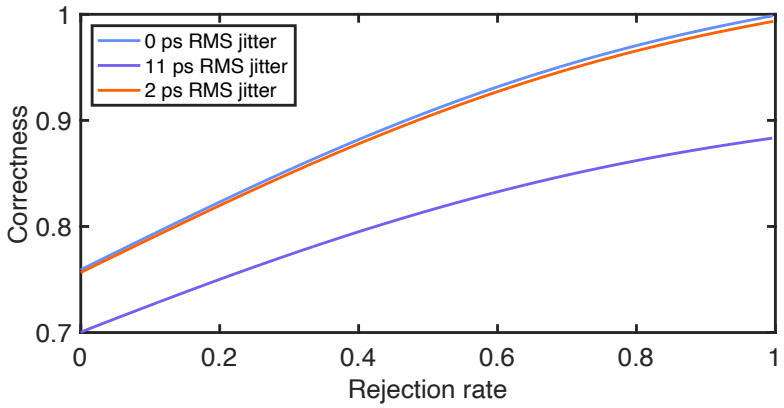

Figure 5.11: Correctness of four-dimensional discrete Fourier transform states with postselection across various rejection rates: evaluated under ideal conditions without detection noise, with 11 ps root mean square (RMS) noise corresponding to our experimental setup, and with a reduced but experimentally obtainable 2 ps RMS noise.

to 63.5%. The results demonstrate that any deviation from the Talbot separation leads to a reduction in correctness, indicating that the measurements occur outside the temporal far-field regime. Furthermore, the analysis shows that correctness can be improved using a postselection strategy, wherein the most ambiguous measurement outcomes are discarded.

The results present good agreement of experimentally-obtained results with the theory, although some systematic error is present. The constant mismatch between the measured and

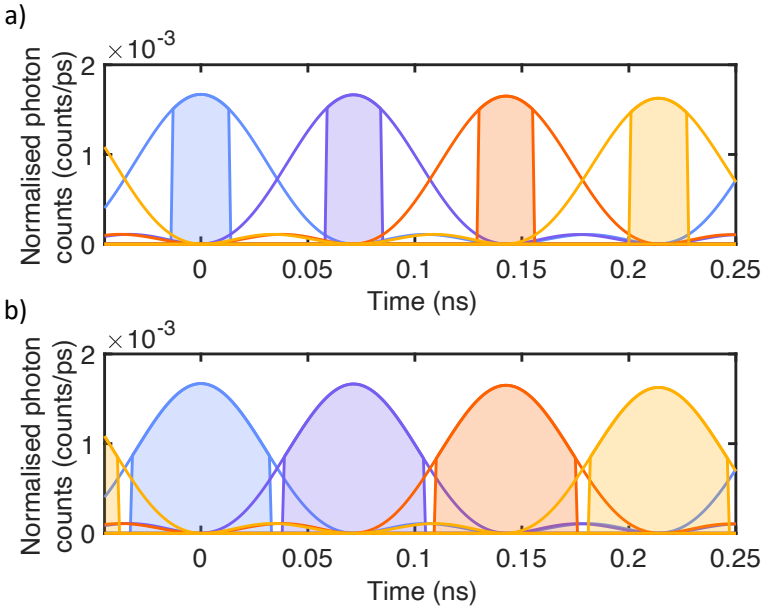

Figure 5.12: Simulated spectral interference fringes considering a) 90% rejection rate, b) 50% rejection rate. Highlighted area correspond to the data considered for the calculation of correctness. Detection events occupying the non-highlighted part are rejected.

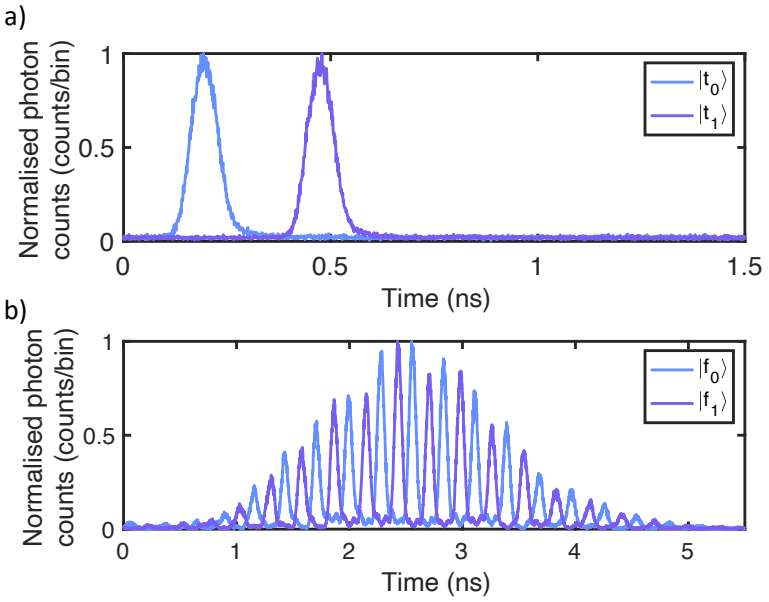

Figure 5.13: Measured histograms of two-dimensional symbols: a) in the Z basis, b) in the X basis.

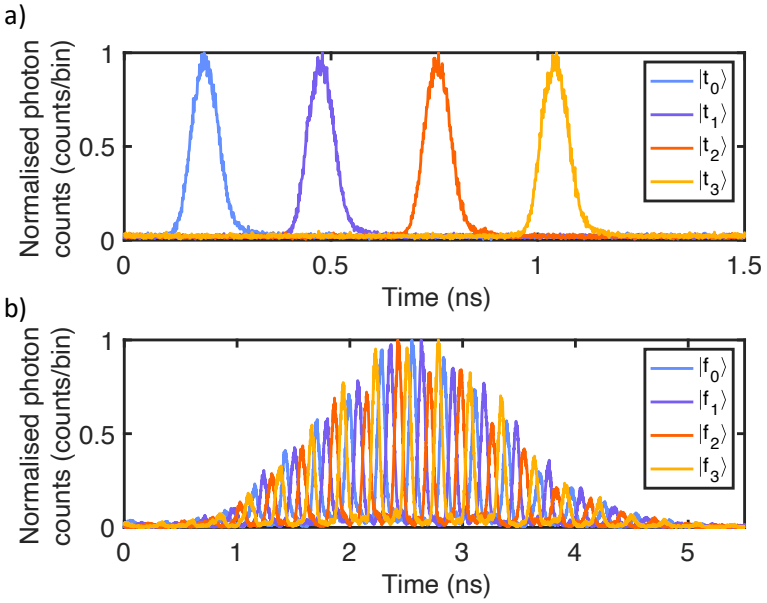

Figure 5.14: Measured histograms of four-dimensional symbols: a) in the Z basis, b) in the X basis.

expected values could originate from error in pulse preparation or underestimation of the detection timing jitter value. Nevertheless, the method is highly practical, as it can be implemented for other dimensions while maintaining the same experimental setup and improvements in single photon detection systems could enable far less-erroneus measurements [159].

5.2.5 Jitter influence and dimension scalability

In a d-dimensional basis, each state encodes $\log_2(d)$ bits of information. Under ideal detection conditions, this would result in $\log_2(d)$ bits of mutual information between the prepared state and the measurement outcome. In Fig. 5.18, I compare the mutual information obtained using our method to the ideal detection case, which achieves the theoretical limit of $\log_2(d)$ bits. This comparison reveals that the scaling of information in temporal Talbot method is more complex than the logarithmic scaling observed in ideal detection.

Figure 5.17 illustrates how correctness varies with dimension. As the dimensionality increases, correctness decreases due to the increasing overlap of probability density functions. This effect is particularly pronounced at higher levels of detection timing jitter, which further complicates state discrimination in higher-dimensional systems.

The states from a discrete Fourier transform basis can also be measured using a Franson interferometer tree, as proposed in [147, 113]. For a system of dimension d, the Franson interferometer tree method requires $d-1$ precisely aligned Franson interferometers and d detectors. It relies on postselection, which results in discarding $\frac{d-1}{d}$ of the measurements. Additionally, the practical efficiency of this method is further constrained by the insertion loss of the interferometers along the optical path. In principle, the efficiency of the Franson interferometer tree approach can be improved to nearly 100% by incorporating active switches, as demonstrated in [160, 161]. However, this enhancement comes at the cost of increased experimental complexity

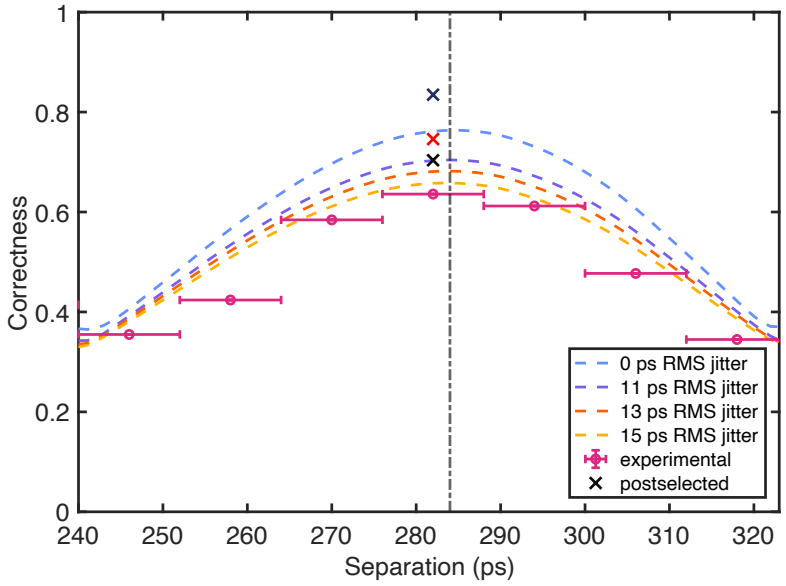

Figure 5.15: Measured correctness of X-basis state discrimination, compared with theoretical predictions for both the ideal case without jitter (noiseless) and the $11, 13, 15$ ps RMS jitter scenarios (noisy). Error bars represent sampling errors arising from the finite sampling frequency of the AWG. Small discrepancies in measured correctness, not accounted for in the simulation, result from imperfections in symbol preparation. Crosses denote experimentally obtained correctness values after postselection, corresponding to data rejection rates of 0.3 (black), 0.5 (red), and 0.9 (purple).

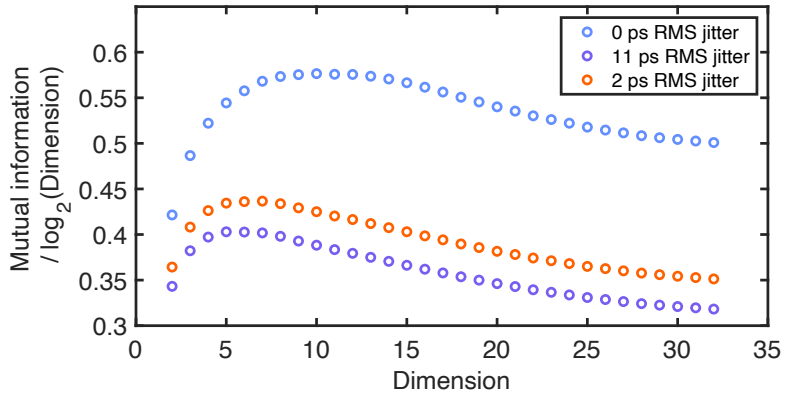

Figure 5.16: Mutual information for detection under three conditions: ideal detection with no noise, detection with 2 ps RMS timing jitter, and detection with 11 ps RMS jitter (matching the experimental setup). The values are normalized by $\log_2(d)$, which represents the total information encoded in a d-dimensional state, with no postselection applied.

and additional insertion loss.

The impact of timing jitter and measurement errors related to spectral overlap can be visualized using confusion matrices. Figure 5.19 compares the experimental results for the four-

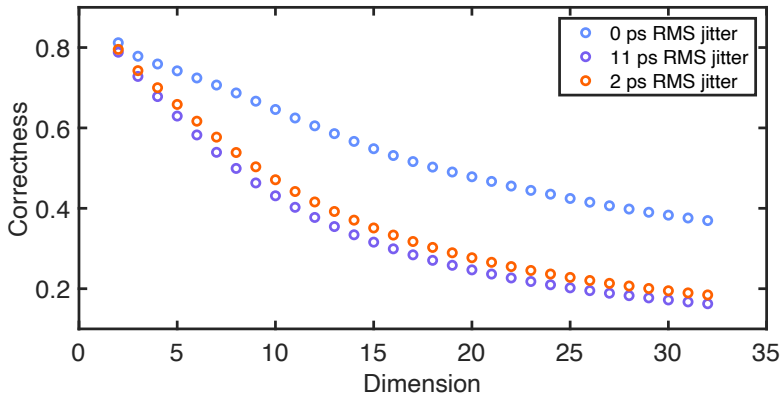

Figure 5.17: Numerical simulation of correctness for various levels of detection timing jitter, conducted without applying postselection.

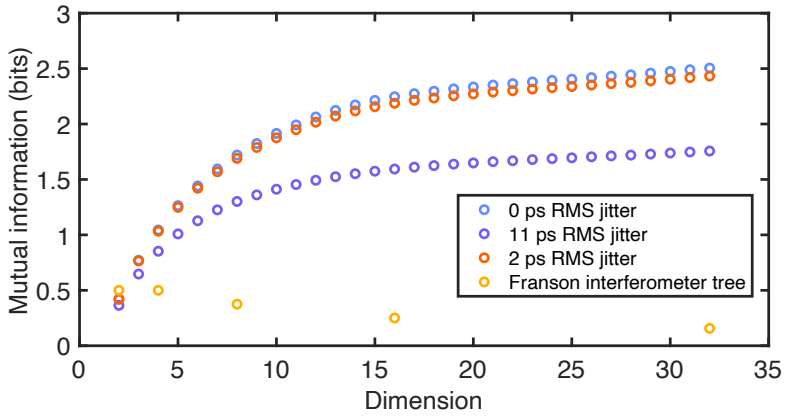

Figure 5.18: Numerical simulation of mutual information between the input state and time of arrival random variables across different levels of detection noise. The results are compared with the Franson interferometer tree method, which provides $\log_2(d)$ bits of information per received pulse, scaled by a detection efficiency factor of $\frac{1}{d}$. This accounts for information obtained only from the central time-bin. While measurements in the side bins do not enable perfect state detection, they may still contribute additional information. The plotted points correspond only to dimensions that align with physically feasible interferometer configurations. It is important to emphasize that the maximum achievable mutual information is $\log_2(d)$.

dimensional case under two conditions: 11 ps RMS jitter and an idealized 0 ps RMS jitter scenario. Similarly, Figure 5.19 presents a simulation of detection in an eight-dimensional setting. All confusion matrices were computed without applying postselection. Since the dark count rate is low relative to the number of detected photons, its influence can be considered negligible. The detection probabilities shown were obtained following the procedure detailed in the "Detecting superpositions" section. Correctness was calculated based on the diagonal elements of the confusion matrices.

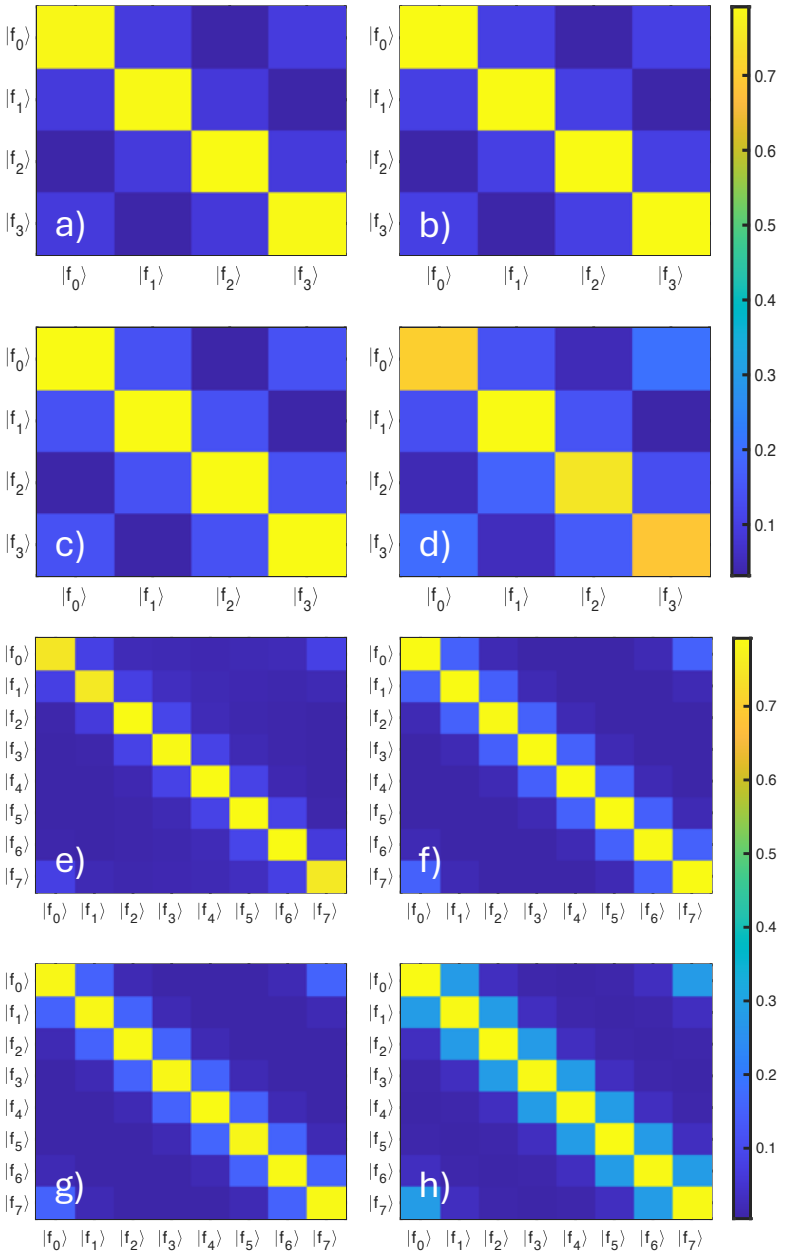

Figure 5.19: Confusion matrices for the detection of X-basis states: a) Simulation of ideal spectrally-resolved detection for $d = 4$. b) Detection using the Talbot effect with 0 ps RMS jitter for= $d = 4$. c) Detection using the Talbot effect, accounting for 2 ps RMS jitter for $d = 4$. d) Detection using the Talbot effect, considering 11 ps RMS jitter for $d = 4$. e) Simulation of ideal spectrally-resolved detection for $d = 8$. f) Detection using the Talbot effect with 0 ps RMS jitter for $d = 8$. g) Detection using the Talbot effect, accounting for 2 ps RMS jitter for $d = 8$. h) Detection using the Talbot effect, considering 11 ps RMS jitter for $d = 8$.

5.3 Chapter summary

This chapter demonstrates the detection of four different four-dimensional quantum superpositions using the temporal Talbot effect. This method is based on a temporal analog of the spatial Talbot effect, a phenomenon where periodic objects self-image. Just as diffraction produces interference fringes with varying separations, the temporal Talbot effect generates spectral interference fringes, whose temporal separation depends on the amount of GDD. The detection principle relies on analyzing these fringes at specific time instances corresponding to the first Talbot period. This period is achieved when the separation between the superposition components is precisely matched to the GDD coefficient of the medium. To verify this condition, correctness—the measure of successful information assignment to the correct time bin—was analyzed. The results indicate that the optimal strategy is always to select the most probable symbol at a given detection time. Additionally, the proposed method requires significantly less dispersion compared to conventional dispersive frequency-to-time mapping. The primary limitation in measurement accuracy comes from timing jitter, as reflected in the presented confusion matrices. However, accuracy can be improved through postselection, though at the cost of data loss. The receiver setup consists of only a beam splitter, a DCM, and a time-correlated single-photon counter for each measurement basis. This configuration offers both flexibility and tunability, as the DCM can be adjusted based on the encoding symbols and link length—an approach commonly used in fiber-optic communication systems. Furthermore, digital control allows for dynamic adjustment of pulse parameters according to the expected dispersion of the link and the receiver's characteristics. Notably, this method supports different dimensions within the same experimental setup, making it suitable for the development of software-defined quantum transmitters. The techniques described in this chapter form the foundation for constructing a quantum key distribution link based on time-phase encoding, which will be explored in the next part of the thesis.

Chapter 6

Urban quantum key distribution link based on high-dimensional time-phase encoding

This chapter focuses on the primary objective of this thesis: constructing a QKD link using the high-dimensional time-phase degree of freedom. The content builds on previous chapters, particularly on the method of detecting high-dimensional time-bin superpositions using the temporal Talbot effect. The chapter is structured into sections covering both theoretical aspects and practical implementations. First, I introduce the high-dimensional BB84 protocol and the tunable beam splitter protocol, a novel contribution of this work. This section concludes with secret key rate calculations as an overview. Next, I describe the experimental setup in detail, including its layout and calibration procedures essential for proper operation. Finally, I present the measured secret key rate values obtained in both a controlled laboratory environment and an urban dark-fiber infrastructure at the University of Warsaw. The theoretical framework and software were developed in collaboration with researchers from Germany and Italy within the Quantera QuICHE consortium – Dr. Federico Grasselli, Dr. Giovanni Chesi, Prof. Nathan Walk, Prof. Hermann Kampermann, Prof. Chiara Macchiavello and Prof. Dagmar Bruß. The initial objective of was to establish a security proof for time-frequency encoding, as proposed for on-chip implementation in Chapter 3. However, this approach proved to be prohibitively complex, leading to the adoption of time-phase encoding instead. The resulting security proof is based on active basis selection using a tunable beam splitter (TBS), which enables improved estimation of the phase error rate and removes the need to assume that detection probability at the receiver does not depend on the measurement basis. On the side of the University of Warsaw, Maciej Ogrodnik contributed to the development of the security proof, participated in the experimental work, and prepared advanced post-processing techniques for extracting secure key data from high-dimensional encoding scheme. My contributions included developing measurement automation and control software, building and calibrating the experimental setup, refining tools for calculating experimental key rates, and simulating theoretical secret key rates. I also carried out key rate simulations for both standard BB84 and the novel TBS-based protocol, across various dimensionalities and timing jitter conditions, using temporal Talbot effect-based detection. Data acquisition was carried out jointly by Maciej and myself. The security proof was published in Physical Review Applied [162]. The experimental results were shared as a preprint on the arXiv [163] and, at the time of writing this thesis, were under peer review.

6.1 Quantum key distribution: theoretical background

The general QKD procedure was demonstrated using an example of polarization-based BB84 in the Chapter 2. In this section I will elaborate more on time-phase variant, which is a particular case of time-frequency encoding. I will introduce two protocols, and show how they relate to each other. Throughout this chapter, finite key length effects are not considered, and presented key rate values are asymptotic. For this chapter the general QBER estimations presented below are valid for both protocols, considering detection based on the temporal Talbot effect.

The QBER in the Z basis is directly related to the extinction ratio of the MZM [164]:

$$QBER_z = \frac{1}{1 + 10^{\frac{ER}{10}}}. \tag{6.1}$$

ER values higher than 20 dB yield QBERs lower than 1%, which is needed for QKD systems as other contributions e.g. dark counts from the single-photon detectors would further deteriorate the key rate values. Such values are easily-achievable with lithium niobate MZMs, and are possible with modulators manufactured within generic photonic integrated circuit technologies. The QBER in the X basis for experiments described in this thesis is stemming from the temporal Talbot effect based method for distinguishing the superpositions. It is given by:

$$QBER_x = 1 - \text{correctness}, \tag{6.2}$$

and is strongly influenced by the timing jitter (see Chapter 5). The scaling of the Z-basis QBER with the extinction ratio and X-basis QBER with the dimension and jitter are presented in Fig. 6.1.

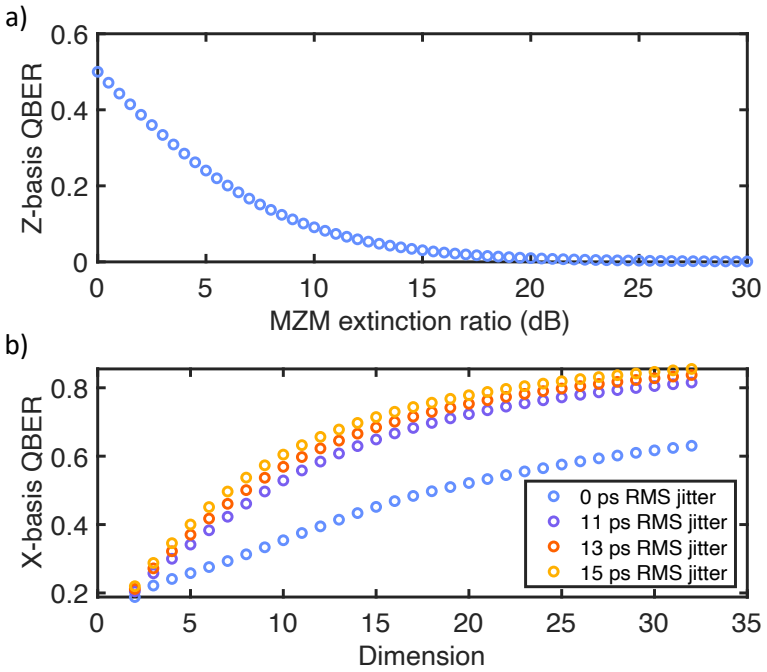

Figure 6.1: QBER in Z and X bases. a) Z-basis QBER scaling with the extinction ratio of the amplitude modulator. b) X-basis QBER scaling with dimension of superposition considering detection based on the temporal Talbot effect.

In the following parts of this chapter, I will introduce two QKD protocols in greater detail.

6.1.1 The high-dimensional BB84 protocol

Below I present an outline of a single measurement round of the standard high-dimensional decoy-state QKD protocol with two decoy states, which is repeated for a sufficient number of rounds [30, 165].

1. Alice prepares a state in the Z-basis with probability p_Z or in the X-basis with probability $1 - p_Z$. When selecting a Z-basis (X-basis) state, Alice randomly chooses a symbol $j \in \{0, \ldots, d-1\}$ ($k \in \{0, \ldots, d-1\}$) uniformly at random and stores it in the variable Z_A (X_A). Then, Alice selects an intensity μ_i from the set $\mathcal{S} = \{\mu_1, \mu_2, \mu_3\}$ with probabilities p_{μ_1}, p_{μ_2}, and $p_{\mu_3} = 1 - p_{\mu_1} - p_{\mu_2}$, storing it in the variable I_A. Based on these selections, Alice prepares the corresponding phase-randomized coherent state $\rho_{Z_j}(\mu_i)$ or $\rho_{X_k}(\mu_i)$ and transmits it to Bob through an insecure quantum channel.

2. Bob randomly chooses to measure the incoming state either in the Z-basis with probability p_Z or in the X-basis with probability $1 - p_Z$. If Bob chooses the Z-basis, he directly measures the photon arrival time. If his detector clicks, returning an outcome j, he records $Z_B = j$. Otherwise, he sets $Z_B = \emptyset$. If Bob chooses the X-basis, he measures the incoming state using an interferometric or analogous setup appropriate for the X-basis. If a click occurs with outcome k, he records $X_B = k$. Otherwise, he sets $X_B = \emptyset$.

3. After the measurement, Alice publicly announces her chosen basis (Z or X) and the intensity I_A. Bob announces his chosen basis (Z or X) and whether or not a detection occurred.

4. If Alice and Bob both choose the Z-basis and Bob obtains a detection ($Z_B \neq \emptyset$), the round is labeled a *key generation round*. All other rounds (including when either party chooses the X-basis or no detection occurs) are classified as *test rounds*. For these rounds, Bob publicly announces the outcome X_B.

5. Both parties estimate the gains for each intensity:

$$G^Z_{\mu_j} = \Pr(Z_B \neq \emptyset | T = Z, I_A = \mu_j), \tag{6.3}$$

$$G^X_{\mu_j} = \Pr(X_B \neq \emptyset | T = X, I_A = \mu_j). \tag{6.4}$$

6. Bob discloses outcomes Z_B for a subset of the key-generation rounds, enabling Alice to estimate the quantum bit error rate (QBER) for each intensity:

$$Q_{Z,\mu_j} = \Pr(Z_A \neq Z_B | T = Z, I_A = \mu_j, Z_B \neq \emptyset). \tag{6.5}$$

7. Alice also calculates the QBER for the test rounds:

$$Q_{X,\mu_j} = \Pr(X_A \neq X_B | T = X, I_A = \mu_j, X_B \neq \emptyset). \tag{6.6}$$

8. Alice and Bob perform classical error correction and privacy amplification procedures on the subset of undisclosed key-generation rounds, producing a shared secret key.

The asymptotic secret key rate for a d-dimensional BB84 protocol in the 2-decoy variant is given by [162]:

$$r_{\mathrm{BB84}} = p_Z^2 \sum_{j=1}^{3} p_{\mu_j} \Big\{ e^{-\mu_j} \underline{Y_0^Z} \log_2 d + e^{-\mu_j} \mu_j \underline{Y_1^Z} \left[\log_2 d - u(\overline{e_{X,1}}) \right] - G_{\mu_j}^Z u(Q_{Z,\mu_j}) \Big\}, \tag{6.7}$$

where p_Z is the probability to prepare (measure) in the Z basis, while the X basis is chosen with probability $1 - p_Z$. Alice selects the symbol $j \in \{0, \ldots, d-1\}$ ($k \in \{0, \ldots, d-1\}$) and intensity $\mu_i \in \mathcal{S} := \{\mu_1, \mu_2, \mu_3\}$ with probabilities p_{μ_1}, p_{μ_2} and $p_{\mu_3} = 1 - p_{\mu_1} - p_{\mu_2}$. An upper bound on the bit error rate in the control basis is denoted as $\overline{e_{X,1}}$, $\underline{Y_0^Z}$ and $\underline{Y_1^Z}$ are 0 and 1-photon yields in the Z-basis, $G_{\mu_j}^Z$ and Q_{Z,μ_j} are respectively the gain and QBER corresponding to a state with μ_j mean photon number.

The function $u(x)$ appearing in (6.7) is defined as:

$$u(x) = \begin{cases} h(x) + x \log_2(d-1) & \text{if } x \in \left(0, 1 - \frac{1}{d}\right) \\ \log_2 d & x \in \left[1 - \frac{1}{d}, 1\right), \end{cases} \tag{6.8}$$

with $h(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ the binary entropy.

The following key rate values were simulated for $\mathrm{QBER}_z = 0.5\%$, which is experimentally-feasible due to modulator's ER, and $QBER_x$ values corresponding to 0 ps, 25 ps, 30 ps, and 35 ps FWHM jitter values and detection method based on the temporal Talbot effect (see Fig. 6.1). These jitter values are experimentally feasible and typical for SNSPD-based detection systems. Additional experimentally relevant parameters used in the simulations—such as detection efficiency and Bob's loss—are provided in Section 6.2.1. Simulated key rate values are presented in figures 6.2, 6.3, 6.4, 6.5.

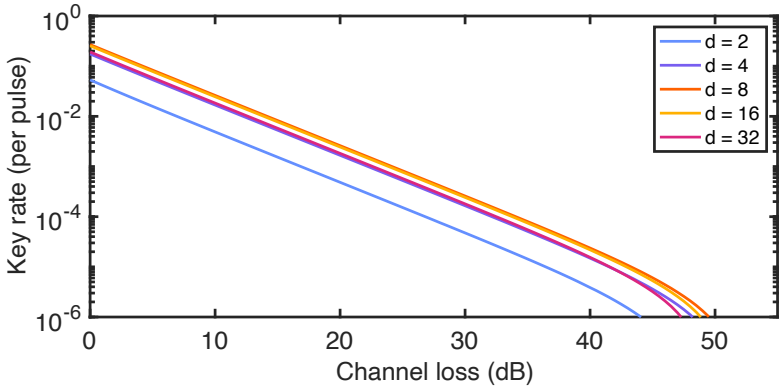

Figure 6.2: Secret key rate values simulated for a range of dimensions and QBER_x corresponding to 0 ps jitter.

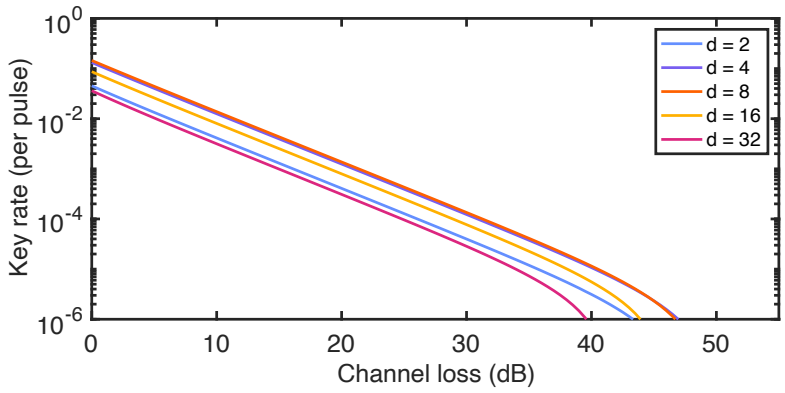

Figure 6.3: Secret key rate values simulated for a range of dimensions and $QBER_x$ corresponding to 25 ps jitter.

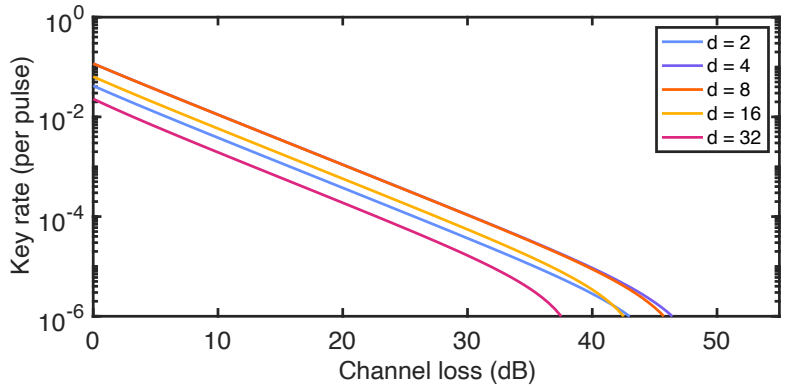

Figure 6.4: Secret key rate values simulated for a range of dimensions and $QBER_x$ corresponding to 30 ps jitter.

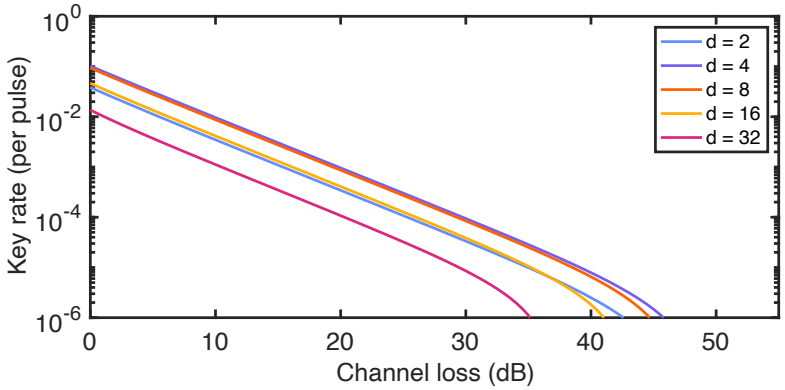

Figure 6.5: Secret key rate values simulated for a range of dimensions and $QBER_x$ corresponding to 35 ps jitter.

For cases with no jitter and with 25 ps FWHM jitter, the highest key rate is achieved at $d = 8$. However, the improvement over $d = 4$ is marginal. At higher jitter values, $d = 4$ consistently yields the highest key rates. Consequently, the experimental implementation will utilize $d = 4$ alongside the qubit case to enable a direct comparison between binary and high-dimensional encoding schemes.

6.1.2 The tunable beam splitter protocol

In the following section, I highlight potential security issues related to the setup and QKD systems in general, particularly those arising from basis-dependent detection probabilities. I analyze these concerns in the context of our setup and discuss them in light of recent theoretical developments.

Many QKD protocols allow measurement rounds to be discarded if the receiver does not detect a photon in any basis. The standard decoy-state BB84 d-dimensional protocol, discussed in Section 6.1.1, follows this approach and assumes that the probability of accepting a round is the same for both measurement bases. In other words, the positive operator-valued measure (POVM) elements corresponding to the rejected rounds should be identical for both the X and Z bases. However, in my setup, the detection efficiencies differ between the two bases. Additionally, in the X basis, an extra insertion loss is introduced by the dispersion-compensating module. This violates the assumption of basis-independent detection efficiency required by the standard security proof [162]. A possible solution is to introduce an additional attenuator in the Z basis.

Detection efficiency mismatches can arise due to several factors, such as the use of delay-line interferometers or modulators in one measurement basis, differences in the efficiency or quality of single-photon detectors, and variations in their dark count rates. Moreover, asymmetric detection efficiencies can also be mode-dependent. For example, single-photon detectors may exhibit different efficiencies depending on the wavelength of the incoming signal. In some cases, this issue can be mitigated by using sufficiently narrow spectral filters before the detectors. However, even if identical detectors were used for both bases, the time-frequency mode dependence of the measurements introduces additional complexities. The dispersion-compensating module introduces wavelength-dependent delays, coupling time and wavelength in a way that is not unique to our setup but is common in spectral-temporal QKD implementations [118, 58, 122]. These delays could shift the signal outside the detection window, reducing detection efficiency in the X basis compared to the Z basis. Similarly, tailored pulses designed to yield a specific outcome in the X basis might partially fall outside the Z basis time window, leading to asymmetric detection probabilities. Discrepancies between theoretical security proofs and real-world experimental implementations can create vulnerabilities that may be exploited in quantum hacking attacks. Such mismatches are common in practical systems. For example, a recent attack on BB84 protocols leveraging asymmetric detectors is discussed in [162]. In real QKD systems, it is impossible to ensure perfectly equal and mode-independent detection probabilities in both bases. Even discrepancies smaller than standard measurement errors in device characterization could, in principle, be exploited by an adversary. Including these discrepancies in security proofs enhances the robustness of real-world implementations. In the following sections, I will discuss a recently proposed global approach to addressing basis detection efficiency mismatches and examine its implications in an experimental context.

Reference [162] presents an analytical security proof that eliminates the assumption of equal detection efficiency for the two bases. The protocol incorporates a tunable beam splitter (TBS) on Bob's side, enabling rapid switching between measurement bases (see Fig. 6.6). In this framework, the TBS is modeled as a realistic device with finite switching contrast, where the maximum and minimum transmission levels are denoted as $\eta_{\downarrow}$ and $\eta_{\uparrow}$, respectively, with η_2

representing an intermediate state.

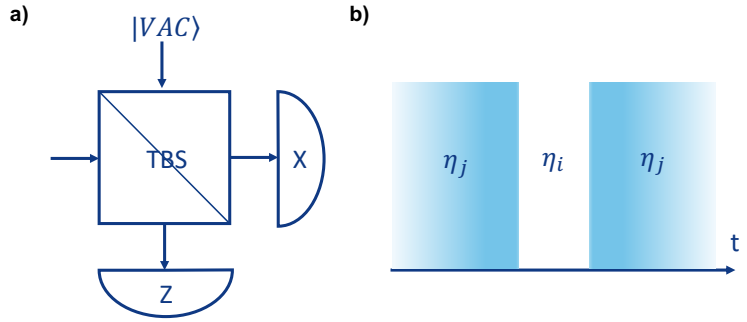

Figure 6.6: TBS protocol schematic. a) A conceptual tunable beam splitter. b) Time-dependent transmission of a tunable beam splitter.

The TBS can alternate its transmission from η_j to η_i and then revert back to η_j, with the period during which the transmission equals η_i aligning with the Z basis time window. To ensure the validity of the security proof, certain assumptions regarding the three possible transmission values must be met:

$$\eta_\uparrow > \frac{\eta_\downarrow}{1-\eta_\downarrow}, \tag{6.9}$$

$$\frac{\eta_X}{\eta_Z} > (\eta_\downarrow)^{-1}\left(1-\sqrt{1-\frac{\eta_\downarrow}{\eta_\uparrow}}\right), \tag{6.10}$$

$$\eta_\downarrow < \eta_2 < \eta_\uparrow. \tag{6.11}$$

In our analysis, we adopt a near-optimal choice for the intermediate transmission, given by:

$$\eta_2 = (1/4)(\sqrt{\eta_\downarrow}+\sqrt{\eta_\uparrow})^2. \tag{6.12}$$

The TBS could be implemented using a dual-output Mach-Zehnder modulator (MZM) [122]. This type of MZM is readily available in generic photonic integrated technology and has previously been used to balance detection efficiencies in a QKD experiment utilizing photonic integrated circuits [82].

The following outlines a single measurement round of the protocol, which must be repeated for a sufficient number of rounds.

1. Alice prepares a state in the Z-basis with probability p_Z or in the X-basis with probability $1-p_Z$. When selecting a Z-basis (X-basis) state, she randomly chooses a symbol $j \in \{0,\ldots,d-1\}$ ($k \in \{0,\ldots,d-1\}$) with uniform probability and records it in the random variable Z_A (X_A). Next, she selects an intensity μ_i from the set $\mathcal{S} := \{\mu_1,\mu_2,\mu_3\}$ with probabilities p_{μ_1}, p_{μ_2}, and $p_{\mu_3} = 1-p_{\mu_1}-p_{\mu_2}$, storing it in the random variable I_A. Based on these choices, Alice prepares the phase-randomized coherent state $\rho_{Z_j}(\mu_i)$ ($\rho_{X_k}(\mu_i)$) and transmits it to Bob over an insecure quantum channel.

2. In each round, Bob selects one of seven possible TBS settings: $(\eta_i,\eta_\uparrow)$ for $i=1,2,3$, $(\eta_i,\eta_\downarrow)$ for $i=1,2,3$, or (η_2,η_2). The transmittances are defined as follows: $\eta_1=\eta_\uparrow$, $\eta_3=\eta_\downarrow$, η_2 satisfies $\eta_\downarrow<\eta_2<\eta_\uparrow$, and they obey relations 6.9, 6.10, 6.11. We use a nearly optimal

setting given by eq. 6.12. Specifically, Bob chooses the setting $(\eta_\downarrow, \eta_\downarrow)$ with probability p_Z, and each of the other six settings with probability $(1-p_Z)/6$. If the Z (X) detector clicks and returns outcome j (k), Bob assigns $Z_B = j$ ($X_B = k$). If the Z (X) detector does not click, Bob assigns $Z_B = \emptyset$ ($X_B = \emptyset$).

3. Rounds where $T = Z$, $Z_B \neq \emptyset$, and Bob has chosen the TBS setting $(\eta_\downarrow, \eta_\downarrow)$ are classified as *key generation rounds*. All other rounds are categorized as *test rounds*. For test rounds, Bob also publicly announces the value of X_B.

4. Gains estimation: Based on the publicly shared information, both parties estimate the gains in the Z-basis:

$$G^Z_{\mu_j,(\eta_l,\eta_l)} = \Pr(Z_B \neq \emptyset | T = Z, I_A = \mu_j, (\eta_l, \eta_l)), \tag{6.13}$$

for each $\mu_j \in \mathcal{S}$ and $\eta_l \in \{\eta_\uparrow, \eta_2, \eta_\downarrow\}$. They also estimate the X-basis gains:

$$G^{X,}_{\mu_j,(\eta_i,\eta_l)} = \Pr(X_B \neq \emptyset, Z_B \neq \emptyset | T = X, I_A = \mu_j, (\eta_i, \eta_l)) \tag{6.14}$$

$$G^{X,\emptyset}_{\mu_j,(\eta_i,\eta_l)} = \Pr(X_B \neq \emptyset, Z_B = \emptyset | T = X, I_A = \mu_j, (\eta_i, \eta_l)), \tag{6.15}$$

for $\mu_j \in \mathcal{S}$ and for $\eta_i \in \{\eta_\uparrow, \eta_2, \eta_\downarrow\}$ and $\eta_l \in \{\eta_\uparrow, \eta_\downarrow\}$.

5. Errors estimation: Bob discloses Z_B for a subset of the key generation rounds, allowing Alice to calculate the QBER for these rounds, categorized by the intensity levels she selected.

$$Q_{Z,\mu_j} = \Pr(Z_A \neq Z_B | T = Z, I_A = \mu_j, (\eta_\downarrow, \eta_\downarrow), Z_B \neq \emptyset). \tag{6.16}$$

Alice also calculates the QBERs for the test rounds in which a detection occurs in the X-basis detector (referred to as the X-basis QBERs):

$$\begin{aligned} &Q_{X,\mu_j,(\eta_i,\eta_\uparrow),} = \\ &\Pr(X_A \neq X_B | T = X, I_A = \mu_j, (\eta_i, \eta_\uparrow), X_B \neq \emptyset, Z_B \neq \emptyset) \end{aligned} \tag{6.17}$$

$$\begin{aligned} &Q_{X,\mu_j,(\eta_i,\eta_\uparrow),\emptyset} = \\ &\Pr(X_A \neq X_B | T = X, I_A = \mu_j, (\eta_i, \eta_\uparrow), X_B \neq \emptyset, Z_B = \emptyset), \end{aligned} \tag{6.18}$$

for $\eta_i \in \{\eta_\uparrow, \eta_2, \eta_\downarrow\}$ and $\mu_j \in \mathcal{S}$.

6. Through error correction and privacy amplification, the parties derive a shared secret key from the variables Z_A (Alice) and Z_B (Bob), considering only the key generation rounds in which Bob did not disclose Z_B.

The asymptotic key rate formula stemming from infinitely many rounds for this protocol is given by:

$$\begin{aligned} r_\infty = & p_Z^2 \sum_{j=1}^{3} p_{\mu_j} \Big\{ e^{-\mu_j} \underline{Y^Z_{0,(\eta_\downarrow,\eta_\downarrow)}} \log_2 d \\ & + e^{-\mu_j} \mu_j \underline{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}} \left[\log_2 \left(\frac{1}{c} \right) - u(\overline{\tilde{e}_{X,1}}) \right] \\ & - G^Z_{\mu_j,(\eta_\downarrow,\eta_\downarrow)} u(Q_{Z,\mu_j}) \Big\}, \end{aligned} \tag{6.19}$$

The c term is a compatibility factor for Alice's states within the one-photon subspace [166]. The key rate is maximized when the compatibility coefficient is minimized (i.e., $c = 1/d$), which occurs when Alice's states in the one-photon subspace form two mutually unbiased sets. Additionally, the statistical lower bound on the n-photon yield in the Z-basis is denoted as $\underline{Y^Z_{n,(\eta_l,\eta_l)}}$. This represents the probability that a Z-detector registers a click, given that n photons were sent by Alice and Bob selected the TBS setting (η_l, η_l). The explicit expressions, derivations and proofs for $\underline{Y^Z_{1,(\eta_\downarrow,\eta_\downarrow)}}$, $\underline{Y^Z_{0,(\eta_\downarrow,\eta_\downarrow)}}$, and other bounds on yields and bit error rates appearing in $\overline{\tilde{e}_{X,1}}$ are obtained through the decoy-state method and are detailed in [162]. The resulting key rate formula follows a structure similar to that of the BB84 protocol (Eq. 6.7). When probability of detection of any signal is independent of the measurement basis, the expression for the phase error rate is equal for the TBS protocol and the BB84 protocol. This is valid under assumption that the phase error is measured in the test basis. The simulated secret key rate values for the TBS protocol and experimentally-feasible parameters are presented figures 6.7, 6.8, 6.9, 6.10.

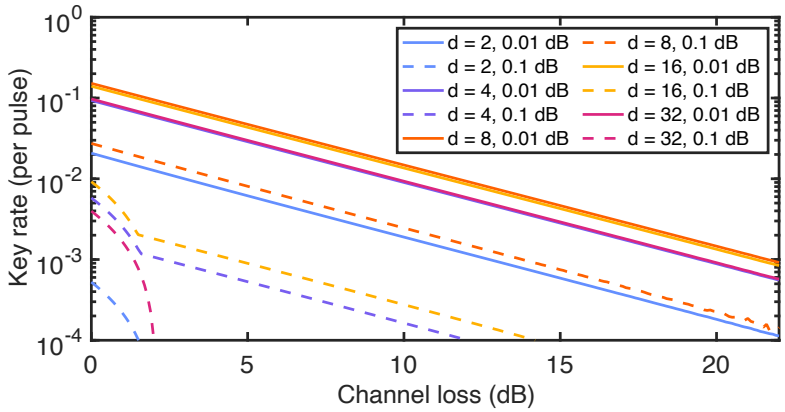

Figure 6.7: Secret key rate values simulated for a range of dimensions and $\mathrm{QBER_x}$ corresponding to 0 ps jitter. Solid lines correspond to 0.01 dB, and dashed lines to 0.1 dB detection efficiency mismatch between X and Z basis.

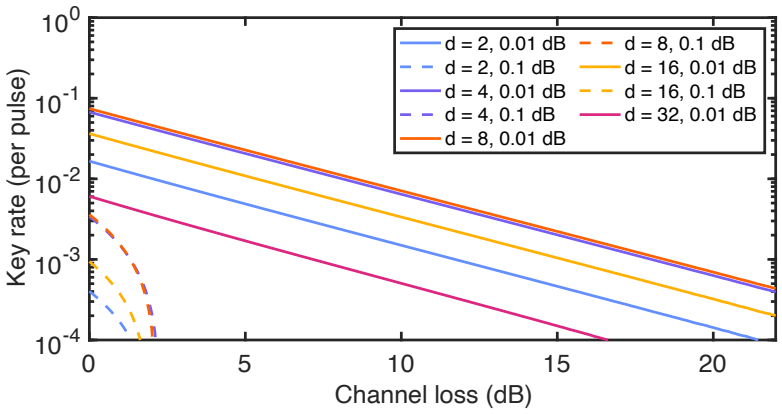

Figure 6.8: Secret key rate values simulated for $QBER_x$ corresponding to 25 ps jitter. Solid lines correspond to 0.01 dB, and dashed lines to 0.1 dB detection efficiency mismatch between X and Z basis.

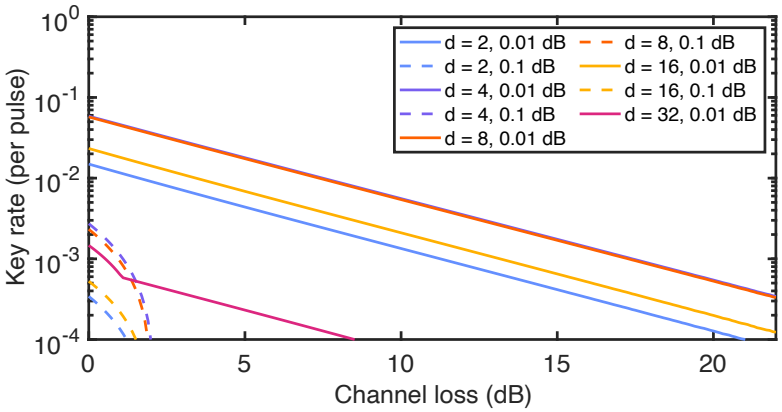

Figure 6.9: Secret key rate values simulated for $QBER_x$ corresponding to 30 ps jitter. Solid lines correspond to 0.01 dB, and dashed lines to 0.1 dB detection efficiency mismatch between X and Z basis.

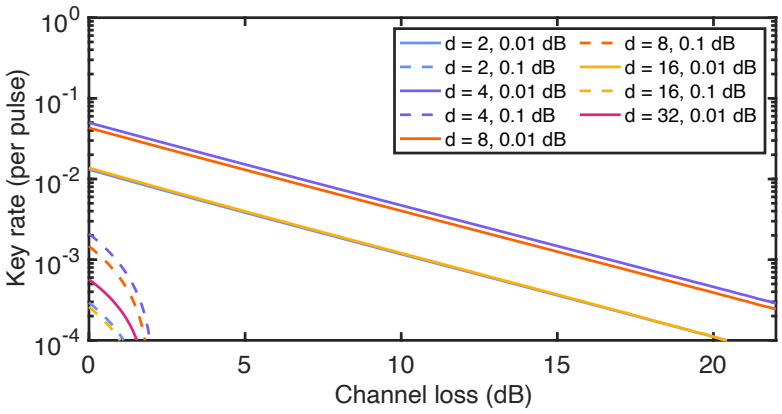

Figure 6.10: Secret key rate values simulated for $\mathrm{QBER_x}$ corresponding to 35 ps jitter. Solid lines correspond to 0.01 dB, and dashed lines to 0.1 dB detection efficiency mismatch between X and Z basis.

As in the case of the BB84 protocol, the highest key rate values are observed for $d = 4$ and $d = 8$, depending on the amount of jitter. Simulation results indicate that the resulting key rate is highly sensitive not only to timing jitter but also to detection efficiency mismatch. In particular, a mismatch greater than 0.01 dB leads to a substantial drop in the achievable key rate.

6.2 Experimental high-dimensional quantum key distribution

In this section I describe the key experiment of the thesis.

6.2.1 The QKD setup

The general setup for the QKD experiment is presented in Fig. 6.11 The distributed-feedback (DFB) laser operating at the telecommunication wavelength of 1560 nm in CW mode was used as the main optical source. The optical signal was amplified with an erbium-doped fiber amplifier (EDFA, Pritel, HPP-PMFA-22-10), and a bandpass spectral filter was employed to reduce the noise and provide sufficient power for a feedback loop, which will be discussed later. The optical signals and decoy states for both the bases were generated by means of cascaded fast electro-optic amplitude modulation with a pair of MZMs (Thorlabs, LNA6213). Both MZMs were biased for extinction with the DC voltage from a stable power supply (Keysight, E36313A) using the feedback loop, which consisted of a 90 : 10 fiber optic beam splitter and a power meter (Thorlabs, PM400) (not shown in Fig. 6.11). The second modulator was biased with another feedback loop, which comprised a separate CW laser for calibration, a power meter, an isolator, and a switch that was used to cut off the calibration laser during key distribution. The mean photon numbers were controlled by driving both the modulators ($\mu 1$), one modulator ($\mu 2$), or none of them ($\mu 3$). The mean photon numbers for in-lab and infrastructural experiments were set to $\mu_1 = 0.06$, $\mu_2 = 6.59 \cdot 10^{-4}$, $\mu_3 = 1.89 \cdot 10^{-4}$ and $\mu_1 = 0.19$, $\mu_2 = 2.11 \cdot 10^{-3}$, $\mu_3 = 3.10 \cdot 10^{-4}$, respectively. These values were determined by analyzing histograms corresponding to one of the Z-basis symbols. Similarly, the dark count probability used for theoretical key rate

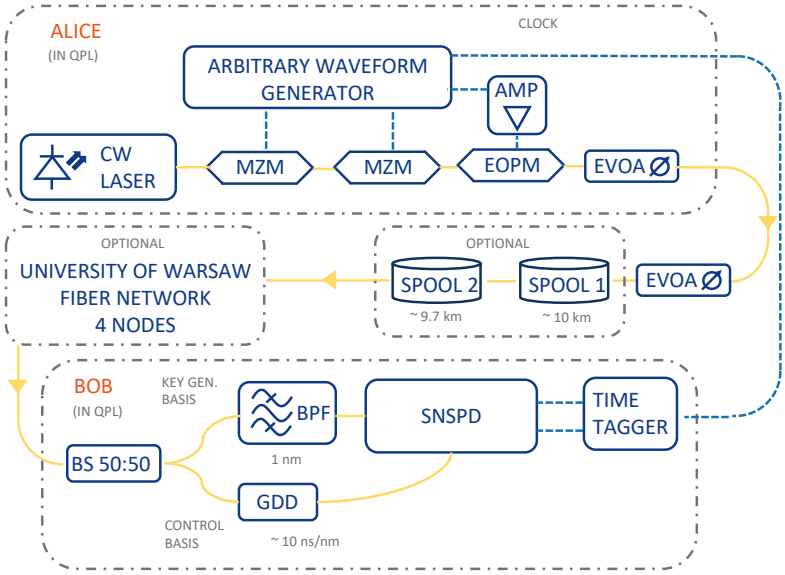

Figure 6.11: The key components of the experimental setup. A CW laser undergoes modulation using a MZM and a EOPM to produce optical pulses, which form superpositions and are used as signal and decoy states. These optical signals are attenuated to the single-photon level with a EVOA. Another EVOA is used to control the attenuation of the quantum channel. To simulate real-world propagation, two optical fiber spools (spool 1 and spool 2) are included in the setup. Alternatively, the quantum channel can utilize dark fibers from the University of Warsaw's urban fiber network, enabling measurements over fixed distances by forming a fiber loop (see Fig. 6.21). The optical signals are directed toward a switch, which determines whether they are measured directly in the key generation basis (Z-basis) or in the control basis (X-basis). In the Z-basis, the signals are detected using time-correlated single-photon counting. In the X-basis, measurement is performed using the temporal Talbot effect, achieved with a DCM that provides GDD. Both Alice and Bob are positioned in the Quantum Photonics Laboratory (QPL) at the Faculty of Physics, University of Warsaw. Optical fiber connections are depicted as yellow lines, while dashed blue lines represent RF cables.

calculations was obtained by recording histogram data while no optical signal was transmitted to the detectors. The measured probability was 2×10^{-7}. Subsequently, adequate phases (Fig. 5.6) were applied to each component of the superposition using an EOPM (EOspace). It should be noted that the EOPM can also be used for phase randomization to eliminate coherence between subsequent rounds [167, 96]. All of the modulators supported 40 GHz of usable analog bandwidth. The RF driving signals were generated with a fast AWG (Keysight, M1896A), which provided a sampling rate of up to 92.16 GSa/s and 35 GHz of analog bandwidth. The phase factors were adjusted using the EOPM by programming four driving voltage signals consisting of approximately 150-ps-wide rectangular pulses, such that their amplitudes corresponded to fractions or multiples of the phase modulator half-wave voltage (V_π).Three samples of AWG memory were used to generate a single optical pulse. The RF signals driving the EOPM were also amplified with a high-bandwidth RF amplifier (RFLambda RFLUPA01G31GHz). The AWG also served as a source for the 10 MHz clock signal, which was distributed over an electrical cable to Bob. Finally, weak coherent states were generated by attenuating optical symbols to the single-photon level using an EVOA (Thorlabs, EVOA1550F). To demonstrate the feasibility

of our approach, a pre-programmed random sequence of symbols occupying 510720 samples of AWG's memory was used. The sequence was then transmitted for 1 minute at each μ level, for different quantum channel attenuations. For the in-laboratory measurements, the attenuation was set with another EVOA up to 20 dB. For convenience, the measurements were performed with a beam splitter, which distributed the signal to two detectors, effectively adding 3 dB of attenuation. Additionally, two approximately 10-km-long spools of single-mode fiber were added to simulate a real link, which contributed 4.24 dB of attenuation (including the insertion loss of the EVOA). To further demonstrate the feasibility, measurements were performed over deployed dark fiber infrastructure (Fig. 6.21) by creating a fiber loop that reached the desired destination and reflected the signal back to the Quantum Photonics Laboratory. Data were acquired for every available node with and without the two fiber spools. The measurement basis on the receiver side was manually switched. The niobium-nitride SNSPDs were used for time-domain measurements (Single Quantum). The detector efficiency was reported to be 84% according to the calibration data provided by the manufacturer. Detection events were registered with a time-to-digital converter set to 1-ps-wide bins (Swabian Instruments, Time Tagger Ultra). The SNSPDs exhibited a jitter of 5 ps RMS, and the time tagger had a jitter of 10 ps. Therefore, Bob's resultant jitter was 11 ps RMS. To measure in the control basis, the photons were additionally transmitted through a chirped-fiber-Bragg-grating-based DCM, resulting in dispersive temporal broadening of the pulses. The measured insertion loss of the DCM was 2.67 dB, which constituted the main contribution to the detection loss in the X basis. The contribution from other sources of optical loss was below 0.2 dB, primarily due to fiber connector losses. The DCM provided GDD of 12900 ps^2, equivalent to 562 km of SMF-28 fiber. This amount of dispersion enabled the observation of the temporal Talbot effect [130], which was used to distinguish superpositions of the optical signals with different phases, as discussed in chapter 5. The DCM also acted as a bandpass filter, transmitting wavelengths in the range of 1558-1562 nm. To suppress noise originating from the fiber network, an additional bandpass spectral filter (Haphit FPBP, 1 nm BW) was added in the Z basis.

6.2.2 Calibration

Ensuring reliable operation of the QKD experiment requires that the entire setup maintains stable output power and operating points. First, I measured the laser's output power stability over both long (one hour) and short duration (five minutes). For this and subsequent characterization steps, a calibrated optical power meter with a 3.5% uncertainty was used. The results are illustrated in Fig. 6.12.

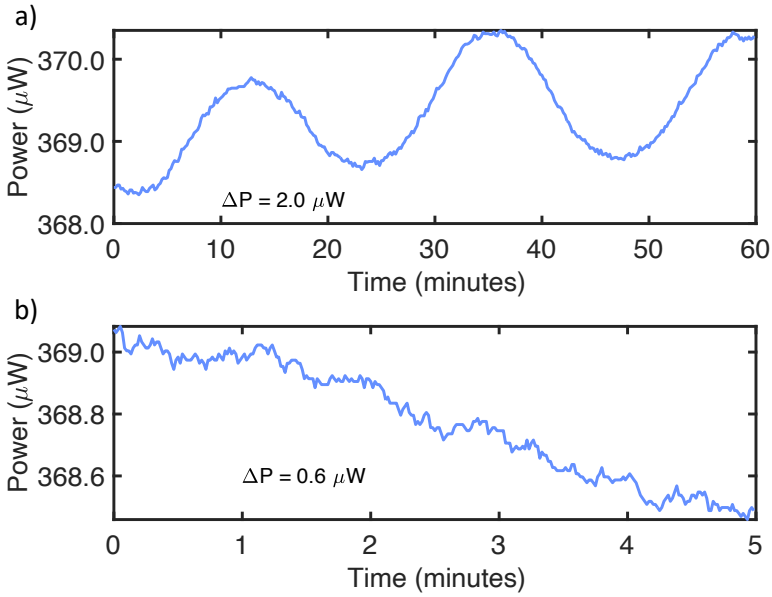

Figure 6.12: Tunable laser source output power stability measurement.

To provide enough power for identifying the MZM operating points, the laser beam was further boosted using an EDFA. Since the EDFA's gain depends on its driving current, Fig.6.13 displays the resulting optical power alongside the corresponding gain.

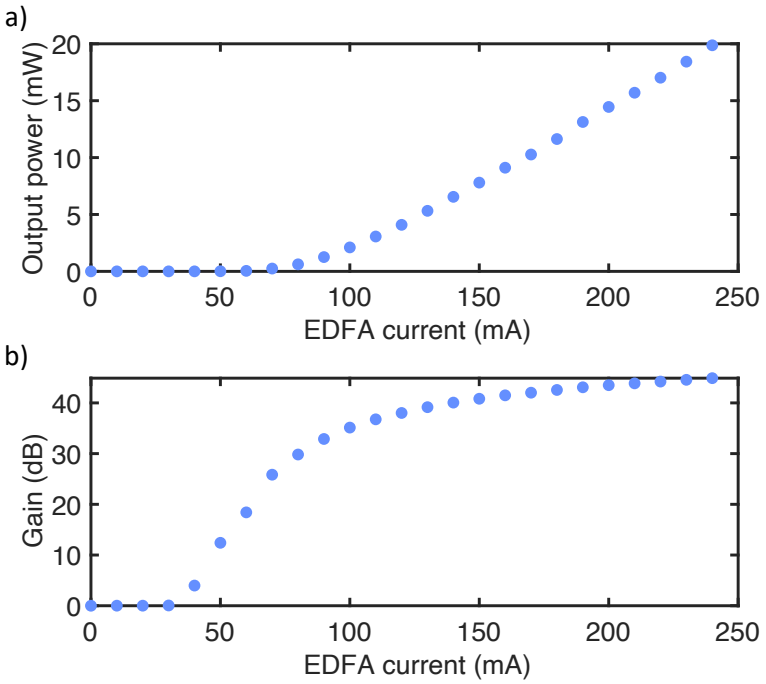

Figure 6.13: EDFA calibration measurement: a) output optical power, b) optical power gain.

To assess the EDFA's impact on the system's stability, the amplified laser power was monitored over both a one-hour and a five-minute period. The findings are shown in Fig. 6.14

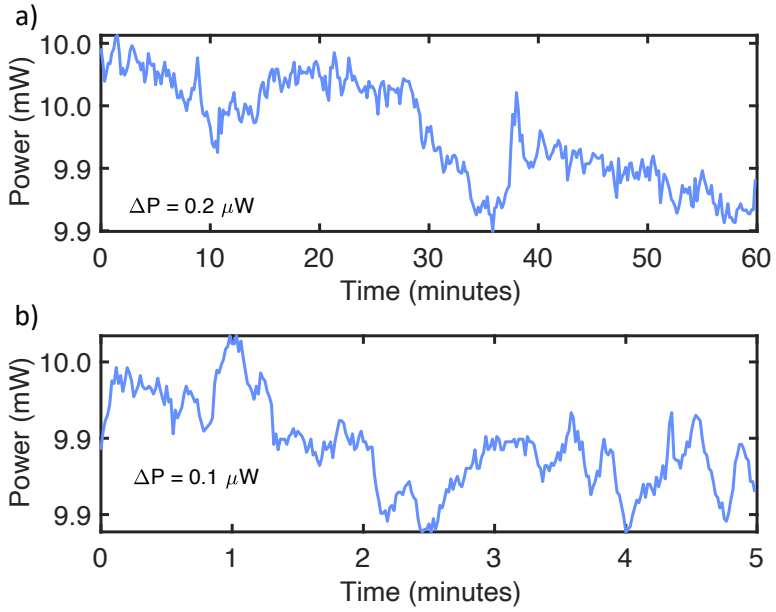

Figure 6.14: EDFA output power stability: a) long-term measurement, b) short-term measurement.

The use of an EDFA provides adequate output power levels while maintaining good stability. After amplification, the beam was directed to the MZM through a bandpass filter to suppress noise from spontaneous emission. The MZM was characterized in terms of its extinction ratio, half-wave voltage, temperature dependency, and operating point stability—evidenced by a drift of its output power. In Fig. 6.15, the transmission is plotted as a function of the driving voltage.

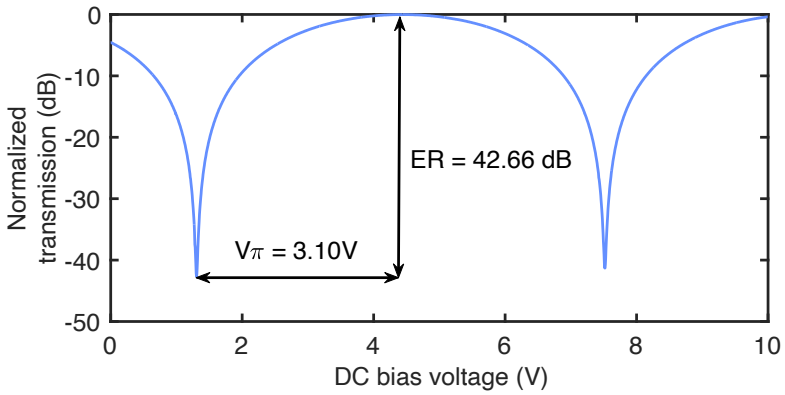

Figure 6.15: Transmission curve of the lithium niobate MZM.

The dependence of the operating point on temperature was investigated using a TEC-controlled micro bench with a cover. For each temperature, the transmission curve was measured to identify the voltage corresponding to the minimal transmission operating point. The results are shown in Fig. 6.16.

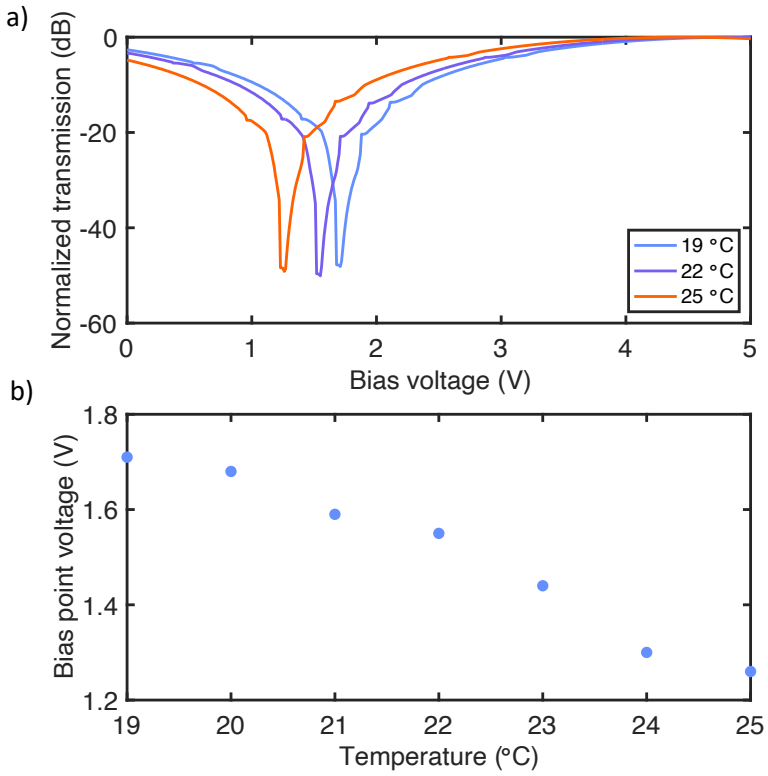

Figure 6.16: Influence of temperature on the minimal transmission operating point of the lithium niobate MZM.

In the laboratory, temperature variations are kept below 1°C, and the modulators are periodically realigned, making temperature dependency negligible. However, experimental findings reveal that overall stability is highly sensitive to the voltage step size used during the biasing process, as well as to the method and range of the voltage scan. It was experimentally verified that the best method is to perform a set of scans in a specific order. The first scan covers a voltage range up to twice the expected value of V_π using a 10 mV step every 10 milliseconds. The second scan, with the same step size and delay, is performed over a narrower range starting at a higher voltage value. Finally, a fine scan over 200 mV with a 1 mV resolution and a 0.5-second delay per step is conducted to bias the modulator for extinction without causing a significant voltage jump that might destabilize its operating point. The effects of this procedure are compared with those of a manual operating point search in Fig. 6.17.

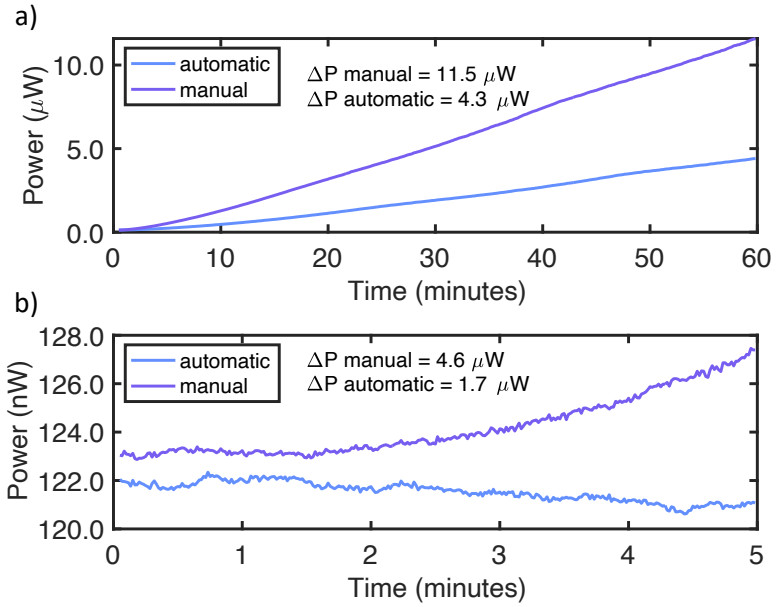

Figure 6.17: MZM bias stability measured for manual and automatic procedure: a) long-term stability, b) short-term stability.

To conduct the QKD experiment, both cascaded MZMs are biased by first performing a coarse scan followed by a fine scan for each of the modulators. The final step in the electro-optic characterization of the modulators involved measuring the dependence of the output pulse width on the number of samples used to program the waveform on the AWG when the modulator was set for extinction. The calibration results are shown in Fig. 6.18. The widths of the pulses were analyzed by finding the FWHM of a histogram measured for 60 s with the time-correlated single-photon counter in the receiver (Bob). Therefore, the results are corrupted by the detection timing jitter.

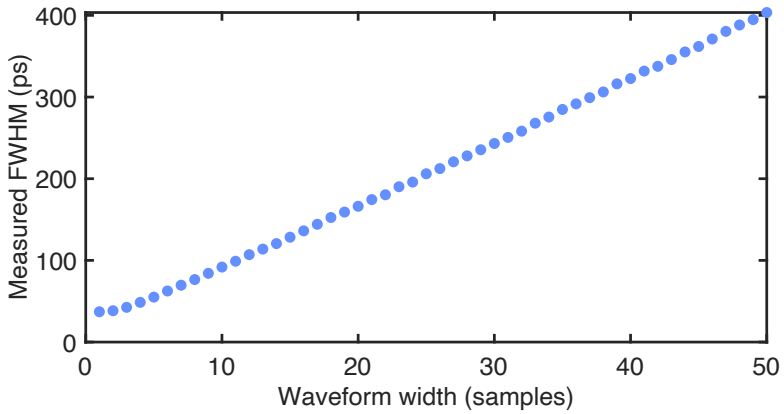

Figure 6.18: Dependency of output pulse duration on number of samples used for programming the waveform on the AWG.

Electrical signals used for generating symbols and modulating the phase of superpositions are presented in Fig. 6.19.

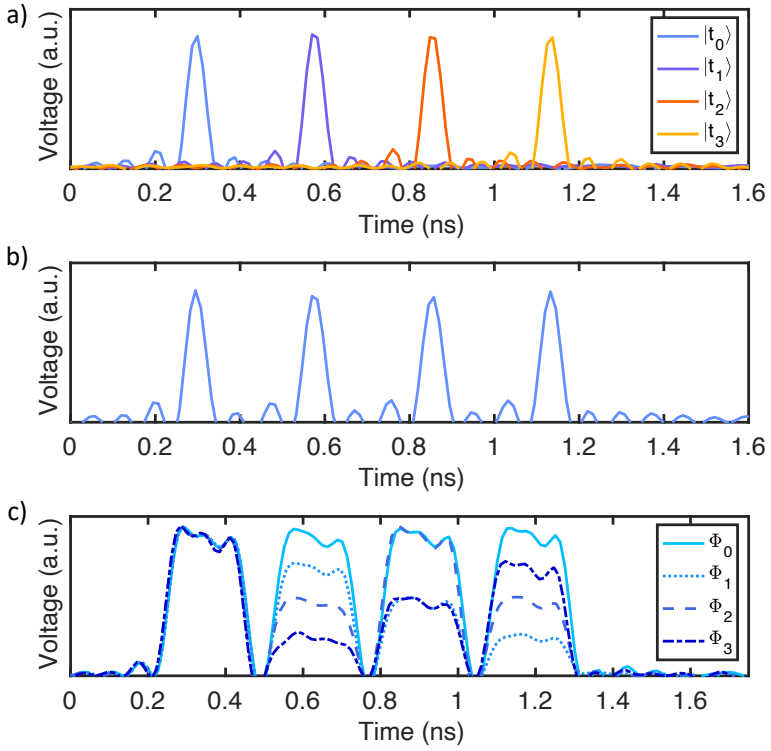

Figure 6.19: Oscilloscope traces of signals generated with the AWG used in the QKD experiment. a) Electrical pulses for generating Z-basis symbols. b) Electrical pulses for generating X-basis symbols. c) Electrical pulses for establishing relative phase difference between different components of the X-basis symbols.

The mean photon number of optical pulses was controlled by driving both MZMs for the μ_1 signal level, one MZM for the μ_2 decoy state 1, or none for the μ_3 decoy state 2. This required finding the delay between different channels of the AWG and ensuring that the delay remained constant. Marker channels were used to maintain a fixed temporal relationship, as they ensure a constant offset relative to the data channel. However, a small residual delay—on the order of tens of picoseconds—remains due to slight differences in the lengths of RF tracks within the AWG. This delay, known as skew, can be compensated for during signal generation by introducing an offset in the digital pattern. The delay between the data channels used for intensity and phase modulation and their corresponding marker channel was measured by analyzing histograms of a fixed symbol. Fine adjustments were made by reprogramming the waveform to introduce small timing offsets. Proper calibration was confirmed by achieving a high extinction ratio, the correct number and shape of peaks, and clearly visible interference fringes in the X basis measurements. Optimizing the visibility, and therefore correctness, required additional fine tuning of the waveform's amplitude. Once calibrated, the setup remained stable and could operate from a cold start without requiring delay adjustments. The resultant signal power levels could be adjusted using the EVOA. The results of the EVOA calibration are presented in the following part of this

chapter. The final optical power stability data for the transmitter measured in neutral conditions are shown in Fig. 6.20.

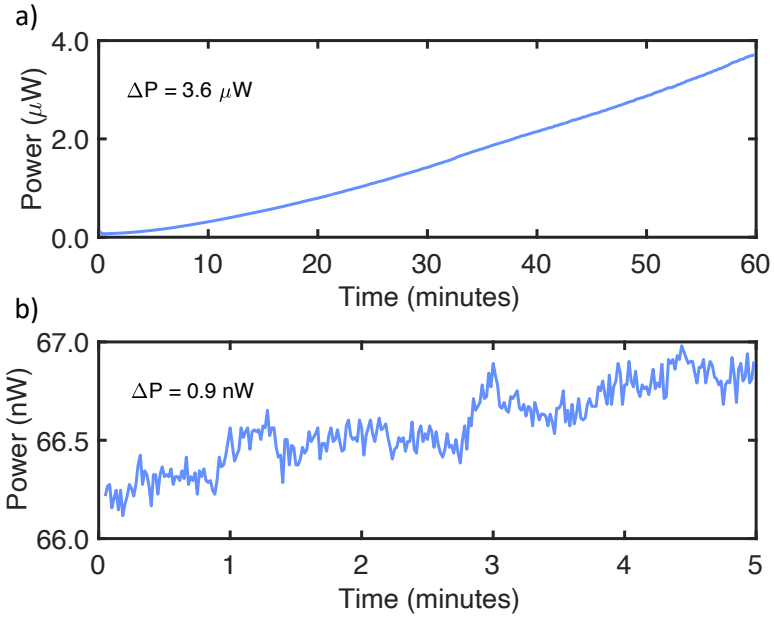

Figure 6.20: QKD transmitter output power stability: a) long-term stability, b) short-term stability.

In QKD the properties of the quantum channel play a crucial role in efficient key exchange. Factors such as loss, noise, and temporal fluctuations directly impact the transmission of quantum states and the overall performance of the protocol. Understanding these characteristics allows optimization of system design, improved error correction, and enhanced eavesdropping detection. In this part of the chapter I present the results of quantum channel characterization and its implications for the QKD experiment.

The fiber-optic quantum channel was set up either in a controlled laboratory environment or using dark fibers from the University of Warsaw's infrastructure. To assess each network node, attenuation and the corresponding key rate were measured by forming a fiber loop with two dark fibers. Attenuation measurements were conducted using a calibrated optical power meter and a tunable laser source (TLS). The nodes and corresponding attenuations are presented in Fig. 6.21.

Meas. point	Attenuation (dB)
1	0.30
2	0.89
3	13.04
4	16.40

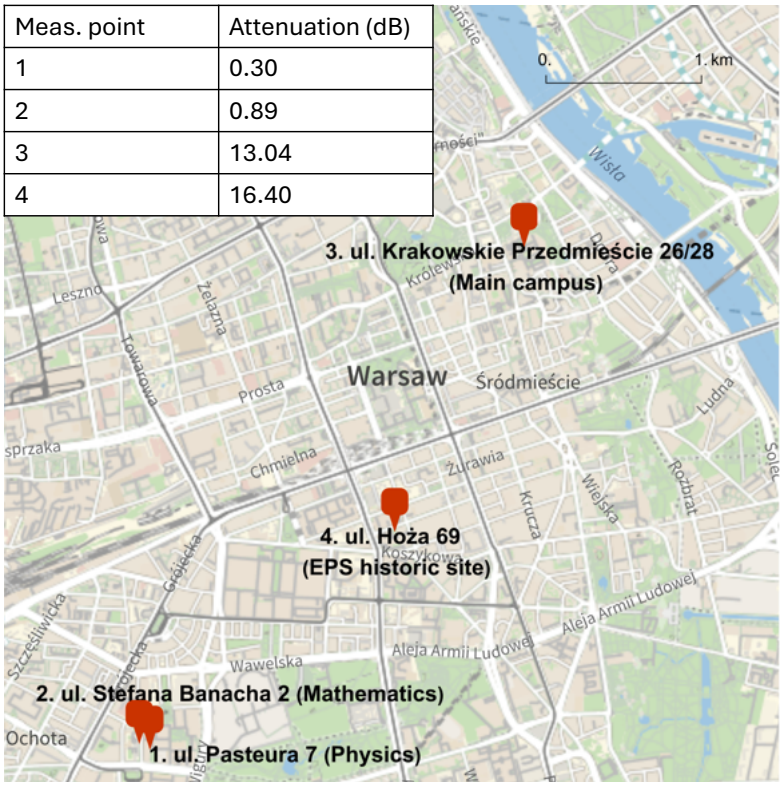

Figure 6.21: The nodes of the University of Warsaw's dark fiber network shown on an OpenStreetMap of central Warsaw. Due to the network's design, signals were transmitted over a 13-km fiber link through the University's southern campus, connecting node 2 to node 3. Node 4 is situated at the former location of the Faculty of Physics, Hoża 69.

Although infrastructure of the University is separate from other networks, measurements detected light leakage from a nearby urban fiber network. The leak of optical power was saturating the single-photon detectors after establishing a connection to the node no. 3 at Krakowskie Przedmieście. The optical spectra of this leakage were recorded using an optical spectrum analyzer set for long acquisition. The results, shown in Fig. 6.22. Spectra reveal peaks corresponding to Cisco L-Band Channels 13, 14, or DWDM ITU Channels $43 - 35.5$, as well as Cisco L-Band Channel 20.

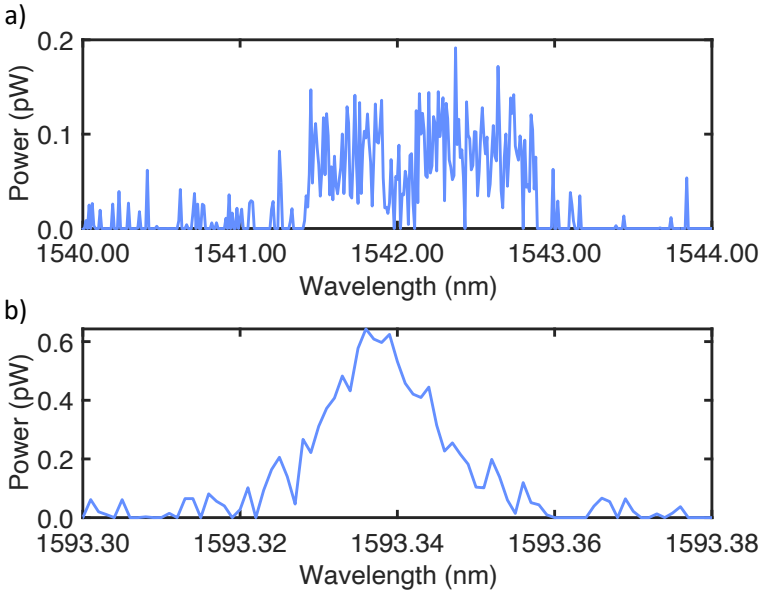

Figure 6.22: Light leak into University's dark fiber infrastructure at: a) Cisco L-Band Channels 13, 14, b) Cisco L-Band Channel 20.

The problem of light leakage was resolved by adding a bandpass filter to the receiver.

The in-laboratory fiber-optic quantum channel was established by connecting Alice to Bob either through a short fiber for back-to-back measurements or via one or two SMF-28 fiber spools, approximately 9.7 km and 10 km in length. Attenuation was controlled using an in-line EVOA, which consisted of a MEMS-based attenuator driven by a voltage source. The attenuator was calibrated and tested for linearity, as well as for its practical range of attenuation. The calibration results for both a quasi home-made and a commercially available EVOA are shown in Fig. 6.23.

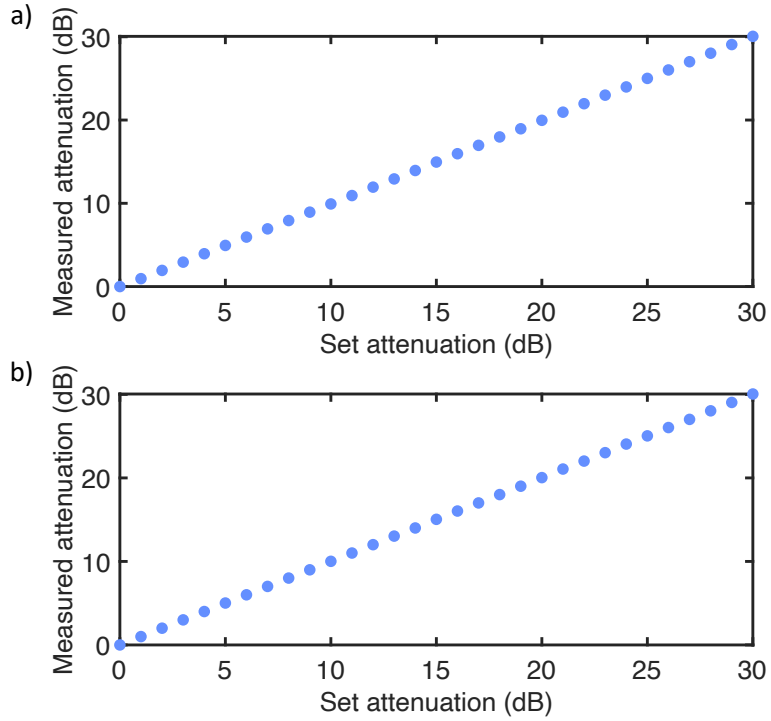

Figure 6.23: Attenuation calibration. a) Thorlabs EVOA b) quasi home-made EVOA.

Both EVOAs offered a sufficient attenuation range to control the mean photon values and simulate quantum channel attenuation equivalent to a maximum propagation distance of 150 km, assuming a standard silica fiber loss of 0.2 dB/km.

The spooled fibers inherently affect pulse width due to dispersion during propagation, as described in Chapter 3. This impact was measured for various input pulse widths, with the results presented in Fig. 6.24. The combined effect of quantum channel and the DCM at the receiver on

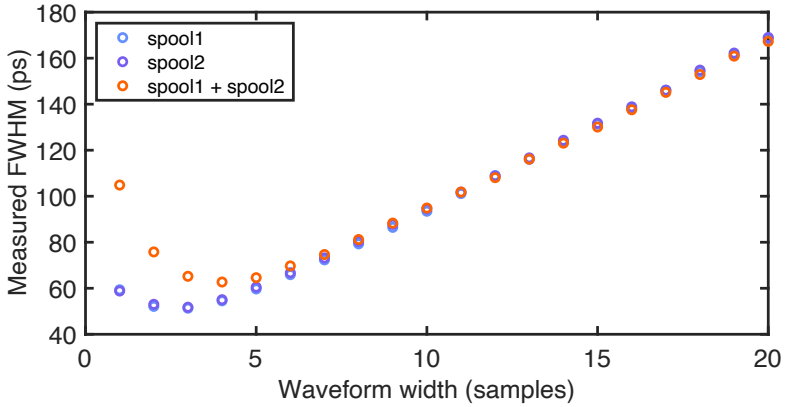

Figure 6.24: Pulse broadening due to propagation via quantum channel comprising either one of the fiber spools, or both spools connected.

the pulse width is visualized in Fig. 6.25. Exemplary pulse evolution due dispersion is illustrated

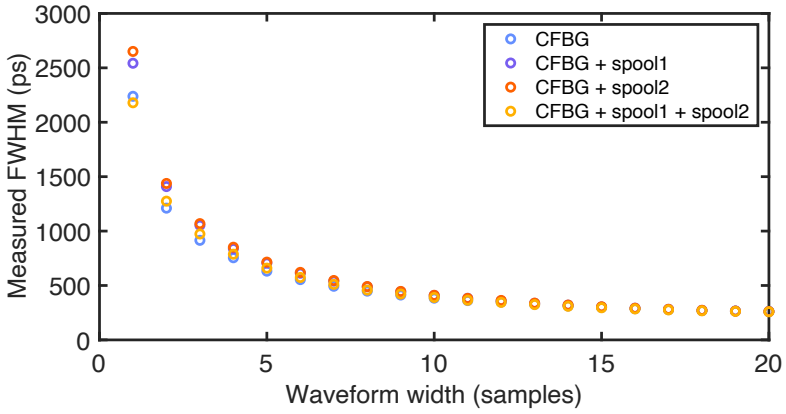

Figure 6.25: Pulse broadening measured at the receiver after the DCM considering a variety of quantum channel fiber lengths.

in Fig. 6.26. The DCM at the receiver has the most significant influence on the resulting pulse width and shape. Due to its substantial dispersion—equivalent to approximately 500 km of standard SMF-28 fiber—it primarily enables detection with the temporal Talbot effect. As a result, the effects of pulse propagation over distances within the city network can be considered negligible. The range of transmitted wavelengths was characterized using a femtosecond pulsed laser in combination with an optical spectrum analyzer, revealing a spectral span of 1558–1563 nm. The corresponding results are shown in Fig. 6.27.

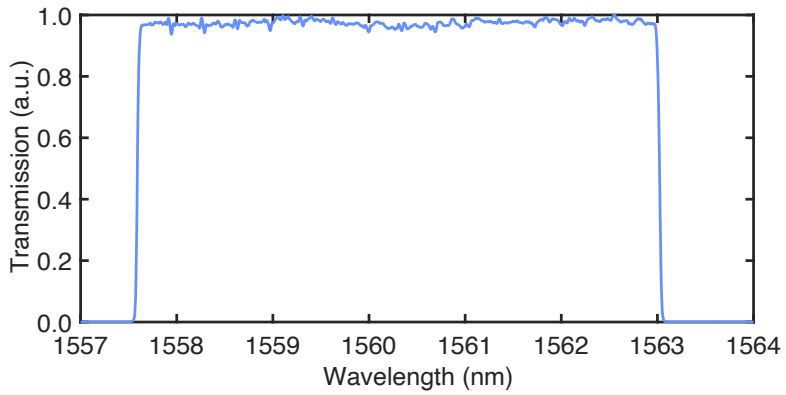

Figure 6.27: DCM transmission measurement.

The transmission is well-linear for a 5-nm-wide wavelength span centered around 1560 nm. The DCM itself acts like a spectral filter, which helps to reduce parasitic light leak which would have increased the QBER.

6.2.3 Symbol detection and secret key rate measurements

The final validation of the setup was performed by measuring histograms of the symbols used for encoding. The data should exhibit a high extinction ratio and strong fringe visibility in the

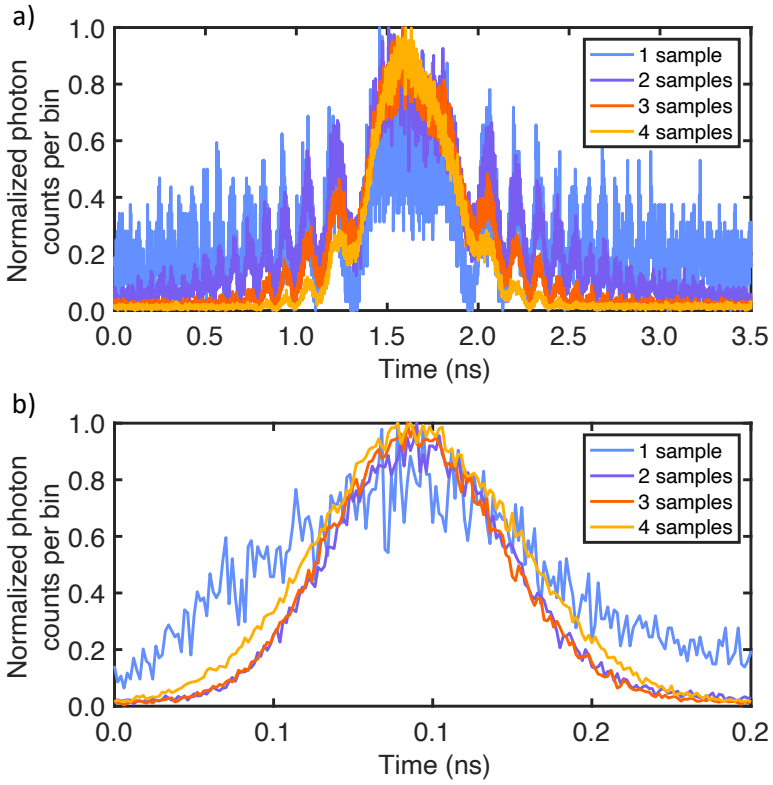

Figure 6.26: The dispersion-induced evolution of pulses measured for input pulse widths corresponding to 1, 2, 3, and 4 samples as generated by the AWG. a) Influence of the DCM. b) Influence of propagation over two fiber spools.

X-basis measurement. Additionally, the symbols should be analyzed in the respective conjugate basis to identify any potential threats to the QKD system. Histograms were recorded for 10 seconds in each case, after biasing both modulators for extinction. They illustrate the symbols that would be used for QKD. The symbols were generated as a pseudo-random sequence long enough to occupy the whole memory of the AWG, implying that some of the peaks may be higher (more probable) than the others. All the symbols presented below were measured using node no. 4 placed at ul. Hoża 69 (the former Faculty of Physics). Measurements for two-dimensional and four-dimensional signal symbols are presented in Figures 6.28 and 6.29.

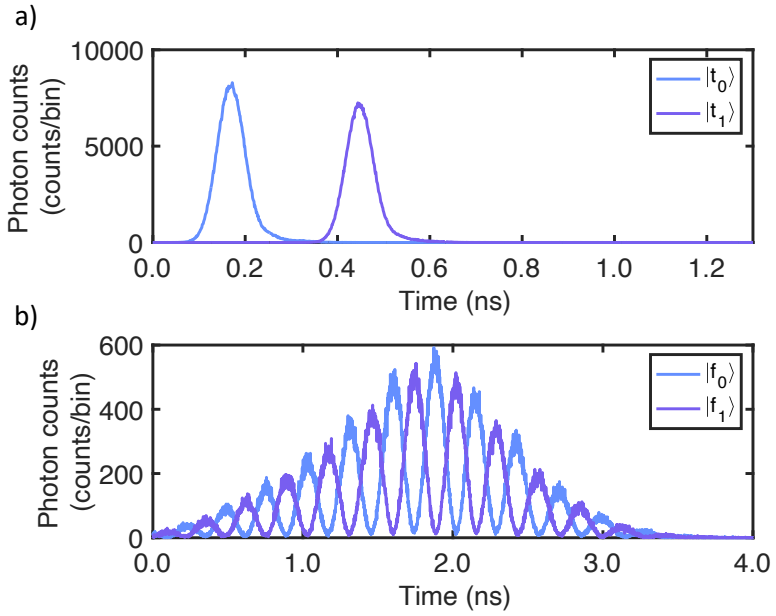

Figure 6.28: Histograms of qubits. a) In the Z basis. b) In the X basis.

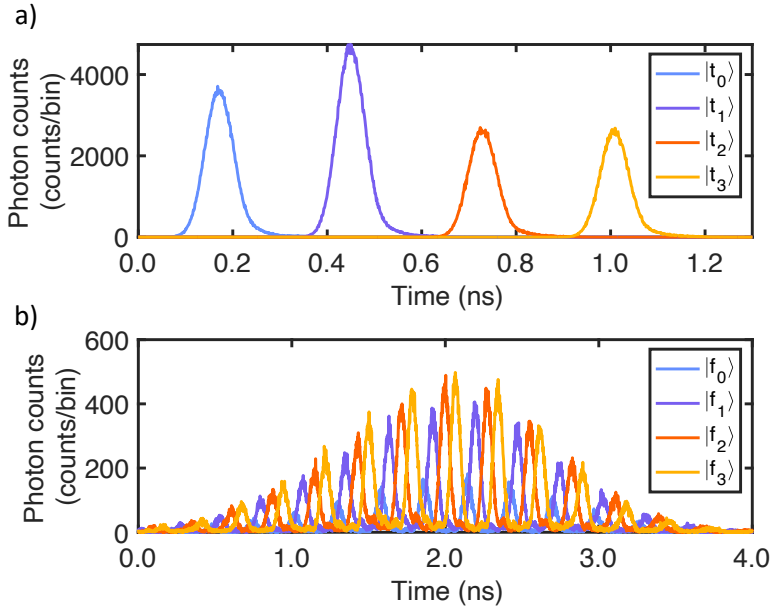

Figure 6.29: Histograms of ququarts. a) In the Z basis. b) In the X basis.

The histograms of the decoy states are lustrated in Fig. 6.30. Even at very low optical power levels the symbols are distinguishable due to high modulation contrast. The general shape of symbols in the conjugate bases was analyzed in the four-dimensional case. The corresponding

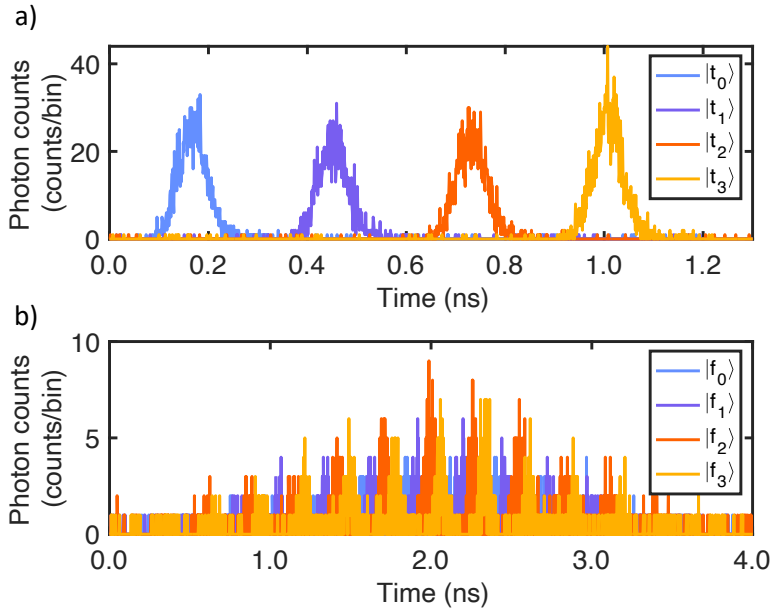

Figure 6.30: Histograms of decoy states μ_2 in a four-dimensional case. a) In the Z basis. b) In the X basis.

histograms are shown in Fig. 6.31.

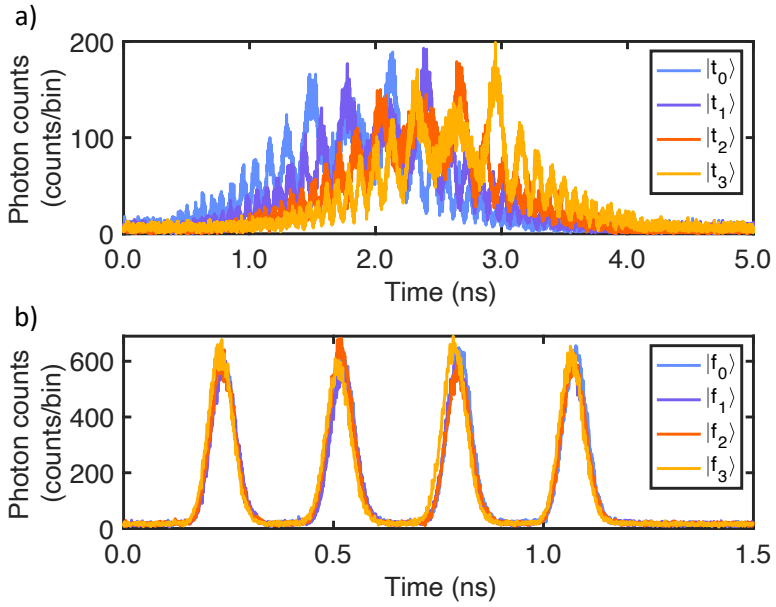

Figure 6.31: Histograms of ququarts in the conjugate bases a) Z-basis symbols measured in the X basis. b) X-basis symbols measured in the Z basis.

The symbols from the control basis are indistinguishable from the symbols belonging to the key generation basis in time domain. The symbols from the key generation basis take a form of stretched pulses in the control basis. They share a common shape and occupy the interval that normally would be occupied by the interference fringes, so contribution from from every key generation basis state is equal. In practice this would satisfy the MUB condition. Moreover, security proof [162] drops the assumption about the independence of the detection probability on of a state from the measurement basis by introducing the compatibility factor c (see eq. 6.19). Similar approach was taken in [113].

After calibrating the transmitter, the receiver, and characterizing the properties of the quantum channel both in the laboratory and within the network infrastructure, I proceeded with the secret key rate measurements. Each measurement was conducted for one minute per intensity level μ, ensuring high modulation contrast necessary for maintaining low Z-basis QBER values. For measurements performed within the laboratory, the quantum channel attenuation was adjusted after each transmission session. In the measurements over the deployed fibers, the connection was switched at a designated node, and the attenuation was measured accordingly.

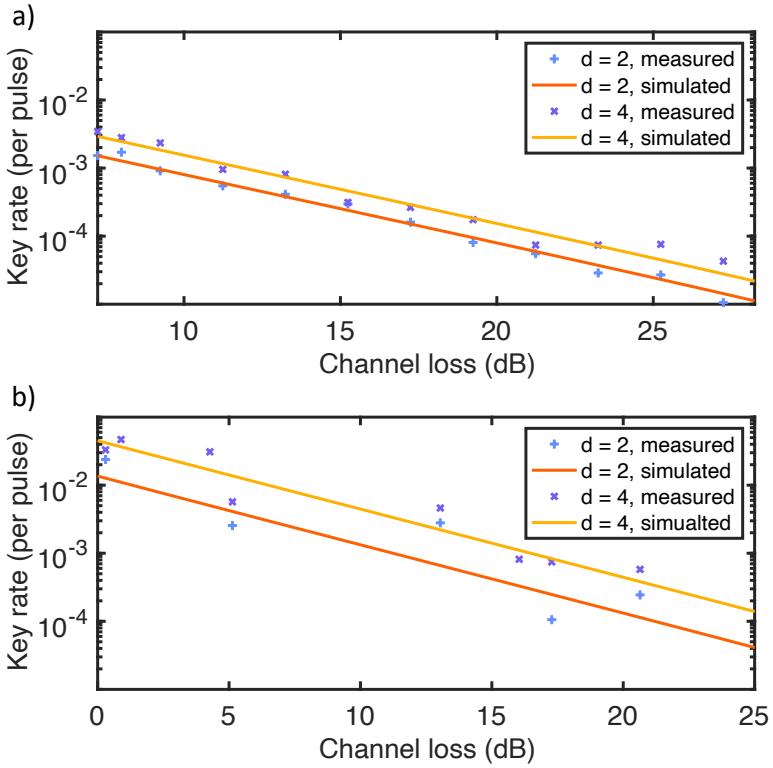

Figure 6.32: Experimentally measured key rates per pulse for two- and four-dimensional encoding. a) In-laboratory measurements, including tests with the two optional fiber spools. b) Measurements over dark fiber infrastructure, both with and without the fiber spools.

To compute the key rates, I applied the standard high-dimensional BB84 formula. A tunable beam splitter (TBS) was not available during the experiments. Additionally, the imbalance introduced by the dispersion compensation module (DCM), combined with the current detection timing jitter, would yield a zero key rate if the TBS protocol formula were used. Nevertheless,

The results obtained within the BB84 framework from the in-lab fiber measurements show good agreement with theoretical predictions for both encoding dimensions, likely due to the controlled environment. Fluctuations in these results are attributed to the drift of the MZMs, which could be mitigated by a continuously operating feedback loop in a system with a higher technological readiness level. In contrast, the spread of values and the deviation from theoretical expectations are significantly greater in measurements over the dark fiber network. These fluctuations may result from unpredictable environmental changes. Both results are presented in Fig. 6.32. The findings highlight the importance of securing the system with additional bandpass filters, as parasitic light leakage could lead to prohibitively high QBER values. Nevertheless, in both cases, the ququart outperforms the qubit, demonstrating higher information entropy and greater resilience to QBER. This aligns with theoretical expectations and supports the central scientific premise of this thesis: high-dimensional symbols generated using spectro-temporal encoding are viable for constructing a quantum key distribution link and present higher robustness to noise. In the future, the experiment could be modernized by using a PIC-based receiver with a TBS [82], as well as a photonic integrated transmitter.

6.3 Chapter summary

In summary, I experimentally demonstrated a high-dimensional BB84 QKD protocol using two- and four-dimensional symbols in an all-fiber setup, utilizing one single-photon detector per measurement basis. By leveraging the temporal Talbot effect, I successfully detect high-dimensional phase-encoded superpositions. Despite a relatively high QBER—primarily caused by the overlap of probability distributions and strongly influenced by detection timing jitter—I achieve positive key rates using the standard HD BB84 security proof. Additionally, I compare theoretically achievable key rates across various dimensions through simulations based on experimentally obtained parameters. I further theoretically examine how basis efficiency mismatch and the chosen security proof significantly impact the final key rate. The comparison is stated for a standard high-dimensional BB84 protocol and the new Tunbale Beam Splitter protocol, which assumes using an experimentally-feasible device for basis choice. My results reveal substantial variations in key rates, where differences arise from the security framework's treatment of potential eavesdropper attacks.

Chapter 7

Final conclusions and outlook

This thesis addresses building a quantum key distribution link using high-dimensional encoding in time and phase. The methods and results obtained during this project pave the way towards constructing simple and secure urban fiber-optic links for exchange of cryptographic keys. The outcomes comprise conclusions from three areas: utilizing photonic integrated circuits for constructing QKD transmitters, detecting high-dimensional superpositions by means of temporal Talbot effect, and conducting the QKD experiment over an in-laboratory fiber and dark fiber network belonging to the University of Warsaw.

The first part serves as a general overview on current optical communication technologies stating the motivation for constructing high-dimensional QKD links. It also serves as an introduction to QKD and photonic integrated circuits.

Experimental techniques are introduced in the Methods section. The discussion encompasses topics around generating and detecting optical signals. It provides a detailed description of electro-optic modulation, addressing both amplitude and phase modulation, as well as related propagation of high-speed electrical signals required for encoding. Emphasis is placed on understanding and characterizing timing jitter effects, which significantly influence quantum effects which are the subject of this dissertation. Furthermore, the use of chromatic dispersion for measuring single-photon spectral properties is discussed.

The following chapter is dedicated to exploring potential of generic indium phosphide PICs for constructing transmitters capable of generating single-photon-level pulses for establishing a QKD link. The exact focus is placed on showcasing the use of an ASPIC for precise temporal and spectral quantum state control capabilities through on-chip components and relative control equipment. The design, fabrication, and characterization of these integrated circuits are detailed, highlighting their potential to significantly reduce complexity, enhance system stability, and support scalability in practical quantum communication applications. Issues such as component integration, thermal management, and electrostatic discharge precautions are discussed, emphasizing best practices essential for maintaining device integrity and operational reliability. The ASPIC was successfully employed for precise generation and control of temporal and spectral profiles of symbols generated at the C-band telecom wavelengths. The system enables simultaneous temporal and spectral measurements resolved at the single-photon counting level. The modulation scheme has been validated as effective in producing pulses with precisely tailored temporal profiles, and therefore spectral characteristics, providing relatively short pulse durations compared to the available bandwidth. Furthermore, it allows accurate control of the central wavelength, essential for frequency-shift keying encoding. The precision in wavelength control is sufficient for FSK encoding schemes. Although this kind of encoding may not be feasible for QKD

due to the fact, that properties of physical components can be strongly wavelength-dependent, the tuning capability is crucial to match DWDM channels of interest. Selection of right channels and tunability are key for ensuring good channel separation, which allows to reduce the QBER stemming from noise originating from in-fiber scattering of signals with launch power being orders of magnitude stronger from quantum signals. It also offers flexibility needed to adapt to the changes in networks and channel management. The duration of the pulse position modulation symbols was limited by the bandwidth of the on-chip modulators, and must be adjusted with respect to desired timebin duration. For most QKD encodings, the performance of the on-chip modulators is good enough to enable quantum communications. Moreover, time lensing [133] could be employed to alter the duration or spectrum of optical signals in favor. Further improvements and possibilities may be reached with recently-emerging photonic integrated technologies. Thin-film lithium niobate (TFLN) platform offers high electro-optic bandwidth, low losses, and engineering of chirped fiber Bragg gratings for dispersive and spectral manipulations [168]. Another new approach is granted by the PolyBoard platform [21]. The polyboard integration allows merging components manufactured using different technologies on one chip. An additional advantage is the possibility to include free-space micro-optical components, such as polarizing beam splitter, spectral filters, or waveplates. Advanced devices such as SPADs can also be integrated, opening new ways for engineering compact transmitters and receivers.

The fifth chapter reports on the development of a quantum state detection method based on the temporal Talbot effect, leveraging space-time duality to achieve robust detection of timebin superpositions without active modulation or complex interferometric setups. This passive method provides a practical alternative to traditional interferometric approaches, notably reducing experimental complexity and minimizing optical losses. The technique's effectiveness is validated experimentally for four-dimensional superposition discrimination, supported by detailed theoretical analysis. Crucial to practical considerations, the thesis examines the influence of timing jitter on detection performance, proposing a post-selection strategy to significantly improve measurement fidelity. The analysis focuses on cases corresponding to different values of timing jitter, as it has the greatest impact of the resultant correctness of the measurement. This detection method is imperfect. Quantum states cannot be distinguished with 100% likelihood due to the overlap of finite number probability distributions of finite-widths. Nevertheless, the method remains considerably useful as it can be scaled to d dimensions while maintaining constant setup complexity. It only requires a single dispersive medium and a time-correlated single photon counter, which makes it an excellent alternative to the Franson interferometer tree and quantum pulse gate approaches. This novel approach to detection constitutes a basis for constructing the final QKD experiment.

In the final chapter of this thesis the construction of an urban QKD link based on high-dimensional spectral-temporal encoding is presented. Two distinct protocols are explored: a high-dimensional BB84 protocol variant and a novel tunable beam splitter protocol designed explicitly to address real-world challenges such as basis-dependent detection efficiencies. A comparison of simulated key rates stemming from the two protocols considering various yet experimentally-feasible QBER values and jitters is provided. The new TBS protocol reveals high sensitivity to detection efficiency mismatch, which could quickly degrade the performance of a QKD system. This is one of the main results of this project. The theoretical analysis is followed by a thorough characterization of the transmitter, quantum channel link, and the receiver, stressing critical values such as modulation contrast, pulse duration, relative impact of chromatic dispersion or stability over long and short periods. Additionally, practical considerations, such as attenuation management, or spectral filtering strategies to suppress noise are highlighted. Experimental validation was performed both in controlled laboratory environments and within the University of Warsaw's urban fiber-optic infrastructure, clearly displaying advantage of ququarts over qubits

in terms of information capacity for both cases, considering security proof for the BB84. This is the second main result of this project. Overall, the thesis advances the fundamental understanding of high-dimensional quantum communication but also contributes tangible solutions and methodologies towards overcoming critical practical limitations, laying the groundwork for next-generation secure quantum networks.

Future advancements in QKD will likely be driven by progress in theoretical security proofs. Practical deployments inherently involve finite-size key blocks, which must be explicitly accounted for in the security analysis. Additionally, extending the formalism to high-dimensional encoding is essential for deriving tighter bounds on achievable key rates in the relevant scenarios. These mathematical developments will pave the way for the introduction of standardization and certification frameworks—critical steps toward the widespread adoption of quantum-secure technologies. From a technical standpoint, higher key rates can be achieved either by employing high-dimensional encoding schemes or by utilizing qubit-based protocols operating at high repetition rates. Choosing the optimal strategy requires careful consideration of system-level trade-offs, including detector dead times, link attenuation, cost, and compliance with implementation recommendations. Furthermore, the use of multiplexing across various degrees of freedom—such as wavelength, time, space, or polarization—can significantly enhance throughput, enabling scalable quantum communication networks.

Bibliography

[1] M. Born, E. Wolf, A. B. Bhatia, P. Clemmow, D. Gabor, A. Stokes, A. Taylor, P. Wayman, and W. Wilcock, *Principles of optics: electromagnetic theory of propagation, interference and diffraction of light*, vol. 7 (Cambridge university press Cambridge, 1999).

[2] F. Arecchi and R. Bonifacio, "Theory of optical maser amplifiers," IEEE Journal of Quantum Electronics **1**, 169–178 (1965).

[3] L. N. Binh, *Optical modulation: Advanced techniques and applications in transmission systems and networks* (CRC Press, 2017).

[4] B. Lavigne, O. Bertran-Pardo, C. Bresson, M. Lefrancois, E. Balmefrezol, M. Le Monnier, L. Raddatz, and L. Suberini, "400 gb/s real-time trials on commercial systems for next generation networks," Journal of Lightwave Technology **34**, 477–483 (2016).

[5] G. Rademacher, R. S. Luis, B. J. Puttnam, T. A. Eriksson, R. Ryf, E. Agrell, R. Maruyama, K. Aikawa, Y. Awaji, H. Furukawa *et al.*, "High capacity transmission with few-mode fibers," Journal of Lightwave Technology **37**, 425–432 (2019).

[6] H. Kanamori, H. Yokota, G. Tanaka, M. Watanabe, Y. Ishiguro, I. Yoshida, T. Kakii, S. Itoh, Y. Asano, and S. Tanaka, "Transmission characteristics and reliability of pure-silica-core single-mode fibers," Journal of Lightwave Technology **4**, 1144–1150 (1986).

[7] E.-G. Neumann, *Single-mode fibers: fundamentals*, vol. 57 (Springer, 2013).

[8] B. J. Puttnam, R. S. Luís, E. Agrell, G. Rademacher, J. Sakaguchi, W. Klaus, G. M. Saridis, Y. Awaji, and N. Wada, "High capacity transmission systems using homogeneous multi-core fibers," Journal of Lightwave Technology **35**, 1157–1167 (2017).

[9] G. P. Agrawal, *Fiber-optic communication systems* (John Wiley & Sons, 2012).

[10] I. Kaminow and T. Li, *Optical fiber telecommunications IV-B: systems and impairments*, vol. 2 (Elsevier, 2002).

[11] P. Cao, X. Hu, L. Zhang, J. Wu, X. Jiang, and Y. Su, "Photonic generation of microwave frequency shift keying signal using a single-drive mach–zehnder modulator," Optics Express **22**, 14433–14440 (2014).

[12] G. Keiser, *Optical fiber communications*, vol. 2 (McGraw-Hill New York, 2000).

[13] I.-T. S. Sector, "Spectral grids for wdm applications: Cwdm wavelength grid," ITU-T Recommendation G. 694.2 (2002).

[14] I. Recommendation *et al.*, "Spectral grids for wdm applications: Dwdm frequency grid," ITU-T G **694** (2006).

[15] H. Rohde, E. Gottwald, A. Teixeira, J. D. Reis, A. Shahpari, K. Pulverer, and J. S. Wey, "Coherent ultra dense wdm technology for next generation optical metro and access networks," Journal of Lightwave Technology **32**, 2041–2052 (2014).

[16] Z.-Y. Chen, L.-S. Yan, Y. Pan, L. Jiang, A.-L. Yi, W. Pan, and B. Luo, "Use of polarization freedom beyond polarization-division multiplexing to support high-speed and spectral-efficient data transmission," Light: Science & Applications **6**, e16207–e16207 (2017).

[17] P. Sillard, M. Bigot-Astruc, and D. Molin, "Few-mode fibers for mode-division-multiplexed systems," Journal of Lightwave Technology **32**, 2824–2829 (2014).

[18] L.-W. Luo, N. Ophir, C. P. Chen, L. H. Gabrielli, C. B. Poitras, K. Bergmen, and M. Lipson, "Wdm-compatible mode-division multiplexing on a silicon chip," Nature Communications **5**, 3069 (2014).

[19] G. Cincotti, T. Murakawa, T. Nagashima, S. Shimizu, M. Hasegawa, K. Hattori, M. Okuno, S. Mino, A. Himeno, N. Wada *et al.*, "Enhanced optical communications through joint time-frequency multiplexing strategies," Journal of Lightwave Technology **38**, 346–351 (2019).

[20] B. Docter, J. Pozo, T. de Vries, E. Geluk, J. Bolk, E. Smalbrugge, F. Karouta, Y. Oei, H. Ambrosius, and M. Smit, "The 243 steps of making photonic integrated circuits in inp," in *Proceedings of the 15th Annual Symposium of the IEEE Photonics Benelux Chapter, 18-19 November 2010, Delft, The Netherlands,* (TNO, 2010), pp. 89–92.

[21] D. De Felipe, M. Kleinert, C. Zawadzki, A. Polatynski, G. Irmscher, W. Brinker, M. Moehrle, H.-G. Bach, N. Keil, and M. Schell, "Recent developments in polymer-based photonic components for disruptive capacity upgrade in data centers," Journal of Lightwave Technology **35**, 683–689 (2016).

[22] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, "New high-intensity source of polarization-entangled photon pairs," Physical Review Letters **75**, 4337 (1995).

[23] A. Trenti, M. Achleitner, F. Prawits, B. Schrenk, H. Conradi, M. Kleinert, A. Incoronato, F. Zanetto, F. Zappa, I. D. Luch *et al.*, "On-chip quantum communication devices," Journal of Lightwave Technology **40**, 7485–7497 (2022).

[24] S. Gyger, J. Zichi, L. Schweickert, A. W. Elshaari, S. Steinhauer, S. F. Covre da Silva, A. Rastelli, V. Zwiller, K. D. Jöns, and C. Errando-Herranz, "Reconfigurable photonics with on-chip single-photon detectors," Nature Communications **12**, 1408 (2021).

[25] F. Beutel, H. Gehring, M. A. Wolff, C. Schuck, and W. Pernice, "Detector-integrated on-chip qkd receiver for ghz clock rates," npj Quantum Information **7**, 40 (2021).

[26] J. Wang, F. Sciarrino, A. Laing, and M. G. Thompson, "Integrated photonic quantum technologies," Nature Photonics **14**, 273–284 (2020).

[27] E. Pelucchi, G. Fagas, I. Aharonovich, D. Englund, E. Figueroa, Q. Gong, H. Hannes, J. Liu, C.-Y. Lu, N. Matsuda *et al.*, "The potential and global outlook of integrated photonics for quantum technologies," Nature Reviews Physics **4**, 194–208 (2022).

[28] R. Wolf, "Quantum key distribution," Lecture notes in physics **988** (2021).

[29] R. Renner, "Security of quantum key distribution," Ph.D. thesis, ETH Zurich (2005).

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

[31] A. Acín, N. Gisin, and L. Masanes, "From bell's theorem to secure quantum key distribution," Physical Review Letters **97**, 120405 (2006).

[32] S. Pironio, A. Acín, S. Massar, A. B. de La Giroday, G. Haack, N. Riba, V. Scarani, G. Ribordy, and H. Zbinden, "Device-independent quantum key distribution secure against collective attacks," New Journal of Physics **11**, 045021 (2009).

[33] J. Bowles, T. Vértesi, M. T. Quintino, and N. Brunner, "One-way einstein–podolsky–rosen steering," Physical Review Letters **112**, 200402 (2014).

[34] L. C. Venancio, R. F. Werner, and C. Palazuelos, "Semi-device-independent quantum key distribution with bounded dimension," Physical Review A **103**, 022422 (2021).

[35] R. Van Handel, J. Habif, and H. Yuen, "Energy-constrained quantum key distribution," IEEE Journal of Selected Topics in Quantum Electronics **15**, 1630–1638 (2009).

[36] A. Winick, N. Lütkenhaus, and P. J. Coles, "Reliable numerical key rates for quantum key distribution," Quantum **2**, 77 (2018).

[37] Y. Piétri, M. Schiavon, V. M. Acosta, B. Gouraud, L. T. Vidarte, P. Grangier, A. Rhouni, and E. Diamanti, "Qosst: A highly-modular open source platform for experimental continuous-variable quantum key distribution," Quantum **8**, 1575 (2024).

[38] M. G. Tanner, V. Makarov, and R. H. Hadfield, "Optimised quantum hacking of superconducting nanowire single-photon detectors," Optics Express **22**, 6734–6748 (2014).

[39] V. Makarov, J.-P. Bourgoin, P. Chaiwongkhot, M. Gagné, T. Jennewein, S. Kaiser, R. Kashyap, M. Legré, C. Minshull, and S. Sajeed, "Creation of backdoors in quantum communications via laser damage," Physical Review A **94**, 030302 (2016).

[40] V. Makarov, "Controlling passively quenched single photon detectors by bright light," New Journal of Physics **11**, 065003 (2009).

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

[42] French Cybersecurity Agency (ANSSI), Federal Office for Information Security (BSI), Netherlands National Communications Security Agency (NLNCSA), and Swedish National Communications Security Authority, Swedish Armed Forces, "Position paper on quantum key distribution," (2024). Accessed March 2025.

[43] Federal Office for Information Security (BSI), "Implementation attacks against qkd systems," (2023).

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

[45] T. Tsurumaru and M. Hayashi, "Dual universality of hash functions and its applications to quantum cryptography," IEEE transactions on information theory **59**, 4700–4717 (2013).

[46] N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," Physical Review A **61**, 052304 (2000).

[47] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, "Quantum key distribution over a 40-db channel loss using superconducting single-photon detectors," Nature Photonics **1**, 343–348 (2007).

[48] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, "Provably secure and practical quantum key distribution over 307 km of optical fibre," Nature Photonics **9**, 163–168 (2015).

[49] C. J. Pugh, S. Kaiser, J.-P. Bourgoin, J. Jin, N. Sultana, S. Agne, E. Anisimova, V. Makarov, E. Choi, B. L. Higgins *et al.*, "Airborne demonstration of a quantum key distribution receiver payload," Quantum Science and Technology **2**, 024009 (2017).

[50] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai *et al.*, "Satellite-based entanglement distribution over 1200 kilometers," Science **356**, 1140–1144 (2017).

[51] J. Krause, N. Walenta, J. Hilt, and R. Freund, "Clock-offset recovery with sublinear complexity enables synchronization on low-level hardware for quantum key distribution," Physical Review Applied **23**, 044015 (2025).

[52] C. Spiess, S. Töpfer, S. Sharma, A. Kržič, M. Cabrejo-Ponce, U. Chandrashekara, N. L. Döll, D. Rieländer, and F. Steinlechner, "Clock synchronization with correlated photons," Physical Review Applied **19**, 054082 (2023).

[53] M. Genovese and P. Traina, "Review on qudits production and their application to quantum communication and studies on local realism," Advanced Science Letters **1**, 153–160 (2008).

[54] N. T. Islam, C. Cahall, A. Aragoneses, A. Lezama, J. Kim, and D. J. Gauthier, "Robust and stable delay interferometers with application to d-dimensional time-frequency quantum key distribution," Phyical Review Applied **7**, 044010 (2017).

[55] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, "Security of quantum key distribution using d-level systems," Physical Review Letters **88**, 127902 (2002).

[56] M. Y. Niu, F. Xu, J. H. Shapiro, and F. Furrer, "Finite-key analysis for time-energy high-dimensional quantum key distribution," Physical Review A **94**, 052323 (2016).

[57] H. Bechmann-Pasquinucci and W. Tittel, "Quantum cryptography using larger alphabets," Physical Review A **61**, 062308 (2000).

[58] C. Lee, D. Bunandar, Z. Zhang, G. R. Steinbrecher, P. Ben Dixon, F. N. Wong, J. H. Shapiro, S. A. Hamilton, and D. Englund, "Large-alphabet encoding for higher-rate quantum key distribution," Optics Express **27**, 17539–17549 (2019).

[59] R. Terhaar, J. Rödiger, M. Häußler, M. Wahl, H. Gehring, M. A. Wolff, F. Beutel, W. Hartmann, N. Walter, J. Hanke *et al.*, "Ultrafast quantum key distribution using fully parallelized quantum channels," Optics Express **31**, 2675–2688 (2023).

[60] F. Grünenfelder, A. Boaron, G. V. Resta, M. Perrenoud, 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 enable high secret-key-rate quantum key distribution systems," Nature Photonics **17**, 422–426 (2023).

[61] F. Grünenfelder, R. Sax, A. Boaron, and H. 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** (2021).

[62] F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden, "Performance and security of 5 ghz repetition rate polarization-based quantum key distribution," Applied Physics Letters **117** (2020).

[63] U. L. Andersen, T. Gehring, C. Marquardt, and G. Leuchs, "30 years of squeezed light generation," Physica Scripta **91**, 053001 (2016).

[64] A. Marie and R. Alléaume, "Self-coherent phase reference sharing for continuous-variable quantum key distribution," Physical Review A **95**, 012316 (2017).

[65] Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, "Long-distance continuous-variable quantum key distribution over 202.81 km of fiber," Physical Review Letters **125**, 010502 (2020).

[66] 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).

[67] 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 *et al.*, "Twin-field quantum key distribution over 830-km fibre," Nature Photonics **16**, 154–161 (2022).

[68] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, "Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system," Physical Review X **9**, 021046 (2019).

[69] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin *et al.*, "Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km," Physical Review Letters **124**, 070501 (2020).

[70] X. Zhong, W. Wang, L. Qian, and H.-K. Lo, "Proof-of-principle experimental demonstration of twin-field quantum key distribution over optical channels with asymmetric losses," npj Quantum Information **7**, 8 (2021).

[71] C. Clivati, A. Meda, S. Donadello, S. Virzì, M. Genovese, F. Levi, A. Mura, M. Pittaluga, Z. Yuan, A. J. Shields *et al.*, "Coherent phase transfer for real-world twin-field quantum key distribution," Nature Communications **13**, 157 (2022).

[72] A. Ekert, "Quantum cryptography based on Bell's theorem," Physical Review Letters **67**, 661—663 (1991).

[73] M. Fujiwara, K.-i. Yoshino, Y. Nambu, T. Yamashita, S. Miki, H. Terai, Z. Wang, M. Toyoshima, A. Tomita, and M. Sasaki, "Modified e91 protocol demonstration with hybrid entanglement photon source," Optics Express **22**, 13616–13624 (2014).

[74] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," Physical Review Letters **108**, 130503 (2012).

[75] K. N. Wilkinson, P. Papanastasiou, C. Ottaviani, T. Gehring, and S. Pirandola, "Long-distance continuous-variable measurement-device-independent quantum key distribution with postselection," Physical Review Research **2**, 033424 (2020).

[76] H. Liu, W. Wang, K. Wei, X.-T. Fang, L. Li, N.-L. Liu, H. Liang, S.-J. Zhang, W. Zhang, H. Li *et al.*, "Experimental demonstration of high-rate measurement-device-independent quantum key distribution over asymmetric channels," Physical Review Letters **122**, 160501 (2019).

[77] J. Nunn, L. Wright, C. Söller, L. Zhang, I. Walmsley, and B. Smith, "Large-alphabet time-frequency entangled quantum key distribution by means of time-to-frequency conversion," Optics Express **21**, 15959–15973 (2013).

[78] X. Liu, X. Yao, H. Wang, H. Li, Z. Wang, L. You, Y. Huang, and W. Zhang, "Energy-time entanglement-based dispersive optics quantum key distribution over optical fibers of 20 km," Applied Physics Letters **114** (2019).

[79] Y. Pelet, G. Sauder, M. Cohen, L. Labonté, O. Alibart, A. Martin, and S. Tanzilli, "Operational entanglement-based quantum key distribution over 50 km of field-deployed optical fibers," Physical Review Applied **20**, 044006 (2023).

[80] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," Advances in Optics and Photonics **12**, 1012–1236 (2020).

[81] C. Ma, W. D. Sacher, Z. Tang, J. C. Mikkelsen, Y. Yang, F. Xu, T. Thiessen, H.-K. Lo, and J. K. Poon, "Silicon photonic transmitter for polarization-encoded quantum key distribution," Optica **3**, 1274–1278 (2016).

[82] 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**, 13984 (2017).

[83] D. Bunandar, A. Lentine, C. Lee, H. Cai, C. M. Long, N. Boynton, N. Martinez, C. DeRose, C. Chen, M. Grein *et al.*, "Metropolitan quantum key distribution with silicon photonics," Physical Review X **8**, 021009 (2018).

[84] G. Zhang, J. Y. Haw, H. Cai, F. Xu, S. Assad, J. F. Fitzsimons, X. Zhou, Y. Zhang, S. Yu, J. Wu *et al.*, "An integrated silicon photonic chip platform for continuous-variable quantum key distribution," Nature Photonics **13**, 839–842 (2019).

[85] W. Geng, C. Zhang, Y. Zheng, J. He, C. Zhou, and Y. Kong, "Stable quantum key distribution using a silicon photonic transceiver," Optics Express **27**, 29045–29054 (2019).

[86] K. Wei, W. Li, H. Tan, Y. Li, H. Min, W.-J. Zhang, H. Li, L. You, Z. Wang, X. Jiang *et al.*, "High-speed measurement-device-independent quantum key distribution with integrated silicon photonics," Physical Review X **10**, 031030 (2020).

[87] T. K. Paraïso, I. De 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 Information **5**, 42 (2019).

[88] 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," Nature Photonics **15**, 850–856 (2021).

[89] 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).

[90] J. A. Dolphin, T. K. Paraïso, H. Du, R. I. Woodward, D. G. Marangon, and A. J. Shields, "A hybrid integrated quantum key distribution transceiver chip," npj Quantum Information **9**, 84 (2023).

[91] S. Pirandola, "Symmetric collective attacks for the eavesdropping of symmetric quantum key distribution," International Journal of Quantum Information **6**, 765–771 (2008).

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

[93] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, "Optimal eavesdropping in quantum cryptography. i. information bound and optimal strategy," Physical Review A **56**, 1163 (1997).

[94] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Physical Review Letters **94**, 230504 (2005).

[95] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," Physical Review A **72**, 012326 (2005).

[96] D. Rusca, A. Boaron, F. Grünenfelder, A. Martin, and H. Zbinden, "Finite-key analysis for the 1-decoy state qkd protocol," Applied Physics Letters **112** (2018).

[97] J. Wiesemann, J. Krause, D. Tupkary, N. Lütkenhaus, D. Rusca, and N. Walenta, "A consolidated and accessible security proof for finite-size decoy-state quantum key distribution," arXiv preprint arXiv:2405.16578 (2024).

[98] F. Grasselli, *Quantum Cryptography* (SpringerCham, 2021).

[99] B. E. Saleh and M. C. Teich, *Fundamentals of photonics* (john Wiley & sons, 2019).

[100] L. M. Augustin, R. Santos, E. Den Haan, S. Kleijn, P. J. Thijs, S. Latkowski, D. Zhao, W. Yao, J. Bolk, H. Ambrosius *et al.*, "Inp-based generic foundry platform for photonic integrated circuits," IEEE Journal of Selected Topics in Quantum Electronics **24**, 1–10 (2017).

[101] Z. Li, R. N. Wang, G. Lihachev, J. Zhang, Z. Tan, M. Churaev, N. Kuznetsov, A. Siddharth, M. J. Bereyhi, J. Riemensberger *et al.*, "High density lithium niobate photonic integrated circuits," Nature Communications **14**, 4856 (2023).

[102] M. Seimetz, *High-order modulation for optical fiber transmission*, vol. 143 (Springer, 2009).

[103] K. Kurokawa, "Power waves and the scattering matrix," IEEE transactions on microwave theory and techniques **13**, 194–202 (1965).

[104] D. M. Pozar, *Microwave engineering: theory and techniques* (John wiley & sons, 2021).

[105] G. Gonzalez, *Microwave Transistor Amplifiers analysis and design* (Prentice Hall, Inc, 1997).

[106] European Telecommunications Standards Institute, "Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems," Tech. Rep. GS QKD 011 V1.1.1, ETSI (2023). Accessed: 2025-04-12.

[107] M. R. B. Wagner, D. Vogrig, P. Villoresi, G. Vallone, and A. Stanco, "A time-to-digital converter with steady calibration through single-photon detection," arXiv preprint arXiv:2406.01293 (2024).

[108] L. You, "Superconducting nanowire single-photon detectors for quantum information," Nanophotonics **9**, 2673–2692 (2020).

[109] D. Pastor, J. Capmany, D. Ortega, V. Tatay, and J. Martí, "Design of apodized linearly chirped fiber gratings for dispersion compensation," Journal of Lightwave Technology **14**, 2581–2588 (1996).

[110] T. Erdogan, "Fiber grating spectra," Journal of Lightwave Technology **15**, 1277–1294 (1997).

[111] A. Golestani, "Temporal shaping and measurement of pulsed quantum light," Ph.D. thesis, University of Warsaw (2023).

[112] A. M. Weiner, *Ultrafast optics* (John Wiley & Sons, 2011).

[113] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, "Provably secure and high-rate quantum key distribution with time-bin qudits," Science Advances **3**, e1701491 (2017).

[114] A. Widomski, S. Stopiński, K. Anders, R. Piramidowicz, and M. Karpiński, "Precise on-chip spectral and temporal control of single-photon-level optical pulses," Journal of Lightwave Technology pp. 1–8 (2023).

[115] 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 *et al.*, "Long-distance copropagation of quantum key distribution and terabit classical optical data channels," Physical Review A **95**, 012301 (2017).

[116] Z. Chang-Hua, P. Chang-Xing, Q. Dong-Xiao, G. Jing-Liang, C. Nan, and Y. Yun-Hui, "A new quantum key distribution scheme based on frequency and time coding," Chinese Physics Letters **27**, 090301 (2010).

[117] S. F. Yelin and B. C. Wang, "A novel time-frequency quantum key distribution technique for optical fiber communication systems," in *Optical Fiber Communication Conference,* (Optica Publishing Group, 2004), p. TuN1.

[118] T. Zhong, H. Zhou, R. D. Horansky, C. Lee, V. B. Verma, A. E. Lita, A. Restelli, J. C. Bienfang, R. P. Mirin, T. Gerrits *et al.*, "Photon-efficient quantum key distribution using time–energy entanglement with high-dimensional encoding," New Journal of Physics **17**, 022002 (2015).

[119] N. T. Islam, C. C. W. Lim, C. Cahall, B. Qi, J. Kim, and D. J. Gauthier, "Scalable high-rate, high-dimensional time-bin encoding quantum key distribution," Quantum Science and Technology **4**, 035008 (2019).

[120] L. Serino, J. Gil-Lopez, M. Stefszky, R. Ricken, C. Eigner, B. Brecht, and C. Silberhorn, "Realization of a multi-output quantum pulse gate for decoding high-dimensional temporal modes of single-photon states," PRX Quantum **4**, 020306 (2023).

[121] D. Bacco, B. Da Lio, D. Cozzolino, F. Da Ros, X. Guo, Y. Ding, Y. Sasaki, K. Aikawa, S. Miki, H. Terai *et al.*, "Boosting the secret key rate in a shared quantum and classical fibre communication system," Communications Physics **2**, 140 (2019).

[122] M. Leifgen, R. Elschner, N. Perlot, C. Weinert, C. Schubert, and O. Benson, "Practical implementation and evaluation of a quantum-key-distribution scheme based on the time-frequency uncertainty," Physical Review A **92**, 042311 (2015).

[123] J. Rödiger, N. Perlot, R. Mottola, R. Elschner, C.-M. Weinert, O. Benson, and R. Freund, "Numerical assessment and optimization of discrete-variable time-frequency quantum key distribution," Physical Review A **95**, 052312 (2017).

[124] G. E. Hoefler, Y. Zhou, M. Anagnosti, A. Bhardwaj, P. Abolghasem, A. James, S. Luna, P. Debackere, A. Dentai, T. Vallaitis *et al.*, "Foundry development of system-on-chip inp-based photonic integrated circuits," IEEE Journal of Selected Topics in Quantum Electronics **25**, 1–17 (2019).

[125] Z. Liu and R. Slavík, "Optical injection locking: From principle to applications," Journal of Lightwave Technology **38**, 43–59 (2020).

[126] C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. W. Mitchell, "Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode," Optics Express **22**, 1645–1654 (2014).

[127] J. Zhang, L. Bogaert, C. Krückel, E. Soltanian, H. Deng, B. Haq, J. Rimböck, J. Van Kerrebrouck, G. Lepage, P. Verheyen *et al.*, "Micro-transfer printing inp c-band soas on advanced silicon photonics platform for lossless mzi switch fabrics and high-speed integrated transmitters," Optics Express **31**, 42807–42821 (2023).

[128] A. J. Ward, D. J. Robbins, G. Busico, E. Barton, L. Ponnampalam, J. P. Duck, N. D. Whitbread, P. J. Williams, D. C. Reid, A. C. Carter *et al.*, "Widely tunable ds-dbr laser with monolithically integrated soa: Design and performance," IEEE Journal of Selected Topics in Quantum Electronics **11**, 149–156 (2005).

[129] K. Vanmol, K. Saurav, V. Panapakkam, H. Thienpont, N. Vermeulen, J. Watté, and J. Van Erps, "Mode-field matching down-tapers on single-mode optical fibers for edge coupling towards generic photonic integrated circuit platforms," Journal of Lightwave Technology **38**, 4834–4842 (2020).

[130] A. Widomski, M. Ogrodnik, and M. Karpiński, "Efficient detection of multidimensional single-photon time-bin superpositions," Optica **11**, 926–931 (2024).

[131] B. H. Kolner, "Space-time duality and the theory of temporal imaging," IEEE Journal of Quantum Electronics **30**, 1951–1963 (1994).

[132] F. Sośnicki, M. Mikołajczyk, A. Golestani, and M. Karpiński, "Interface between picosecond and nanosecond quantum light pulses," Nature Photonics **17**, 761–766 (2023).

[133] F. Sośnicki, "Spectral shaping of quantum light pulses by electro-optic phase modulation," Ph.D. thesis, University of Warsaw (2023).

[134] L. Rayleigh, "Xxv. on copying diffraction-gratings, and on some phenomena connected therewith," The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science **11**, 196–205 (1881).

[135] S. Chowdhury, J. Chen, and J. A. Izatt, "Structured illumination fluorescence microscopy using talbot self-imaging effect for high-throughput visualization," arXiv preprint arXiv:1801.03540 (2018).

[136] A. Isoyan, F. Jiang, Y. Cheng, F. Cerrina, P. Wachulak, L. Urbanski, J. Rocca, C. Menoni, and M. Marconi, "Talbot lithography: self-imaging of complex structures," Journal of Vacuum Science & Technology B: Microelectronics and Nanometer Structures Processing, Measurement, and Phenomena **27**, 2931–2937 (2009).

[137] G. S. Spagnolo, D. Ambrosini, and D. Paoletti, "Displacement measurement using the talbot effect with a ronchi grating," Journal of Optics A: Pure and Applied Optics **4**, S376 (2002).

[138] J. Azaña and M. A. Muriel, "Temporal self-imaging effects: theory and application for multiplying pulse repetition rates," IEEE Journal of Selected Topics in Quantum Electronics **7**, 728–744 (2001).

[139] A. Eckstein, B. Brecht, and C. Silberhorn, "A quantum pulse gate based on spectrally engineered sum frequency generation," Optics Express **19**, 13770–13778 (2011).

[140] D. V. Reddy and M. G. Raymer, "High-selectivity quantum pulse gating of photonic temporal modes using all-optical Ramsey interferometry," Optica **5**, 423–428 (2018).

[141] V. Ansari, G. Harder, M. Allgaier, B. Brecht, and C. Silberhorn, "Temporal-mode measurement tomography of a quantum pulse gate," Physical Review A **96**, 063817 (2017).

[142] H.-H. Lu, N. B. Lingaraju, D. E. Leaird, A. M. Weiner, and J. M. Lukens, "High-dimensional discrete fourier transform gates with a quantum frequency processor," Optics Express **30**, 10126–10134 (2022).

[143] M. Kues, C. Reimer, P. Roztocki, L. R. Cortés, S. Sciara, B. Wetzel, Y. Zhang, A. Cino, S. T. Chu, B. E. Little, D. J. Moss, L. Caspani, J. Azaña, and R. Morandotti, "On-chip generation of high-dimensional entangled quantum states and their coherent control," Nature **546**, 622–626 (2017).

[144] H.-H. Lu, K. V. Myilswamy, R. S. Bennink, S. Seshadri, M. S. Alshaykh, J. Liu, T. J. Kippenberg, D. E. Leaird, A. M. Weiner, and J. M. Lukens, "Bayesian tomography of high-dimensional on-chip biphoton frequency combs with randomized measurements," Nature Communications **13**, 4338 (2022).

[145] J. M. Lukens and P. Lougovski, "Frequency-encoded photonic qubits for scalable quantum information processing," Optica **4**, 8–16 (2017).

[146] J. D. Franson, "Bell inequality for position and time," Physical Review Letters **62**, 2205 (1989).

[147] T. Brougham, S. M. Barnett, K. T. McCusker, P. G. Kwiat, and D. J. Gauthier, "Security of high-dimensional quantum key distribution protocols using Franson interferometers," Journal of Physics B **46**, 104010 (2013).

[148] M. Karpiński, A. O. Davis, F. Sośnicki, V. Thiel, and B. J. Smith, "Control and measurement of quantum light pulses for quantum information science and technology," Advanced Quantum Technologies **4**, 2000150 (2021).

[149] K. Goda and B. Jalali, "Dispersive Fourier transformation for fast continuous single-shot measurements," Nature Photonics **7**, 102–112 (2013).

[150] A. O. C. Davis, P. M. Saulnier, M. Karpiński, and B. J. Smith, "Pulsed single-photon spectrometer by frequency-to-time mapping using chirped fiber Bragg gratings," Optics Express **25**, 12804–12811 (2017).

[151] M. Avenhaus, A. Eckstein, P. J. Mosley, and C. Silberhorn, "Fiber-assisted single-photon spectrograph," Optics Letters **34**, 2873–2875 (2009).

[152] M. Närhi, L. Salmela, J. Toivonen, C. Billet, J. M. Dudley, and G. Genty, "Machine learning analysis of extreme events in optical fibre modulation instability," Nature Communications **9**, 4923 (2018).

[153] K. Sedziak-Kacprowicz, A. Czerwinski, and P. Kolenderski, "Tomography of time-bin quantum states using time-resolved detection," Physical Review A **102**, 052420 (2020).

[154] H. F. Talbot, "Facts relating to optical science. No. IV," Philosophical Magazine **9**, 401–407 (1836).

[155] S. Barnett, *Quantum information*, vol. 16 (Oxford University Press, 2009).

[156] T. Ikuta, S. Akibue, Y. Yonezu, T. Honjo, H. Takesue, and K. Inoue, "Scalable implementation of $(d+1)$ mutually unbiased bases for d-dimensional quantum key distribution," Physical Review Research **4**, L042007 (2022).

[157] V. Torres-Company, J. Lancis, and P. Andres, "Space-time analogies in optics," Progress in Optics **56**, 1–80 (2011).

[158] R. O. Duda, P. E. Hart, and D. G. Stork, *Pattern classification* (John Wiley & Sons, 2000).

[159] B. Korzh, Q.-Y. Zhao, J. P. Allmaras, S. Frasca, T. M. Autry, E. A. Bersin, A. D. Beyer, R. M. Briggs, B. Bumble, M. Colangelo *et al.*, "Demonstration of sub-3 ps temporal resolution with a superconducting nanowire single-photon detector," Nature Photonics **14**, 250–255 (2020).

[160] F. Vedovato, C. Agnesi, M. Tomasin, M. Avesani, J.-A. Larsson, G. Vallone, and P. Villoresi, "Postselection-loophole-free bell violation with genuine time-bin entanglement," Physical Review Letters **121**, 190401 (2018).

[161] S. Wang, Z.-Q. Yin, H. Chau, W. Chen, C. Wang, G.-C. Guo, and Z.-F. Han, "Proof-of-principle experimental realization of a qubit-like qudit-based quantum key distribution scheme," Quantum Science and Technology **3**, 025006 (2018).

[162] F. Grasselli, G. Chesi, N. Walk, H. Kampermann, A. Widomski, M. Ogrodnik, M. Karpiński, C. Macchiavello, D. Bruß, and N. Wyderka, "Quantum key distribution with basis-dependent detection probability," Physical Review Applied **23**, 044011 (2025).

[163] M. Ogrodnik, A. Widomski, D. Bruß, G. Chesi, F. Grasselli, H. Kampermann, C. Macchiavello, N. Walk, N. Wyderka, and M. Karpiński, "High-dimensional quantum key distribution with resource-efficient detection," arXiv preprint arXiv:2412.16782 (2024).

[164] D. Scalcon, E. Bazzani, G. Vallone, P. Villoresi, and M. Avesani, "Low-error encoder for time-bin and decoy states for quantum key distribution," npj Quantum Information **11**, 22 (2025).

[165] I. Vagniluca, B. Da Lio, D. Rusca, D. Cozzolino, Y. Ding, H. Zbinden, A. Zavatta, L. K. Oxenløwe, and D. Bacco, "Efficient time-bin encoding for practical high-dimensional quantum key distribution," Physical Review Applied **14**, 014051 (2020).

[166] M. Tomamichel and A. Leverrier, "A largely self-contained and complete security proof for quantum key distribution," Quantum **1**, 14 (2017).

[167] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," Physical Review Letters **94**, 230503 (2005).

[168] D. Zhu, C. Chen, M. Yu, L. Shao, Y. Hu, C. Xin, M. Yeh, S. Ghosh, L. He, C. Reimer *et al.*, "Spectral control of nonclassical light pulses using an integrated thin-film lithium niobate modulator," Light: Science & Applications **11**, 327 (2022).